Bundesministerium der Verteidigung

A-960/1

Zentrale Dienstvorschrift

Informationssicherheit

Zweck der Regelung:	Festlegung der Grundsätze für die Herstellung, Überwachung, Gewährleistung und Wiederherstellung der Informationssicherheit
Herausgegeben durch:	Bundesministerium der Verteidigung
Beteiligte Interessenvertretungen:	Hauptpersonalrat beim BMVg, Gesamtvertrauenspersonenausschuss beim BMVg
Gebilligt durch:	Staatssekretär Zimmer
Herausgebende Stelle:	BMVg CIT II 2
Geltungsbereich:	Geschäftsbereich des Bundesministeriums der Verteidigung
Einstufung:	Offen
Einsatzrelevanz:	Ja
Berichtspflichten:	Nein
Vorläufig gültig ab:	05.03.2019
Frist zur Überprüfung:	04.03.2024
Version:	2
Ersetzt:	1. A-960/1, Version 1 2. A-960/16 3. BMVg CISO Ressort – Az 82-00-02 vom 06.03.2017 „Aufstellung der Abteilung CIT im BMVg, hier: Änderungen in der IT-Sicherheitsorganisation der Bundeswehr“ 4. BMVg CIT II 2 – Az 82-00-02 vom 13.04.2017 „Aufstellung des KdoCIR, hier: Anpassung der Regelungen zur IT-Sicherheit inkl. Kryptosicherheit und Abstrahlsicherheit“ 5. BMVg CISO Ressort – Az 82-00-02 vom 20.07.2017 „Notwendige Anpassungen in der Organisation der IT-Sicherheit und Erweiterung der IT-Sicherheit um Aspekte der Informationssicherheit“
Aktenzeichen:	82-00-02
Bestellnummer/DSK:	Entfällt

Inhaltsverzeichnis

1 Grundlagen

1.1 Zweck

101. Die vorliegende Zentrale Dienstvorschrift (ZDv) legt auf der Grundlage des Konzeptes K-10/2 „IT-Strategie des Geschäftsbereichs BMVg (siehe Bezug Anlage 11.15 (lfdNr. 13)) die Grundsätze für die Herstellung, Überwachung, Gewährleistung und Wiederherstellung der Informationssicherheit (InfoSichh) fest. Dabei macht diese Zentrale Dienstvorschrift Vorgaben für

- eine übergreifende Betrachtung der InfoSichh[1] einschließlich der IT-relevanten Anteile des Datenschutzes, der Militärischen Sicherheit und des Geheimschutzes,
- die Überwachung der InfoSichh im IT-System der Bundeswehr (IT-SysBw) durch den bzw. die Chief Information Security Officer der Bundeswehr (CISOBw) mit Unterstützung durch das Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw), insbesondere der Abteilungen Cyber Security Operation Center der Bundeswehr (CSOCBw) sowie Überprüfung / Unterstützung (Üprfg/Ustg) im ZCSBw,
- die Planung und Vorgabe von InfoSichh-Maßnahmen sowie deren Umsetzung in den Anwendungsbereichen[2] und
- die Sensibilisierung aller Mitarbeiter bzw. Mitarbeiterinnen, besonders aber aller Vorgesetzen als Grundvoraussetzung für die Stärkung der InfoSichh in der Bundeswehr (Bw)

und berücksichtigt dabei

- Cyber-Sicherheit[3] als Teil der InfoSichh,
- die Bestimmungen der Zentralen Dienstvorschrift A-1130/2 VS-NfD „Militärische Sicherheit in der Bundeswehr – Verschlusssachen“ (siehe Bezug Anlage 11.15 (lfdNr. 15)) und der Verschlusssachenanweisung des Bundes (VSA, siehe Bezug Anlage 11.15 (lfdNr. 11)),
- die Bestimmungen der Zentralen Dienstvorschrift A-2122/4 „Datenschutz“ (siehe Bezug Anlage 11.15 (lfdNr. 10)),
- den IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mit bundeswehrspezifischen Ergänzungen, durch dessen Anwendung die in der Bw zu erstellenden bzw. erstellten Informationssicherheitskonzepte (InfoSichhK) nach einer standardisierten Methodik zu erstellen bzw. fortzuschreiben und an einheitlichen Kriterien auszurichten sind, sowie
- die InfoSichh betreffende Anforderungen der Hauptprozesse sowie der schutzbedarfsverantwortlichen Referate (SBV)[4] im BMVg.

---

1 Definition siehe Nr. 108
2 vgl. Abschnitt 4
3 Unter dem Begriff Cyber-Sicherheit werden alle Maßnahmen der „Cyber-Sicherheitsstrategie für Deutschland“ (siehe Bezug Anlage 11.15 (LfdNr. 44)) sowie die in der Enhanced NATO Policy on Cyber Defence (siehe Bezug Anlage 11.15 (LfdNr. 28)) enthaltenen Vorgaben subsumiert.
4 Zu den SBV gehören u.a. BMVg A I 3, BMVg FüSK II 5, BMVg SE I 1, BMVg R I 5, BMVg R III 4, BMVg R III 3, BMVg R II 5, BMVg R III 2, BMVg CIT II 2.

1.2 Übergangsregelung

102. InfoSichhK der Bw sind nach der Methodik des IT-Grundschutzes gemäß dieser Zentralen Dienstvorschrift zu erstellen.

Die zuständigen Rollenträgerinnen und Rollenträger aller Anwendungsbereiche (siehe Abschnitt 4.1) stellen sicher, dass alle InfoSichhK (siehe Abschnitt 6.3) in ihrer Verantwortung bis spätestens 30.06.2019 (siehe Abschnitte 4.2 – 4.7) bzw. 31.12.2020 (siehe Abschnitte 4.8 – 4.9) nach der Methodik des IT-Grundschutzes erstellt bzw. umgestellt[5] und in Kraft gesetzt sind. Für neu zu erstellende InfoSichhK ist immer die IT-Grundschutz-Methodik des BSI gem. Abschnitt 1.5.2 und ihre Umsetzung in der Bw gem. Anlage 11.1 dieser Zentralen Dienstvorschrift anzuwenden.

Ausnahmen sind durch den bzw. die CISOBw zu genehmigen[6].

103. In begründeten Ausnahmefällen ist eine befristete (bis zu den Terminen gemäß Nr. 102) Weiternutzung der Methodik gemäß Anlage 11.13 (z.B. für die Fortschreibung bereits erlassener InfoSichhK, wenn es sich lediglich um geringfügige Anpassungen handelt)

- mit der Deutschen militärischen Security Accreditation Authority (DEUmilSAA) im ZCSBw für projektbezogene InfoSichhK (InfoSichhKProj, einschl. der InfoSichhK für IT aus Infrastruktur- / Baumaßnahmen gemäß Abschnitt 4.5) sowie InfoSichhK Forschung und Wissenschaft (InfoSichhKFW) und
- mit dem bzw. der CISOBw für dienststellen- / einsatzbezogene InfoSichhK sowie InfoSichh-Befehlen gemäß Abgrenzung in Nr. 648

abzustimmen.

104. Ergänzende Einzelheiten zu Nr. 103 sind durch CISOBw bzw. hinsichtlich einsatzbezogener Belange durch den Informationssicherheitsbeauftragten bzw. die Informationssicherheitsbeauftragte (ISB) Einsatz festzulegen.

1.3 Aufbau der Zentralen Dienstvorschrift

105. Diese Zentrale Dienstvorschrift gliedert sich in drei Teile.

Der „Allgemeine Teil“ beschreibt in den Abschnitten 1 bis 4

- die Grundlagen und übergeordneten Aspekte der InfoSichh,
- den Informationssicherheitsmanagementprozess der Bw,

[5] Umgestellt bedeutet in diesem Zusammenhang, dass das InfoSichhK gemäß der Methodik des IT-Grundschutzes gemäß dieser Zentralen Dienstvorschrift erstellt und in Kraft gesetzt ist. Dabei müssen noch nicht alle im Konzept definierten InfoSichh-Maßnahmen vollständig umgesetzt sein. Jedoch ist für nicht umgesetzte Maßnahmen eine Risikoanalyse gemäß Abschnitt 6.2 dieser Regelung erforderlich.

[6] Anträge an E-Mail-Adresse „CISOBw@bundeswehr.org“.

- die Methodik zur Ermittlung und Deckung des Schutzbedarfes mit dem wesentlichen Element Informationsstruktur,
- die Informationssicherheitsorganisation der Bw mit ihren Aufgaben und Zuständigkeiten,
- die Anwendungsbereiche der InfoSichh (z. B. Dienststellen (DSt), Einsatzkontingente (EinsKtgt), IT-Projekte / Projekte mit IT-Anteil - im Folgenden in dieser Zentralen Dienstvorschrift nur noch als Projekte (Proj) bezeichnet - nach Customer Product Management (CPM), Forschungsvorhaben, Infrastruktur- / Baumaßnahmen mit IT-Anteil) mit den hiermit verbundenen Verantwortlichkeiten und Zuständigkeiten sowie der darin durchzuführenden Tätigkeiten und
- die zuständigen Rollenträgerinnen und Rollenträger der InfoSichh (z. B. Projektleiter bzw. Projektleiterin (ProjLtr), Dienststellenleiter bzw. Dienststellenleiterin (DStLtr), Leitende von Forschungsvorhaben, ISB, Verantwortlicher bzw. Verantwortliche für Infrastruktur- / Baumaßnahmen mit IT-Anteil).

106. Der „Modulteil“ konkretisiert in den Abschnitten 5 bis 10 die im „Allgemeinen Teil“ (siehe Abschnitt 1 – 4) genannten Tätigkeiten der Rollenträgerinnen und Rollenträger. Er beschreibt in einzelnen, den Rollenträgerinnen und Rollenträgern zugeordneten und inhaltlich nicht aufeinander aufbauenden Modulen:

- InfoSichh-Verfahren (Vorgaben zur Evaluierung, Zertifizierung und Zulassung von Produkten der InfoSichh, Akkreditierungen, Freigaben zur Nutzung, Bestellungen von ISB),
- Informationssicherheitsdokumentation (InfoSichhK, Durchführung von Risikoanalysen, Berichte) in den Anwendungsbereichen,
- Tätigkeiten der Rollenträgerinnen und Rollenträger im Rahmen der Gewährleistung und Überwachung der InfoSichh (z.B. das Vorgehen bei Informationssicherheitsvorkommnissen (InfoSichhVork)),
- Aufgaben der ISB sowie
- Grundsätze zur Ausbildung und Sensibilisierung.

107. Der „Anlagenteil“ in Anlage 11 enthält Musterformulare, Gliederungsvorgaben und andere Arbeitsanleitungen (z. B. für die Festlegung des Schutzbedarfes und Grundsätze für die Festlegung von InfoSichh-Maßnahmen) sowie einen Katalog ergänzender InfoSichh-Anforderungen und -Maßnahmen für höheren Schutzbedarf sowie Maßnahmen für Sonstige Schutzbedürftige Informationen (SSI, siehe Nr. 206). Dieser Teil wird bei Bedarf in Verantwortung des bzw. der CISOBw aktualisiert. CISOBw stellt den jeweils aktuellen Stand des „Anlagenteils“ im IntranetBw unter http://infosichh.bundeswehr.org im Bereich „Fachinformationen / Regelungen / A-960/1“ sowie in weiteren hierfür bei der Bw vorgesehenen Medien zur Verfügung (z. B. Regelungen-ONLINE oder dem Formularmanagementsystem).

1.4 Grundlagen der Informationssicherheit in der Bundeswehr

1.4.1 Allgemeines

108. Als InfoSichh **im Sinne dieser Zentralen Dienstvorschrift** bezeichnet man die Eigenschaft informationsverarbeitender und / oder -übertragender Informationstechnik[7] (IT) und ihres Einsatzumfeldes, welche die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen (Grundwerte der InfoSichh gemäß Nr. 111) sowie weitere Gewährleistungsziele wie „Nichtverkettung“, „Transparenz“ und „Intervenierbarkeit“ (siehe Nr. 112) in dem geforderten Maß gewährleistet. InfoSichh wird über das **Informationssicherheitsmanagementsystem der Bundeswehr (ISMS Bw)** sichergestellt. Das ISMS Bw setzt sich zusammen aus

- Sicherheitsprozessen,
- Mitarbeitern,
- Managementprinzipien und
- Ressourcen

und beschreibt das Zusammenspiel von Aufbau- und Ablauforganisation, Anwendungsbereichen und Rollenträgerinnen und Rollenträger (mit ihren Aufgaben, Kompetenzen und Verantwortungen). Durch das ISMS Bw werden – unterstützt durch einen Informationssicherheitsmanagementprozess (Nr. 109) – die Planung, Umsetzung, Gewährleistung und Überwachung

- von technischen Maßnahmen bzw. Maßnahmen an der IT selbst (**Technische InfoSichh**) sowie
- von personellen, infrastrukturellen und organisatorischen Maßnahmen im Einsatzumfeld der IT[8] (**Sicheres IT-Umfeld**).

erreicht.

Der Begriff der InfoSichh entspricht dem der IT-Sicherheit und wird inhaltlich von Aspekten der Computersicherheit, Datensicherheit, Cyber Defence, Cyber-Sicherheit sowie den IT-relevanten Anteilen des Datenschutzes, der Militärischen Sicherheit und des Geheimschutzes bestimmt. Abstrahl- und Kryptosicherheit sind ebenfalls Bestandteil der InfoSichh, wie auch die Belange weiterer fachlich bzw. inhaltlich bestehender Schutzbedarfe im Geschäftsbereich BMVg.

109. Die Planung, Umsetzung, Gewährleistung und Überwachung von InfoSichh-Maßnahmen werden in der Bw in einem Prozessmodell abgebildet, das sich am **PDCA-Modell**[9] orientiert und die in der Abb. 1 dargestellten grundlegenden Prozesse enthält.

---

7 Der Begriff Informationstechnik ist in der Anlage 11.11 „Begriffsbestimmungen“ erläutert.
8 Vergleiche auch Anlage 11.15, (lfdNrn. 10, 14, 20 und 21)
9 Das PDCA-Modell („Plan“ (=Regelungen, Planung und Konzeption), „Do“ (= Umsetzung), „Check“ (= Überwachung), „Act“ (= Optimierung, Verbesserung)) ist Grundlage des IT-Grundschutzes des BSI sowie des ISO-Standards 27001 (siehe Bezug Anlage 11.15 (LfdNr. 38)).

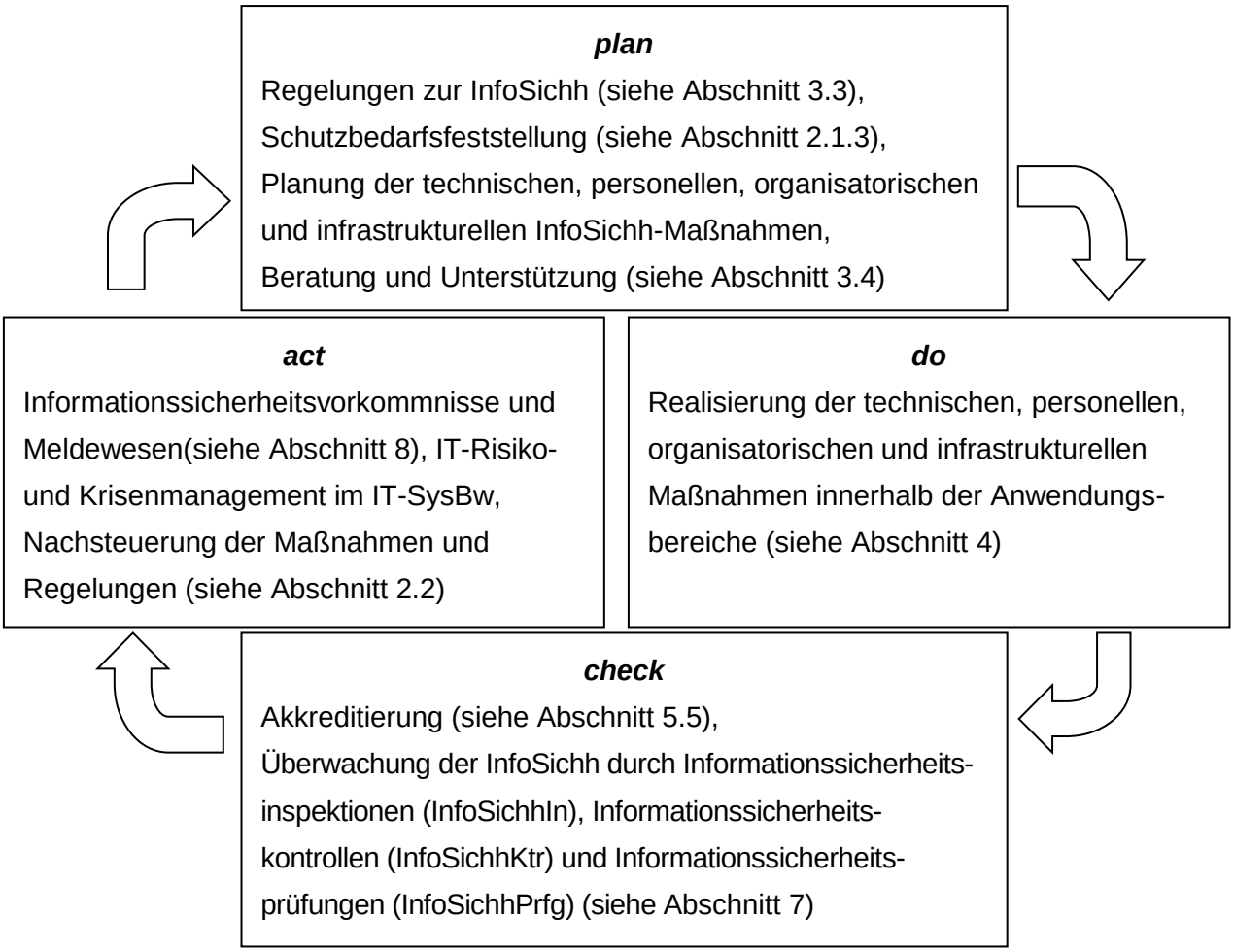

Abb. 1: Informationssicherheitsmanagementprozess der Bundeswehr

110. Schutzobjekte der InfoSichh sind vornehmlich die mit der IT zu verarbeitenden bzw. zu übertragenden Daten und Informationen. Über die Informationen hinaus ist es erforderlich, auch die die Informationen verarbeitende bzw. übertragende IT selbst sowie die Dokumentation zu schützen. Der Schutzbedarf richtet sich nach dem Schaden, der für eine Organisation, Organisationseinheit oder eine natürliche bzw. juristische Person entsteht, wenn ein oder mehrere Grundwerte bzw. Gewährleistungsziele der InfoSichh (siehe Nr. 111 und Nr. 112) beeinträchtigt werden.

1.4.2 Grundwerte der Informationssicherheit

111. Die drei **Grundwerte** der InfoSichh (zur Begriffsbestimmung vgl. Anlage 11.11) sind:

- **Vertraulichkeit (VT)** – Schutz vor unbefugter Informationsgewinnung / -beschaffung,
- **Verfügbarkeit (VF)** – Aufrechterhaltung der zugesicherten Nutzbarkeit von Informationen, IT-Diensten und -Funktionen sowie
- **Integrität (IN)** – Schutz vor unbefugter und unzulässiger Veränderungen von Informationen, IT-Diensten und Eigenschaften von IT sowie Nachweisbarkeit und Beweisbarkeit von IT-gestützten Aktionen.

1.4.3 Gewährleistungsziele der Informationssicherheit

112. Im **Rahmen** der InfoSichh sind – neben den oben definierten Grundwerten – zusätzlich mindestens die folgenden **Gewährleistungsziele** bzgl. ihrer Relevanz zu betrachten (vergleiche Abb. 3). Diese aus dem Datenschutz stammenden Gewährleistungsziele[10] sind **auch** für die anderen Informationskategorien anzuwenden, siehe Abschnitt 2.1.

- **Nichtverkettung (NV)** – Anforderung, dass Informationen nur für den Zweck verarbeitet und ausgewertet werden können, für den sie erhoben wurden und dass eine Verarbeitung nach Zwecken getrennt möglich ist.
- **Transparenz (TR)** – Anforderung, dass in einem unterschiedlichen Maße sowohl Nutzer, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt.
- **Intervenierbarkeit (IV)** – Anforderung, dass den Betroffenen in der Informationstechnik die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt werden können und die verarbeitende Stelle verpflichtet ist, die entsprechenden Maßnahmen umzusetzen. Dazu müssen die für die Verarbeitungsprozesse verantwortlichen Stellen[11] jederzeit in der Lage sein, in die Datenverarbeitung vom Erheben bis zum Löschen der Daten einzugreifen.

Bei Bedarf können weitere Gewährleistungsziele definiert werden. Diese sind dann zu erläutern, in der Informationsstruktur (siehe Abschnitt 2.1) aufzuführen und entsprechend zu bewerten.

1.4.4 Bedrohung, Schwachstelle, Gefährdung, Schaden und (tolerierbares) Risiko

113. Eine **Bedrohung** ist ein Umstand oder Ereignis, der oder das die Grundwerte oder die Gewährleistungsziele der InfoSichh beeinträchtigen kann, wodurch ein Schaden entstehen kann. Beispiele für Bedrohungen sind höhere Gewalt, fahrlässige menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen. Trifft eine Bedrohung auf eine Schwachstelle (insbesondere technische oder organisatorische Mängel), so entsteht eine Gefährdung.

114. Eine **Schwachstelle** ist ein sicherheitsrelevanter Fehler beispielsweise in einem Prozess, in einer Organisation, in einer Regelung, in der IT oder in einer Institution. Ursachen können zum Beispiel

[10] vgl. „Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele“ V.1.0 von November 2016 (Herausgeber: Arbeitskreis Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder)

[11] Siehe A-2122/4 (siehe Bezug Anlage 11.15 (lfdNr. 2))

in der Konzeption, der Unternehmenskultur, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird bzw. die InfoSichh nicht mehr gegeben ist. Eine Schwachstelle entsteht auch immer dann, wenn zu einer möglichen Gefährdung keine hinreichend wirksamen InfoSichh-Maßnahmen existieren oder umgesetzt werden.

115. Eine **Gefährdung** ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt (oder sein Umfeld) einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt mit der Möglichkeit des Eintretens eines Schadens.

116. Ein **Schaden** im Sinne dieser Vorschrift ist der Verlust oder die Minderung von mindestens einem der Grundwerte bzw. eines der Gewährleistungsziele der InfoSichh mit der Folge möglicher negativer Auswirkungen auf das IT-SysBw oder auf Personen (einschließlich eines möglichen Ansehensverlustes in der Öffentlichkeit), auf die Bundeswehr insgesamt, ihre Einsatzbereitschaft oder die Bundesrepublik Deutschland.

117. Ein **Risiko** ist - sofern quantifizierbar bzw. im Sinne der Ausführungen in Anlage 11.4 zuordenbar - die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens. Im Unterschied zu „Gefährdung“ umfasst der Begriff „Risiko“ bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.

118. Risiken sind immer anhand des festgestellten Schutzbedarfs (siehe Abschnitt 2) für Informationen zu bewerten[12] und durch InfoSichh-Maßnahmen auf ein tolerierbares Maß zu reduzieren. Eine Methodik zur Durchführung von Risikoanalysen[13] ist in der Anlage 11.1.10 angegeben. Ob ein Risiko **tolerierbar** ist, liegt in der Entscheidungskompetenz des zuständigen Rollenträgers bzw. der zuständigen Rollenträgerin. In der Vorbereitung dieser Entscheidung wird dieser bzw. diese durch das zuständige Element der Informationssicherheitsorganisation der Bundeswehr beraten (siehe Kapitel 3). Es gibt jedoch Risiken, die sich einer Abwägung der Tolerierbarkeit per se entziehen[14]. Auch bei deren Identifizierung berät die Informationssicherheitsorganisation. Werden im Rahmen der Risikobewertung Risiken als tolerierbar eingestuft, so sind diese zu dokumentieren und immer dann neu zu bewerten, wenn bisher nicht berücksichtigte Gefährdungen auf die betrachtete IT oder ihr Umfeld einwirken, neue Schwachstellen entdeckt werden oder neue InfoSichh-Maßnahmen zur Verfügung stehen. Gesetzesverstöße stellen ein Schaden im Sinne der Nr. 116 dar und sind unabhängig vom Aufwand zu deren Vermeidung im Rahmen dieser Risikobewertung stets nicht tolerierbar.

[12] Eine Risikobewertung ist immer eine Bewertung der Ausnutzbarkeit von bekannten oder möglichen Schwachstellen in der IT unter Berücksichtigung der betrachteten Gefährdungen.
[13] Der IT-Grundschutz des BSI gibt für Risikoanalysen nur einen Rahmen, nicht jedoch konkrete Methodiken vor.
[14] z.B. bei Gefahr für Leib und Leben von Personen.

1.5 Vorgaben und Rahmenbedingungen

1.5.1 Allgemeines

119. Nationale Gesetze und Verordnungen, die die InfoSichh betreffen, sind als verbindliche Vorgaben für die InfoSichh in der Bw in diese Vorschrift eingeflossen.

Die Bw operiert vernetzt mit internationalen Partnern. Zu diesen gehören neben einzelnen Staaten auch internationale Organisationen wie die North Atlantic Treaty Organisation (NATO) oder die Europäische Union (EU). Deutschland hat sich in gegenseitigen Geheimschutzabkommen verpflichtet, die Informationen dieser Partner nach deren Vorgaben (siehe Bezug Anlage 11.15 (lfd. Nrn. 29 bis 36)) zu schützen, wenn sie in nationaler deutscher IT verarbeitet und / oder übertragen werden. Die entsprechenden Referenzdokumente sind in der Anlage 11.15 aufgeführt.

1.5.2 Anwendung des IT-Grundschutzes des BSI in der Bundeswehr

120. Der vom BSI entwickelte IT-Grundschutz ist in allen Bundesbehörden anzuwenden. Er ermöglicht es, durch ein systematisches Vorgehen notwendige InfoSichh-Anforderungen und -Maßnahmen[15] zu identifizieren und umzusetzen. Der IT-Grundschutz basiert auf einer Vorgehensweise, die das BSI als BSI-Standards bereitstellt, einem Katalog von InfoSichh-Anforderungen und -Maßnahmen (zum IT-Grundschutzkatalog der Bw siehe Anlage 11.1.2) und einem Werkzeug (siehe Nr. 124).

121. Die Vorgaben der BSI-Standards werden in der Bw mit dieser Zentralen Dienstvorschrift umgesetzt.

122. Die IT-Grundschutzmethodik, deren Kenntnis für die Erstellung und Prüfung von InfoSichhK notwendig ist, wird für die Bw einschließlich der notwendigen Vorgaben zur Bereitstellung und Pflege eines IT-Grundschutzkataloges der Bw in Anlage 11.1 umgesetzt.

123. Der im IT-Grundschutzkatalog der Bw enthaltene Baustein „Sicherheitsmanagement“ und die damit verbundenen Maßnahmen sind mit dieser Zentralen Dienstvorschrift für die gesamte Bw bereits umgesetzt.

124. Für die Erstellung von InfoSichhK ist das durch die Bw zentral bereitgestellte Werkzeug[16] – unter Berücksichtigung der Übergangsregelung gemäß Abschnitt 1.2 – zu nutzen. Um den Datenaustausch zwischen InfoSichhK innerhalb der Bw sicherstellen und eine einheitliche Ausbildung gewährleisten zu können, ist die Beschaffung bzw. Nutzung alternativer Werkzeuge unzulässig.

---

[15] Anforderungen werden durch eine oder mehrere Maßnahmen erfüllt, Maßnahmen werden umgesetzt (vgl. Nr. 207).

[16] Weitere Informationen zum zentralen Werkzeug werden im Intranetauftritt http://infosichh.bundeswehr.org im Bereich „Fachinformationen / IT-Grundschutz / SAVe“ sowie im Bereich „Fachinformationen / IT-Grundschutz / Bausteine und Metadaten“ bereitgestellt.

125. Die IT-Grundschutzmethodik fordert die Bewertung der mit IT zu verarbeitenden bzw. zu übertragenden Informationen hinsichtlich eines „normalen“, eines „hohen“ oder eines „sehr hohen“ Schutzbedarfes (sog. Schutzbedarfskategorien) in Bezug auf jeden Grundwert der InfoSichh (siehe Nr. 111). Darüber hinaus müssen die Informationen hinsichtlich der Relevanz der Gewährleistungsziele (siehe Nr. 112) bewertet werden. Die diesbezüglich in der Bw anzuwendende Vorgehensweise ist im Abschnitt 2.1.3 beschrieben.

126. Jede den IT-Grundschutz anwendende Institution muss die Bedeutung der Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ für den eigenen Bereich definieren. Für die Bw gelten hierfür die Vorgaben und Hilfestellungen gemäß Anlage 11.4. Für normalen Schutzbedarf befinden sich die Grundsätze und Festlegungen in der Anlage 11.2 dieser Zentralen Dienstvorschrift. In der Anlage 11.3 sind für hohen bzw. sehr hohen Schutzbedarf über die in der Anlage 11.2 genannten Grundsätze und Festlegungen hinaus ergänzende InfoSichh-Anforderungen[17] und -Maßnahmen vorgegeben.

127. Die Fälle, in denen eine Risikoanalyse durchzuführen ist sowie eine konkrete einfache Methodik zur Durchführung von Risikoanalysen im Rahmen der Erstellung von InfoSichhK werden im Abschnitt 6.2 „Risikoanalyse“ und in Anlage 11.1.10 „Ergänzende Sicherheitsanalyse & Risikoanalyse“ dieser Zentralen Dienstvorschrift angegeben.

128. In der Bw werden die Vorgaben zum Notfallmanagement durch Umsetzung der im IT-Grundschutzkatalog der Bw enthaltenen Maßnahmen zur IT-Notfallvorsorge (Maßnahmen der Kategorie 6, z.B. im Baustein „Notfallmanagement“, siehe Anlage 11.1, Nr. 11) erfüllt. Diese sind im Rahmen der Notfallvorsorge der DSt / Liegenschaft durch die jeweils Verantwortlichen gem. A1-250/0-1 „Aufgaben im Standortbereich“ (siehe Bezug 11.16 (lfdNr. 57)) zu berücksichtigen.

129. Als Ergebnis einer grundlegenden Modernisierung hat das BSI im November 2017 drei neue BSI-Standards und im Februar 2018 die erste Edition eines neuen IT-Grundschutzkompendiums[18] veröffentlicht. Die Voraussetzungen für die Nutzung des modernisierten IT-Grundschutzes in der Bw werden schnellstmöglich geschaffen. Dies beinhaltet u.a. die Bereitstellung eines neuen Kataloges mit InfoSichh-Anforderungen und -Maßnahmen[19] sowie einer neuen Version des zentralen Werkzeugs für die Bw, mit der InfoSichhK nach bisherigem und modernisiertem IT-Grundschutz erstellt und überführt werden können. Die Termine gemäß Nr. 102 für die Erstellung bzw. Umstellung von InfoSichhK auf den IT-Grundschutz sind einzuhalten. Daher können diese InfoSichhK mit dem verfügbaren zentralen

[17] Anforderungen werden durch eine oder mehrere Maßnahmen erfüllt, Maßnahmen werden umgesetzt (vgl. Nr. 207).

[18] Dies ist die modernisierte Fassung der bisherigen IT-Grundschutz-Kataloge, die die Basis für den IT-Grundschutzkatalog der Bundeswehr bilden. Veröffentlicht wurde durch das BSI ein erster Teil mit neu geordneten IT-Grundschutzbausteinen, der zunächst nur die wesentlichen bzw. die am häufigsten genutzten Bausteine der 15. Ergänzungslieferung der bisherigen IT-Grundschutz-Kataloge enthält. Die zweite Edition soll im Februar 2019 veröffentlicht werden.

[19] Nach Veröffentlichung der zweiten Edition des IT-Grundschutzkompendiums.

Werkzeug und dem verfügbaren IT-Grundschutzkatalog begonnen bzw. fortgesetzt werden. Abschließende Übergangsfristen für die Umstellung auf den modernisierten IT-Grundschutz in der Bw werden nach Vorliegen der notwendigen Voraussetzungen geregelt.

2 Ermittlung und Deckung des Schutzbedarfs

2.1 Informationsstruktur

2.1.1 Allgemeines

201. Die **Informationsstruktur** ist die Strukturierung der mit der zu beschaffenden oder vorhandenen IT zu verarbeitenden und / oder zu übertragenden Informationen nach **Informationskategorien** (siehe Abschnitt 2.1.2), einschließlich der durch die IT zu protokollierenden Daten, (siehe auch Anlage 11.6) zusammen mit dem jeweiligen **Schutzbedarf** (siehe Abschnitt 2.1.3) der Informationen bezogen auf die drei **Grundwerte** der InfoSichh (siehe Nr. 111) und der Relevanz der **Gewährleistungsziele** (siehe Nr. 112). Hiervon leitet sich gemäß der IT-Grundschutz-Methodik des BSI (siehe Bezug Anlage 11.15 (lfdNr. 46)) der Schutzbedarf für Anwendungen, IT, Infrastruktur und Kommunikationsverbindungen ab. Der Schutzbedarf wird durch die Anforderungen der Schutzbedarfsverantwortlichen bestimmt. Zu den Schutzbedarfsverantwortlichen zählen insbesondere die Vertreter der in Nr. 301 genannten Aufgabenbereiche. In der Bw ist die Informationsstruktur gemäß Abschnitt 11.4 zu dokumentieren.

2.1.2 Informationskategorien

2.1.2.1 Verschlusssachen (VS)

202. Gemäß Zentraler Dienstvorschrift A-1130/2 VS-NfD „Militärische Sicherheit in der Bundeswehr - Verschlusssachen“ (siehe Bezug Anlage 11.15 (lfdNr. 15)) sind **Verschlusssachen** (VS) im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform. VS werden entsprechend ihrer Schutzbedürftigkeit als STRENG GEHEIM, GEHEIM, VS-VERTRAULICH oder VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) sowie vergleichbarer NATO- / EU-Einstufungen bzw. Einstufungen anderer Nationen, sonstiger überstaatlicher Organisationen oder „MISSION“[20] eingestuft. VS können zusätzlich mit Zusatzvermerken (Weitergabe-/ Sperrvermerke) versehen werden. Diese beschränken oder erweitern den Kreis der Personen, der Kenntnis erhalten darf (z.B. KRYPTO-Sicherheit, NDK, Releasable to „…“).

Die Kennzeichnung von VS in der Bw, einschließlich der Kennzeichnung mit Zusatzvermerken, richtet sich dabei nach den Vorgaben der Zentralen Dienstvorschrift A-1130/2 VS-NfD „Militärische Sicherheit in der Bundeswehr - Verschlusssachen“ (siehe Bezug Anlage 11.15 (lfdNr. 15)). Die besonderen Vorgaben für VS der Fernmeldeaufklärung gemäß Zentralerlass B-1100/14 VS-NfD

[20] „*MISSION*“ ist der Platzhalter für eine spätere konkrete Benennung und setzt eine sog. *Security Policy* für den beabsichtigten Einsatz voraus. Insofern ist z.B. MISSION SECRET keine gültige Einstufung, sondern z. B. NATO / ISAF SECRET oder NATO SECRET Releasable to ISAF.

„Sicherheitsbestimmungen für die Fernmeldeaufklärung der Bundeswehr“ (siehe Bezug Anlage 11.15 (lfdNr. 55)) sind zu beachten.

Weiterhin können VS zusätzlich mit „Besonderen Behandlungskennzeichen“ (BesBehKZ, auch als „Special Category (SPECAT)“ bezeichnet) gemäß ACP 127 (siehe Bezug Anlage 11.15 (lfdNr. 37)) oder Zentraler Dienstvorschrift A-961/1 VS-NfD „Kryptosicherheit in der Bundeswehr“ (siehe Bezug Anlage 11.15 (lfdNr. 20)) versehen werden.

2.1.2.2 Personenbezogene Daten (PersDat)

203. Gemäß der Zentralen Dienstvorschrift A-2122/4 „Datenschutz“[21] (siehe Bezug Anlage 11.15 (lfdNr. 10)) sind **Personenbezogene Daten** (PersDat) in PersDat mit geringem Schutzbedarf, PersDat mit mittlerem Schutzbedarf und PersDat mit hohem Schutzbedarf zu unterscheiden[22] und einem Schutzbereich (SB 1 bis SB 3) zuzuordnen. Informationen und Beispiele hierzu sind der Zentralen Dienstvorschrift A-2122/4 und der Anlage 11.4.2.3 zu entnehmen. Die Besonderheiten zum Umgang mit PersDat im Aufgabenbereich des Militärischen Nachrichtenwesens sind in der Zentralen Dienstvorschrift A-1100/8 "Verarbeitung personenbezogener Daten im Militärischen Nachrichtenwesen" (siehe Bezug Anlage 11.15 (lfdNr. 58)) geregelt.

2.1.2.3 Offene Informationen

204. Neben VS und PersDat können gemäß Zentraler Dienstvorschrift A-1130/2 VS-NfD „Militärische Sicherheit in der Bundeswehr - Verschlusssachen“ (siehe Bezug Anlage 11.15 (lfdNr. 15), dort Nr. 606) auch **Offene Informationen** verarbeitet und übertragen werden. Offene Informationen sind nicht eingestufte Informationen, die aus anderen Gründen (nicht Geheimschutz, nicht Datenschutz) der Pflicht zur Verschwiegenheit (Amtsverschwiegenheit) unterliegen. Sie sind hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität zu schützen (siehe Abschnitt 2.1.4) und hinsichtlich der Gewährleistungsziele zu bewerten (siehe Abschnitt 1.4.3).

2.1.2.4 Öffentliche Informationen

205. Informationen, die für die Öffentlichkeit bestimmt sind oder aus öffentlichen Quellen entnommen wurden sowie Daten im Sinne von § 12a Absatz 2 des E-Government-Gesetzes (EGovG), die nach § 12a Absatz 1 in Verbindung mit Absatz 3 EGovG von Behörden der unmittelbaren Bundesverwaltzung bereitzustellen sind, sind **Öffentliche Informationen**. Sie unterliegen nicht der Amtsverschwiegenheit und hinsichtlich der Vertraulichkeit keinen InfoSichh-Anforderungen. Aus

[21] Bis zur Inkraftsetzung der überarbeiten A-2122/4 gilt die Weisung BMVg R I 7 zur A-2122/4 „Datenschutz – Ausführungen zur Europäischen Datenschutzgrundverordnung und dem Bundesdatenschutzgesetz“ vom 25. Mai 2018

[22] Das BDSG verwendet den Begriff „Daten“ anstelle von „Informationen“. Er wird daher in der Verbindung mit PersDat in dieser Zentralen Dienstvorschrift beibehalten.

Gründen des Ansehens in der Öffentlichkeit oder aus rechtlichen Gründen können diese Informationen jedoch Anforderungen an die Verfügbarkeit und / oder Integrität haben.

2.1.2.5 Sonstige schutzbedürftige Informationen

206. Sonstige schutzbedürftige Informationen (SSI) sind solche Informationen, deren Schutzbedarf durch alleinige Zuordnung zu einer der Kategorien öffentlich, offen, VS oder PersDat nicht erreicht werden kann, die aber einen zusätzlichen hinreichenden Schutz erfordern. SSI sind immer hinsichtlich ihres Schutzbedarfes bzgl. der drei Grundwerte und bzgl. der Relevanz der Gewährleistungsziele zu bewerten. Dies kann beispielsweise aus straf-, vergabe- oder vertragsrechtlichen Gründen bei Privat- und Betriebs- oder Geschäftsgeheimnissen der Fall sein[23].

2.1.3 Schutzbedarfsfeststellung

2.1.3.1 Allgemeines

207. Ziel der Schutzbedarfsfeststellung gemäß IT-Grundschutz-Methodik ist es, für die Informationen und davon abhängig für die zu realisierende IT und die dazu gehörigen Anwendungen, Services, Infrastruktur und Kommunikationsverbindungen zu entscheiden, welchen Schutzbedarf sie bezüglich der drei Grundwerte (siehe Nr. 111) Vertraulichkeit, Integrität und Verfügbarkeit besitzen und ob die Gewährleistungsziele (siehe Nr. 112) jeweils relevant sind. Bei allen Grundwerten ist zwischen einem „normalen“, einem „hohen“ und einem „sehr hohen“ Schutzbedarf zu unterscheiden (vgl. Nr. 125). Im Rahmen der Schutzbedarfsfeststellung ist der Schutzbedarf der Informationen sowie der Protokolldaten (vgl. Nr. 201) immer für alle drei Grundwerte zu bewerten. Von dem Schutzbedarf der Informationen und der Relevanz der Gewährleistungsziele leiten sich die zu erfüllenden InfoSichh-Anforderungen und die umzusetzenden InfoSichh-Maßnahmen ab.

2.1.3.2 Vorgehensweise

208. Die Schutzbedarfsfeststellung ist durch die jeweils verantwortlichen Rollenträgerinnen und Rollenträger (siehe Nr. 407, Abb. 9) in fünf Schritten durchzuführen und im InfoSichhK zu dokumentieren. Folgende Schritte sind unter Beachtung des Abschnittes 2.1.4 und der weiteren Hilfestellungen in der Anlage 11.4 erforderlich:

- **Schritt 1:** Festlegung der Informationskategorien einschließlich der Einstufungen für alle verarbeiteten Informationen sowie die Protokolldaten[24].

[23] Weitere Beispiele: Daten aus den Bereichen Compliance Management, Vertrags- und Vergaberecht, Strafrecht, Korruptionsprävention, Soldatenrecht, Beamtenrecht, Arbeitsrecht, Betriebs- und Firmengeheimnisse, Schützenswerte Bereiche bzw. Beschäftigte, Besondere Schutzbedürftigkeit vergaberelevanter Informationen, Persönlichkeitsrecht.

[24] Die im System erfassten Protokolldaten werden nachfolgend immer auch zu den im System verarbeiteten Informationen gezählt. Diese sind grundsätzlich immer mit zu betrachten. Siehe auch Anlage 11.6.

- **Schritt 2:** Bewertung der verarbeiteten Informationen anhand der festgelegten Informationskategorien bzgl. des Schutzbedarfes für alle Grundwerte. Gemäß Grundschutzbaustein Datenschutz ist zunächst die Rechtsgrundlage der Datenverarbeitung von PersDat zu prüfen und entsprechend zu dokumentieren.
- **Schritt 3:** Bei Bedarf Definition und Aufnahme weiterer Gewährleistungsziele.
- **Schritt 4:** Feststellung der Relevanz der Gewährleistungsziele für alle Informationskategorien.
- **Schritt 5:** Zusammenfassung der Schutzbedarfskategorien (siehe Nr. 125) und der Informationskategorien (siehe Nr. 202 ff.) zur Informationsstruktur (siehe Nr. 201). Für die Festlegung des Schutzbedarfes ist die jeweils höchste Schutzbedarfskategorie bzgl. des jeweiligen Grundwertes maßgebend (Maximumprinzip). Hieraus ergeben sich dann gemäß Abschnitt 2.2 die zu erfüllenden Anforderungen und die umzusetzenden Maßnahmen für die Informationskategorien.

209. Die Abb. 2 verdeutlicht die Vorgehensweise insgesamt.

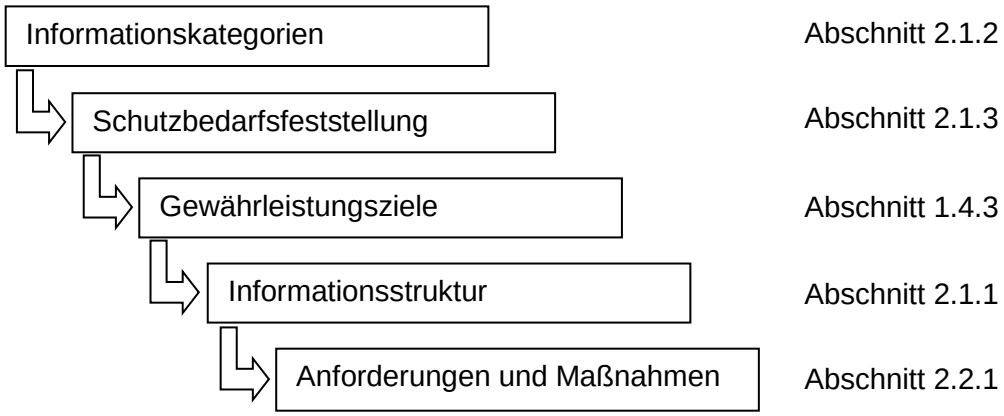

Abb. 2: Vorgehensweise zur Festlegung der Informationsstruktur

2.1.4 Dokumentation

210. In der Bw ist eine Informationsstruktur gem. Abb. 3 aufgebaut. Diese stellt alle Möglichkeiten der Auswahl dar.

Grundwerte / Gewährleistungsziele[25]	**Vertraulich-keit (VT)**			**Verfügbar-keit (VF)**			**Integrität (IN)**			**Nichtverkettung (NV)**	**Transparenz (TR)**	**Intervenierbar-keit (IV)**
Schutzbedarfskategorien[26]	*N*	*H*	*SH*	*N*	*H*	*SH*	*N*	*H*	*SH*			
Informationskategorie / Einstufung										Relevanz (ja / nein) [27]		
Öffentlich	–	–	–	X	X	X	X	X	X	j / n	j / n	j / n
Offen	X	–	–	X	X	X	X	X	X	j / n	j / n	j / n
PersDat SB 1	X	–	–	X	X	X	X	X	X	j / n	j / n	j / n
VS-NfD (ggf. mit BesBehKZ[28], ZV[29])	–	X	–	X	X	X	X	X	X	j / n	j / n	j / n
PersDat SB 2[30]	–	X	–	X	X	X	X	X	X	j / n	j / n	j / n
PersDat SB 3[31]	–	–	X	X	X	X	X	X	X	j / n	j / n	j / n
VS-VERTRAULICH, GEHEIM, STRENG GEHEIM (ggf. mit BesBehKZ, ZV)	–	–	X	–	X	X	–	X	X	j / n	j / n	j / n
Sonstige schutzbedürftige Informationen	X	X	X	X	X	X	X	X	X	j / n	j / n	j / n
Protokolldaten (ohne PersDat)[32]	X	X	X	X	X	X	X	X	X	j / n	j / n	j / n

Abb. 3: Generische Informationsstruktur

Zu beachten ist, dass VS mit sehr hohem Schutzbedarf bezogen auf den Grundwert Vertraulichkeit (Informationen der Geheimhaltungsgrade VS-VERTRAULICH oder höher sowie vergleichbare NATO- / EU-Einstufungen bzw. Einstufungen anderer Nationen, sonstiger überstaatlicher Organisationen

25 In Einzelfällen können Gewährleistungziele in IT auch explizit nur eingeschränkt verfolgt werden, so zum Beispiel im Bereich des Militärischen Nachrichtenwesens (Einschränkung der Intervenierbarkeit) oder zum Schutz der Identität besonders schützenswerter Beschäftigter (Einschränkung der Transparenz). Die Einschränkungen sind jeweils im InfoSichhK zu begründen.

26 N = normal, H = hoch, SH = sehr hoch

27 siehe Nr. 112

28 BesBehKZ = Besonderes Behandlungskennzeichen

29 ZV = Zusatzvermerke

30 Schließt PersDat im Rahmen der Protokollierung und Auditings mit ein.

31 Schließt PersDat im Rahmen der Protokollierung und Auditings mit ein.

32 Bei Protokolldaten handelt es sich nicht um eine Informationskategorie gemäß Abschnitt 2.1.2, sie sind jedoch bei der Informationsstruktur zu berücksichtigen (vergleiche Nr. 201 und Nr. 207).

oder „MISSION“[33]) wegen ihrer Nachweispflicht gemäß Zentraler Dienstvorschrift A-1130/2 VS-NfD „Militärische Sicherheit in der Bundeswehr - Verschlusssachen“ (siehe Bezug Anlage 11.15 (lfdNr. 15)) einen mindestens hohen Schutzbedarf bezogen auf die Grundwerte Verfügbarkeit und Integrität haben.

Ein Beispiel für eine konkrete Informationsstruktur ist mit Anlage 11.4.4 beigefügt.

2.2 Auswahl, Anpassung und Konkretisierung von Informations-sicherheitsmaßnahmen

2.2.1 Allgemeines

211. Jede IT muss zum Schutz der mit ihr zu verarbeitenden und / oder zu übertragenden Informationen in Abhängigkeit von deren Schutzbedarf und der Relevanz der Gewährleistungsziele über geeignete InfoSichh-Maßnahmen verfügen und in einem, den Gefährdungen angemessenen organisatorischen, personellen und infrastrukturellen IT-Umfeld betrieben werden. Durch ein Risikomanagement sind Risiken durch Anwendung von angemessenen Sicherheitsmaßnahmen zu reduzieren sowie die verbleibenden Risiken zu identifizieren, die mit den getroffenen Maßnahmen nicht mitigiert werden können. Eine Maßnahme ist angemessen, wenn der Aufwand zur Umsetzung und das verbleibende Risiko in einem ausgewogenen Verhältnis stehen. Die Bewertung der Angemessenheit erfolgt auf der Grundlage einer Risikoanalyse (siehe Abschnitt 6.2).

212. **Technische InfoSichh-Maßnahmen** müssen so implementiert sein, dass sie grundsätzlich zwangsweise wirken, d. h. nur von autorisiertem Personal (z. B. Administratoren) bzw. in Notfällen geändert bzw. deaktiviert werden können. Sie müssen dem Grundsatz Security-by-Design folgen.

213. Der **IT-Grundschutz des BSI** enthält alle notwendigen InfoSichh-Maßnahmen, die einem normalen Schutzbedarf für alle Grundwerte angemessen sind. Er stellt die Mindestanforderungen an die InfoSichh in der Bw dar und ist für jedes Projekt **grundsätzlich** umzusetzen. Ausnahmen bzgl. der Vertraulichkeit sind bei der Verarbeitung und Übertragung öffentlicher Informationen sowie bei den PersDat SB 1 zulässig. Bei Relevanz der Gewährleistungsziele sind bei Bedarf zusätzliche InfoSichh-Maßnahmen festzulegen.

214. Zur Herstellung der InfoSichh sind daher durch die zuständigen Rollenträgerinnen und Rollenträger (siehe Nr. 407, Abb. 9) die als Ergebnis der Modellierung gemäß IT-Grundschutz jeweils erforderlichen InfoSichh-Maßnahmen nach IT-Grundschutz-Methodik (siehe Anlage 11.1) zu ermitteln und unter Beachtung der Grundsätze gemäß Anlage 11.1 umzusetzen.

215. Ist der Schutzbedarf für mindestens einen Grundwert höher als „normal“ bzw. ist mindestens ein Gewährleistungsziel relevant (vgl. Nr. 207), sind darüber hinaus gemäß Anlage 11.3 zusätzliche

[33] „MISSION“ ist der Platzhalter für eine spätere konkrete Benennung und setzt eine sog. *Security Policy* für den beabsichtigten Einsatz voraus. Insofern ist z.B. MISSION SECRET keine gültige Einstufung, sondern z. B. NATO / ISAF SECRET oder NATO SECRET Releasable to ISAF.

InfoSichh-Anforderungen zu beachten und mit geeigneten InfoSichh-Maßnahmen zu erfüllen bzw. ergänzende InfoSichh-Maßnahmen zu ermitteln und umzusetzen.

216. Die in der Bw anzuwendenden InfoSichh-Maßnahmen werden durch den jeweils aktuellen IT-Grundschutzkatalog der Bw (siehe Anlage 11.1.2) zur Verfügung gestellt und sind unter Berücksichtigung der Grundsätze und Erläuterungen gemäß Anlagen 11.1 bis 11.3 umzusetzen.

217. Die abschließend festgelegten InfoSichh-Maßnahmen, inklusive der gemäß IT-Grundschutz-Methodik vorgesehenen Begründungen, sind im InfoSichhK zu dokumentieren. Die Umsetzung dieser InfoSichh-Maßnahmen ist grundsätzlich verpflichtend. Können InfoSichh-Maßnahmen nicht oder nur zum Teil umgesetzt werden, so ist dies zu begründen, im Rahmen einer Risikoanalyse (siehe Abschnitt 6.2) zu bewerten und in den entsprechenden InfoSichhK zu dokumentieren.

2.2.2 Ermittlung zusätzlicher bzw. alternativer Informationssicherheits-maßnahmen

218. In bestimmten Fällen reichen die im IT-Grundschutzkatalog der Bw (siehe Anlage 11.1.2) zur Herstellung und Gewährleistung der InfoSichh genannten Maßnahmen nicht aus (z. B. nicht vorhandene IT-Grundschutz-Bausteine des BSI für eine spezielle Technologie (Fall 1) oder keine ergänzende InfoSichh-Maßnahme der Bw vorhanden (Fall 2)) bzw. InfoSichh-Maßnahmen sind ggf. nicht anwendbar oder umsetzbar (Fall 3). In diesen Fällen ist wie in der Abb. 4 beschrieben zu verfahren:

Fall	Vorgehen
1. Im Rahmen der Modellierung nach IT-Grundschutz sind keine geeigneten InfoSichh-Maßnahmen des BSI vorhanden (z. B. existiert für eine spezielle Technologie kein geeigneter IT-Grundschutz-Baustein).	Die für die Erstellung von InfoSichhK zuständigen Rollenträgerinnen und Rollenträger (siehe Abschnitt 4) können sich an die jeweils für die Beratung, Prüfung bzw. Mitzeichnung von InfoSichhK zuständigen Rollenträgerinnen und Rollenträger bzw. Stellen wenden. Diese prüfen in Abstimmung mit dem Referat InfoSichh im Kommando Cyber- und Informationsraum (KdoCIR) Abteilung Planung, ob das BSI zeitgerecht geeignete InfoSichh-Maßnahmen oder Bausteine bereitstellen kann. Falls nicht, sind geeignete InfoSichh-Maßnahmen oder Bausteine unter Beachtung der Anlage 11.1.8 zu ermitteln und solange im jeweiligen InfoSichhK zu dokumentieren, bis diese ggf. zentral im IT-Grundschutzkatalog der Bw bereitgestellt werden. Die für die Prüfung bzw. Mitzeichnung von InfoSichhK zuständigen Rollenträgerinnen und Rollenträger bzw. Stellen leiten querschnittlich für die Bw geeignete InfoSichh-Maßnahmen oder Bausteine dem Referat InfoSichh im KdoCIR Abteilung Planung zur Veröffentlichung im IT-Grundschutzkatalog der Bw zu (siehe Anlage 11.1.2 Nr. 5).

Fall	Vorgehen
	KdoCIR prüft fortlaufend in Abstimmung mit dem BSI, ob neue IT-Grundschutz-Bausteine erstellt oder neue InfoSichh-Maßnahmen in bestehende IT-Grundschutz-Bausteine integriert werden sollen und ergreift die notwendigen Maßnahmen zur Bereitstellung im IT-Grundschutzkatalog der Bw ggf. in Abstimmung mit CISOBw. KdoCIR stimmt mit BSI ab, ob diese Bausteine oder InfoSichh-Maßnahmen in den IT-Grundschutz des BSI übernommen oder ausschließlich querschnittlich für die Bw bereitgestellt werden.
2. Es existieren keine ergänzenden InfoSichh-Maßnahmen im IT-Grundschutzkatalog der Bw.	Wenn das Ergebnis der durchzuführenden Risikoanalyse gemäß Abschnitt 6.2 keine Tolerierbarkeit ergibt bzw. die InfoSichh-Maßnahmen aus dem IT-Grundschutzkatalog der Bw nicht ausreichen, sind unter Berücksichtigung der gültigen Vorschriften und Regelungen und in Abstimmung mit den jeweils für die Prüfung bzw. Mitzeichnung von InfoSichhK zuständigen Rollenträgerinnen und Rollenträgern bzw. Stellen geeignete alternative bzw. zusätzliche InfoSichh-Maßnahmen unter Beachtung der Anlage 11.1.8 zu ermitteln. Diese InfoSichh-Maßnahmen sind jeweils einem der Maßnahmenbereiche (Technik, Organisation, Personal, Infrastruktur) zuzuordnen und im jeweiligen InfoSichhK zu dokumentieren. Die für die Prüfung bzw. Mitzeichnung von InfoSichhK zuständigen Rollenträgerinnen und Rollenträger bzw. Stellen leiten querschnittlich für die Bw geeignete InfoSichh-Maßnahmen oder Bausteine dem Referat InfoSichh im KdoCIR Abteilung Planung zur Veröffentlichung im IT-Grundschutzkatalog der Bw zu (siehe Anlage 11.1.2 Nr. 5). KdoCIR prüft, ob diese InfoSichh-Maßnahmen oder Bausteine in den IT-Grundschutzkatalog der Bw oder in Abstimmung mit dem BSI in die IT-Grundschutzkataloge des BSI, ggf. in angepasster Form, übernommen werden.
3. Einzelne InfoSichh-Maßnahmen aus vorhandenen IT-Grundschutz-Bausteinen oder aus dieser Zentralen Dienstvorschrift sind nicht anwendbar oder umsetzbar bzw. die betrachtete IT enthält erkennbare bzw. bekannte Schwachstellen, die das Wirksamwerden einer Gefährdung besonders begünstigen.	

Abb. 4: Festlegung zusätzlicher bzw. alternativer InfoSichh-Maßnahmen

3 Informationssicherheitsorganisation in der Bundeswehr

3.1 Allgemeines

301. Die in diesem Abschnitt beschriebene Informationssicherheitsorganisation im Zusammenwirken mit schutzbedarfsverantwortlichen Organisationselementen (siehe Nr. 101) mit ihren Rollenträgerinnen und Rollenträgern und Aufgaben ist zuständig für den in der Bw umzusetzenden Informationssicherheitsmanagementprozess (siehe Nr. 109, Abb. 1). Zum Schutz der Bw müssen die Bereiche InfoSichh, Datenschutz, Geheimschutz und Militärische Sicherheit eng zusammenarbeiten. Um dem Schutzbedarf für die Bw ganzheitlich gerecht zu werden, sollen in den DSt der Bw die Aufgaben des bzw. der ADSB, des bzw. der Beauftragten für den Geheimschutz und der Militärischen Sicherheit und des bzw. der ISB in einem Organisationselement Sicherheitsmanagement – unter Beibehaltung der zuständigen Fachaufsichten im BMVg[34] – zusammengeführt werden. Dieses Organisationselement Sicherheitsmanagement ist in jeder DSt der Bw als Immediatselement[35] dem bzw. der für InfoSichh (vgl. Abschnitt 4), Datenschutz und Militärische Sicherheit / Geheimschutz jeweils Verantwortlichen[36] unmittelbar[37] zuzuordnen (siehe nachfolgende Abb. 5). Das unmittelbare Vortragsrecht der einzelnen Rollenträgerinnen und Rollenträger in ihrer Fachtätigkeit in diesem Organisationselement bei der Dienststellenleitung bleibt hiervon unberührt.

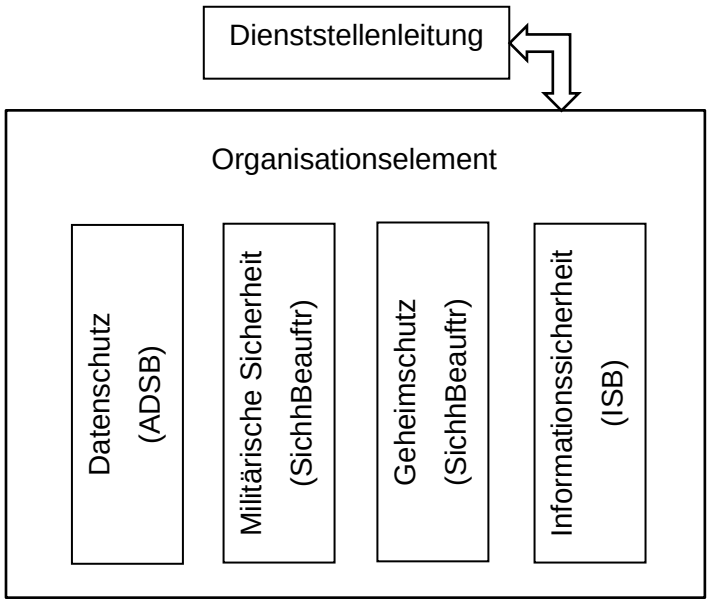

Abb. 5: Organisationselement Sicherheitsmanagement

[34] BMVg R III 4 für den Datenschutz, BMVg SE I 1 für die Militärische Sicherheit, BMVg R III 3 für den personellen Geheimschutz, BMVg CIT II 2 für die Informationssicherheit

[35] Ein Element mit unmittelbarem Zugangs- und Vortragsrecht bei der höchsten verantwortlichen Person.

[36] Die jeweils diese Rollenträgerinnen und Rollenträger bestellenden Personen (für die ISB vgl. Nr. 593), i.d.R. die Dienststellenleitung.

[37] Bedeutet, dass das Organisationselement nicht in der Linie, sondern direkt der Dienstellenleitung zugeordnet wird.

3.2 Zentrale und dezentrale Organisationselemente und Rollen der Bundeswehr, Stellen außerhalb der Bundeswehr und Zuständigkeiten

3.2.1 Allgemeines

302. Der bzw. die **CISO Ressort**[38] ist in allen Angelegenheiten der InfoSichh im gesamten Verteidigungsressort weisungsbefugt, soweit die Fachaufsicht anderer Bereiche nicht tangiert ist. In für die Leitung des BMVg relevanten Angelegenheiten hat er bzw. sie im Rahmen seiner bzw. ihrer fachlichen Zuständigkeit ein unmittelbares Vortragsrecht beim Staatssekretär bzw. bei der Staatsekretärin für Planung, Ausrüstung, Informationstechnik und Nutzung. Seine bzw. ihre Aufgaben sind im Detail im Abschnitt 9.1 beschrieben.

303. Der bzw. die **CISOBw** ist in allen Angelegenheiten der InfoSichh nach Vorgaben des bzw. der CISO Ressort in der gesamten Bw weisungsbefugt[39], soweit die Fachaufsicht anderer Bereiche nicht tangiert ist. Seine bzw. ihre Aufgaben sind detailliert im Abschnitt 9.2 beschrieben.

304. Zur Unterstützung der **Verantwortlichen in den Anwendungsbereichen** der InfoSichh sind ISB gemäß den Festlegungen in den Abschnitten 4 und 5.7 zu bestellen.

305. Das IT-SysBw wird durch **IT-Betriebsführungseinrichtungen** (IT-BtrbFüEinr) und **IT-Betriebseinrichtungen** (IT-BtrbEinr) betrieben. Das **Betriebszentrum IT-System der Bundeswehr** (BtrbZ IT-SysBw) bzw. vergleichbare Einrichtungen[40] und die **Network Operation Center im Einsatz** (NOC i.E.) sind die IT-BtrbFüEinr der Bw.

IT-BtrbEinr sind Organisationselemente von Bundeswehrdienststellen oder vertraglich durch die Bw verpflichtete Unternehmen (z. B. BWI GmbH), welche unmittelbar die Verantwortung für den Betrieb von IT tragen. IT-BtrbEinr umfassen sowohl die IT selbst, die ggf. notwendige Infrastruktur als auch das für den Betrieb der IT verantwortliche IT-Personal.

306. In jeder IT-BtrbFüEinr und jeder IT-BtrbEinr ist ein bzw. eine **ISB Betrieb** (ISBBtrb) für den Betrieb der betreffenden IT-BtrbFüEinr bzw. IT-BtrbEinr zu bestellen[41].

---

[38] Der bzw. die CISO Ressort nimmt im Verteidigungsressort zugleich die Aufgaben des „IT-Sicherheitsbeauftragten Ressort“ gemäß IT-Steuerung des Bundes wahr. Die Rolle des bzw. der Chief Information Security Officer des Verteidigungsressorts (CISO Ressort) wird vom Unterabteilungsleiter bzw. der Unterabteilungsleiterin CIT II wahrgenommen. Er bzw. sie wird vom Referatsleiter bzw. der Referatsleiterin BMVg CIT II 2 vertreten.

[39] Die Rolle des bzw. der Chief Information Security Officers der Bundeswehr (CISOBw) wird von dem Stellvertreter bzw. Stellvertreterin InspCIR wahrgenommen. Er bzw. sie wird durch den Gruppenleiter bzw. die Gruppenleiterin Informationssicherheit in der Abteilung Einsatz im KdoCIR vertreten. Regelungs- und Weisungsbedarf des CISOBw in Angelegenheiten des Datenschutzes und des Geheimschutzes ist über den bzw. die CISO Ressort in den Steuerkreis Informationssicherheit einzubringen.

[40] z.B. der Fleet Entry Point der Marine bzw. vergleichbare Einrichtungen

[41] In IT-BtrbEinr kann der bzw. die ISBBtrb in Personalunion mit dem bzw. der ISB der betreibenden DSt bestellt werden.

307. Wenn IT-Betriebsaufgaben durch **andere Behörden** oder durch von diesen Behörden vertraglich verpflichtete Unternehmen wahrgenommen werden, so sind im Rahmen von zugehörigen Verwaltungsvereinbarungen Regelungen zu treffen, die eine Wahrnehmung der gemäß dieser Zentralen Dienstvorschrift erforderlichen Aufgaben sicherstellen. Bei der Wahrnehmung von IT-Betriebsaufgaben im Rahmen von Einsätzen durch andere Stellen (z. B. Bündnispartner, beauftragte Unternehmen) sind entsprechende Vereinbarungen zu treffen.

308. **Unternehmen**, die Betriebsaufgaben für die Bw übernehmen, sind vertraglich zu verpflichten, gegenüber dem Auftraggeber einen bzw. eine **ISB Auftragnehmer** (ISBAN) zu benennen, der bzw. die in allen Fragen der

- InfoSichh der Ansprechpartner bzw. die Ansprechpartnerin für den bzw. die ISB des Projektes (ISBProj) des Auftraggebers,
- InfoSichhVork an den ISB Projekt wendet,
- betrieblichen Anteile der InfoSichh der Ansprechpartner bzw. die Ansprechpartnerin für den bzw. die ISBBtrb und
- vom IT-Betrieb betroffenen DSt / EinsKtgt bzgl. InfoSichh der Ansprechpartner bzw. die Ansprechpartnerin für die ISB der Dienststelle (ISBDSt) / ISB im Einsatzgebiet (ISB i.E.)

ist.

309. Für die Überwachung von Kryptomitteln der Bw, die im Rahmen von Projekten oder IT-Betrieb und Aufgabenübernahme durch Dritte in der gewerblichen Wirtschaft betrieben werden, ist beim ZCSBw ein bzw. eine **ISB Geheimschutzbetreute Wirtschaft** (ISBGBW) durch den Kommandeur bzw. der Kommandeurin ZCSBw zu bestellen.

310. Konkrete Vorgaben zu den Aufgaben und zur Bestellung der bzw. des ISB sind den Abschnitten 4 und 5.7, die Aufgabenbeschreibungen, Zuständigkeiten und Befugnisse der bzw. des ISB dem Abschnitt 9 zu entnehmen.

3.2.2 Zentrale Organisationselemente und Rollen der Bundeswehr

311. Folgende Organisationselemente (siehe Abb. 6) der Bw haben organisationsbereichs-übergreifende Aufgaben und Befugnisse zur InfoSichh:

Rolle / Organisationselement	**Wesentliche Zuständigkeit (Details siehe Abschnitte 3.3, 3.4 und 3.5)**
Lenkungs- und Kontrollreferat (LuK) für InfoSichh in der Abteilung Cyber / Informations-technik (CIT) im BMVg (CIT II 2)	Vertreten aller ministeriellen Angelegenheiten der InfoSichh inkl. IT-Risikomanagement (IT-RM)[42] und Zuarbeit für den bzw. die CISO Ressort, soweit die Fachaufsicht anderer Bereiche nicht tangiert ist.

[42] BMVg R II 5 ist LuK für Angelegenheiten der InfoSichh des BAMAD.

Rolle / Organisationselement	**Wesentliche Zuständigkeit (Details siehe Abschnitte 3.3, 3.4 und 3.5)**
Fachaufsicht für Datenschutz im BMVg (R III 4)	Vertreten aller ministeriellen Angelegenheiten des Datenschutzes Siehe auch Nr. 301
Fachaufsicht für personellen Geheimschutz im BMVg (R III 3)	Vertreten aller ministeriellen Angelegenheiten des personellen Geheimschutzes Siehe auch Nr. 301
Fachaufsicht für Miltärische Sicherheit im BMVg (SE I 1)	Vertreten aller ministeriellen Angelegenheiten der Militärischen Sicherheit Siehe auch Nr. 301
CISO Ressort im BMVg	siehe Nr. 302
CISOBw im KdoCIR	siehe Nr. 303
Grp DEUmilSAA im ZCSBw	Beraten der Leiter bzw. Leiterinnen der Integrierten Projektteams (Ltr IPT) bzw. der ProjLtr in allen Angelegenheiten der InfoSichh. Beraten der für die Erstellung von InfoSichhKProj zuständigen Rollenträgerinnen und Rollenträgerinnen in allen Projektphasen. Prüfen und Mitzeichnen von InfoSichhKProj und InfoSichhKFW. Akkreditieren von IT.
Abteilung CSOCBw im ZCSBw	Durchführen der zentralen technischen Überwachung der InfoSichh (24/7). Führen der aktuellen bundeswehrgemeinsamen Informationssicherheitslage im Auftrag CISOBw. Zentrale Stelle für die Erfassung, Koordinierung von und Beratung bei Informationssicherheitsvorkommnissen einschließlich deren technische und IT-forensische Bearbeitung.
Abteilung Überprüfung / Unterstützung (Üprfg / Ustg) im ZCSBw	Durchführen technischer Schwachstellenanalysen. Erarbeiten von Vorgaben zu Informationssicherheitsprüfungen (InfoSichhPrfg) und Informationssicherheitsinspektionen (InfoSichhIn) unter Beteiligung der Regionalzentren (RegZ).
Regionalzentren des ZCSBw	Durchführen von InfoSichhIn in allen Anwendungsbereichen (Nr. 402)[43]. Beraten der Dienststellen in ihrem jeweiligen Zuständigkeitsbereich in Angelegenheiten der InfoSichh.

[43] Zu Besonderheiten im Einsatz siehe Nr. 312, Abb. 7, ISBEinsatz und ISBEinsatz SpezKr

Rolle / Organisationselement	**Wesentliche Zuständigkeit (Details siehe Abschnitte 3.3, 3.4 und 3.5)**
National Distribution Agency (NDA Germany) im ZCSBw	Zentrales Kryptomittel- / Schlüsselmanagement für die Bw. COMSEC-Officer NATO gemäß SDIP 293/1 NATO RESTRICTED „Instructions for the control and safeguarding of NATO crypto-material“ (siehe Bezug Anlage 11.15 (lfdNr. 33)).
Abstrahlprüfzentrum der Bundeswehr (APZBw) im ZCSBw	Durchführen von Geräte-, System- und Infrastrukturvermessungen.
Prüfzentrum IT-Sicherheit Bw (PZITSichhBw) in der Wehrtechnischen Dienststelle (WTD) 81 / Geschäftsfeld (GF) 210	Durchführen technischer Prüfungen und Evaluierungen von IT-Produkten, -Geräten und -Systemen.
Militärischer Abschirmdienst (MAD)	Maßnahmen der IT-Abschirmung sowie Beratung von Dienststellen und Projekten in Belangen des materiellen Geheimschutzes.
ISB Geheimschutzbetreute Wirtschaft (ISBGBW) im ZCSBw	Ausüben der Fachaufsicht Krypto / COMSEC gegenüber der geheimschutzbetreuten Wirtschaft in der Bundesrepublik Deutschland für die Unternehmen, die Kryptomittel der Bw einsetzen. Durchführen bzw. Koordinieren von InfoSichhIn, InfoSichhPrfg und Informationssicherheitskontrollen (InfoSichhKtr) bei der geheimschutzbetreuten Wirtschaft.

Abb. 6 Zentrale Organisationselemente und Rollen der Bw zur InfoSichh und wesentliche Zuständigkeiten

3.2.3 Dezentrale Organisationselemente und Rollen der Bundeswehr

312. Folgende Organisationselemente (siehe Abb. 7) der Bw haben organisationsbereichs-, einsatz-, dienststellen-, projekt- und betriebsspezifische Aufgaben und Befugnisse zur InfoSichh:

Rolle / Organisationselement	**Wesentliche Zuständigkeit (Details siehe Abschnitte 3.3, 3.4 und 3.5)**	**Fachliche / organisatorische Zuordnung**
Informationssicherheitsbeauftragte Organisationsbereiche (ISBOrgBer)	Beraten und Unterstützen des bzw. der bestellenden Vorgesetzten in allen Angelegenheiten der InfoSichh inkl. des IT-RM. Führen der organisationsbereichsspezifischen Informationssicherheitslage und IT-Risikolandkarte[44]. Auswerten der Lageinformationen aus der bundeswehrgemeinsamen Informationssicherheitslage hinsichtlich Relevanz für den Organisationsbereich (OrgBer)[45].	OrgBer
Informationssicherheitsbeauftragte BMVg (ISBBMVg) und Militärischer Abschirmdienst (ISBMAD). Diese sind innerhalb dieser Zentralen Dienstvorschrift im Rahmen der InfoSichh den ISBOrgBer gleichgestellt[46].	Beraten und Unterstützen der Bevollmächtigten Vertreterin bzw. Vertreter (BV) ihrer DSt im Integrierten Projektteam (IPT) sowie der Leitung in Angelegenheiten der InfoSichh inkl. des IT-RM. Überwachen der InfoSichh des BMVg bzw. des BAMAD einschließlich MAD-Stellen.	

[44] Risikomatrix mit Kennzahlen. Kann auch über IT-Unterstützung (ITU) realisiert werden.
[45] Der bzw. die ISBSKB berät und unterstützt zusätzlich die dem Generalinspekteur bzw. der Generalinspekteurin der Bundeswehr truppendienstlich unmittelbar unterstellten Dienststellen.
[46] Sofern nicht explizit darauf hingewiesen wird, gelten somit die in dieser Zentralen Dienstvorschrift gemachten Angaben für ISBOrgBer analog für den bzw. die ISBBMVg und den bzw. die ISBMAD.

Rolle / Organisationselement	**Wesentliche Zuständigkeit (Details siehe Abschnitte 3.3, 3.4 und 3.5)**	**Fachliche / organisatorische Zuordnung**
Kryptobereichsleitstellen der Teilstreitkräfte (TSK)	Beraten und Unterstützen der DSt/ EinsKtgt, die Kryptoverfahren nutzen.	
Informationssicherheitsbeauftragter bzw. Informationssicherheits-beauftragte Einsatz (ISBEinsatz)[47]	Beraten des Befehlshabers bzw. der Befehlshaberin EinsFüKdoBw in Angelegenheiten der InfoSichh inkl. des IT-RM. Auswerten der Lageinformationen aus der bundeswehrgemeinsamen Informationssicherheitslage hinsichtlich Relevanz für den Einsatz. Terminliche Planung der InfoSichhIn in den deutschen EinsKtgt in Abstimmung mit Regionalzentrum OST im ZCSBw[48].	Einsatz
Informationssicherheitsbeauftragter bzw. Informationssicherheits-beauftragte Einsatz Spezialkräfte (ISBEinsatzSpezKr)	Durchführung von InfoSichhIn in Einsätzen von SpezKr der Bw im Ausland in Abstimmung mit ZCSBw.	
Informationssicherheitsbeauftragter bzw. Informationssicherheits-beauftragte im Einsatzgebiet (ISB i.E.). Dieser bzw. diese kann ISB des deutschen Einsatzkontingentes (ISB DEU EinsKtgt, zuständig für alle Einsatzstandorte des Einsatzkontingentes) oder ISB am Einsatzstandort (ISB EinsStO, zuständig für einen Einsatzstandort des Einsatzkontingentes) sein	Beraten des Kontingentführers bzw. der Kontingentführerin in Angelegenheiten der InfoSichh inkl. des IT-RM. Überwachen der InfoSichh im EinsKtgt / EinsStO.	

[47] Befh EinsFüKdoBw stellt sicher, dass die Aufgaben gemäß Abschnitt 9.3 dieser Zentralen Dienstvorschrift für alle Kräfte im Einsatz – einschließlich Spezialkräfte (SpezKr) – wahrgenommen werden. Er bestellt dazu neben dem bzw. der ISBEinsatz einen bzw. eine ISBEinsatzSpezKr und regelt deren Aufgabenwahrnehmung, Abgrenzung der Zuständigkeiten und die Zusammenarbeit (einschließlich Berichtswesen an CISOBw). Am Erlass der Regelungen sowie bei Änderungen sind CISO Ressort bzw. CISOBw im Sinne der Nr. 315 dieser Zentralen Dienstvorschrift zu beteiligen. Die Bezeichnung ISB Einsatz beinhaltet, soweit nicht explizit anders aufgeführt, immer ISB Einsatz und ISB Einsatz SpezKr.

[48] Schwerpunkte der InfoSichhIn und Erstellung des Berichtes erfolgen in Federführung Regionalzentrum OST des ZCSBw in Abstimmung mit ISBEinsatz.

Informationssicherheitsbeauftragter bzw. Informationssicherheits-beauftragte Dienststelle (ISBDSt)	Beraten des bzw. der DStLtr in allen Angelegenheiten der InfoSichh inkl. des IT-RM. Überwachen der InfoSichh in Dienststellen / bei Übungen	Dienststelle
Informationssicherheitsbeauftragter bzw. Informationssicherheits-beauftragte Übung (ISBÜb)		
CISO Rüstung	Beraten der Leitung des BAAINBw und aller Ltr IPT / ProjLtr im OrgBer AIN in allen projekt- / programmbezogenen Fragen zur InfoSichh inkl. des IT-RM. Führen der Gesamtlage InfoSichh in Projekten des BAAINBw als Lagebeitrag ZCSBw / CISOBw.	Projekt / Vorhaben
CISO Infrastruktur	Beraten der Leitung des BAIUDBw, aller Infrastruktur-referate im BAIUDBw einschließlich der KompZ BauMgmt und der DSt mit Infrastruktur / Bauaufgaben in allen Fragen zur InfoSichh inkl. des IT-RM mit Bezug zu IT in / aus Infrastrukturprojekten. Führen der Gesamtlage InfoSichh in Vorhaben des BAIUDBw als Lagebeitrag ZCSBw / CISOBw.	
Informationssicherheitsbeauftragter bzw. Informationssicherheits-beauftragte Projekt (ISBProj)	Beraten des bzw. der Ltr IPT / ProjLtr in allen Angelegenheiten der InfoSichh inkl. des IT-RM.	
Informationssicherheitsbeauftragter bzw. Informationssicherheits-beauftragte Forschung und Wissenschaft (ISBFW)	Beraten des bzw. der Ltr des entsprechenden Vorhabens in allen Angelegenheiten der InfoSichh inkl. des IT-RM.	
Informationssicherheitsbeauftragter bzw. Informationssicherheits-beauftragte Auftragnehmer (ISBAN)	Ansprechpartner bzw. Ansprech-partnerin des Auftragnehmers für die Bw in Angelegenheiten der InfoSichh inkl. des IT-RM.	

ISB IT-Betriebsführungseinrichtung bzw. IT-Betriebseinrichtung (ISBBtrb)	Überwachen der Umsetzung von technischen Vorgaben der InfoSichh inkl. des IT-RM im Zuständigkeitsbereich. Zusammenarbeiten mit dem ISBEinsatz und den ISBProj seines bzw. ihres Zuständigkeitsbereiches.	Betrieb

Abb. 7: Dezentrale Organisationselemente und Rollen der Bw zur InfoSichh, wesentliche Zuständigkeiten und fachliche Zuordnung

313. ISBOrgBer, ISBBMVg, ISBMAD, ISBDSt, ISBEinsatz und ISB i.E. sind im Rahmen der ihnen übertragenen Aufgaben anordnungs- / weisungsbefugt gegenüber allen Soldaten bzw. Soldatinnen, Beamten bzw. Beamtinnen und Arbeitnehmern bzw. Arbeitnehmerinnen in ihrem jeweiligen Zuständigkeitsbereich. Fachliche Weisungsrechte anderer Schutzbedarfsverantwortlicher gem. Nr. 301 bleiben hierdurch unberührt. Der bzw. die ISB in militärischen Dienststellen und den Einsatzgebieten sind in ihrem jeweiligen Zuständigkeitsbereich Vorgesetzte aller Soldatinnen und Soldaten gemäß § 3 VorgV (siehe Bezug Anlage 11.15 (lfdNr. 8)).

CISO Rüstung und CISO Infrastruktur haben ein fachliches Weisungsrecht gegenüber allen Rollenträgerinnen und Rollenträgerinnen, die Aufgaben der InfoSichh in Projekten oder in Infrastrukturvorhaben wahrnehmen.

3.2.4 Externe Stellen

314. Folgende für die Bw relevante externe Stellen haben Einfluss auf die Regelung und Herstellung der InfoSichh in der Bw:

- Nationale Sicherheitsbehörde (National Security Authority, NSA) beim Bundesministerium des Inneren (BMI)[49],
- Beauftragter bzw. Beauftragte für den Datenschutz und die Informationsfreiheit (BfDI),
- Cyber-Sicherheitsrat,
- Rat der IT-Beauftragten der Ressorts (IT-Rat),
- das für den Geheimschutz in der Wirtschaft zuständige Organisationselement im Bundesministerium für Wirtschaft und Energie (BMWi),
- Nationale Kommunikationssicherheitsbehörde (National Communication Security Authority, NCSA) beim Bundesamt für Sicherheit in der Informationstechnik (BSI),
- National Cyber Defence Authority (NCDA) beim BSI,

[49] Repräsentiert durch die Abteilung Öffentliche Sicherheit (ÖS)

- NATO Military Committee (NAMILCOM) mit der Military Committee Communication and Information Systems Security and Evaluation Agency (SECAN),
- NATO Security Committee (NSC), NATO C3 Board - Capability Panel 4 - Information Assurance and Cyber Defence (C3B – CaP / 4 - IACD),
- NATO Cyber Defence Management Board (CDMB) mit der NATO Computer Incident Response Capability (NCIRC),
- EU Council Security Committee (CSC) beim EU-Rat und
- EU Council Security Committee on INFOSEC (CSCI) mit dem General Secretariat of the Council (GSC) INFOSEC Office.

3.3 Regelungskompetenzen zur Informationssicherheit

315. Die für Vorgaben und Hinweise zuständigen Organisationselemente, deren Regelungsbefugnisse sowie ergänzende Bestimmungen bzgl. zu beteiligender Stellen sind der folgenden Tabelle zu entnehmen.

Vorgaben und Hinweise **Zuständige OrgElemente** Federführung (FF) Billigung (Bl) Mitzeichnung (Mz) Beteiligung[50] (Bt)	**Zentrale Vorgaben und Hinweise zur InfoSichh**	**Dezentrale Vorgaben und Hinweise zur Infosichh**
BMVg CIT II 2 (FF) CISO Ressort (Bl) CISOBw (Bt) ISBOrgBer (Bt) ISBEinsatz (Bt)	Organisationsbereichsüber-greifende Weisungen / Regelungen[51] und Erlasse[52]	---

[50] Information vor Herausgabe
[51] Bzgl. der Regelungsarten wird auf die A-550/1 verwiesen. Die zweite nachgeordnete Ebene gemäß A-550/1 ist nicht befugt, eigenständig Regelungen zur Informationssicherheit zu erlassen.
[52] Alle anderen zentralen und dezentralen Vorgaben und Hinweise müssen diese organsisationsbereichs-übergreifenden Vorgaben berücksichtigen.

Vorgaben und Hinweise **Zuständige OrgElemente** Federführung (FF) Billigung (Bl) Mitzeichnung (Mz) Beteiligung[50] (Bt)	**Zentrale Vorgaben und Hinweise zur InfoSichh**	**Dezentrale Vorgaben und Hinweise zur Infosichh**
CISOBw (FF) BMVg CIT II 2 (Mz)[53] ISBOrgBer (Bt) ISBEinsatz (Bt) ISB BtrbFüEinr (Bt)	Organisationsbereichsüber-greifende Regelungen / Weisungen / technische Vorgaben / Ausnahme-regelungen / Warnhinweise	---
CISO Rüstung (FF) CISOBw (Mz) ISBProj (Bt)	---	Projektspezifische Vorgaben / Weisungen / Regelungen im Zuständigkeitsbereich
CISO Infrastruktur (FF) CISOBw (Mz)	---	Infrastrukturvorhabenspezifische Vorgaben / Weisungen / Regelungen im Zuständigkeitsbereich
CSOCBw (FF) CISOBw (Bt)	Warnhinweise, Advisories, Kurzlagen	---
ISBOrgBer (FF) CISOBw (Mz)	---	Organisationsbereichsspezifische Vorgaben / Weisungen / Regelungen, Hinweise und Handlungsanweisungen im jeweiligen Zuständigkeitsbereich
ISBEinsatz (FF) EinsFüKdoBw (Bl) CISOBw (Mz) betroffene ISBBtrb(Fü)Einr (Bt) betroffene ISBOrgBer (Bt)	---	Einsatzspezifische Weisungen / Regelungen

[53] Dies gilt nur für organisationsbereichsübergreifende Regelungen / Weisungen.

Vorgaben und Hinweise / **Zuständige OrgElemente** Federführung (FF) Billigung (Bl) Mitzeichnung (Mz) Beteiligung[50] (Bt)	**Zentrale Vorgaben und Hinweise zur InfoSichh**	**Dezentrale Vorgaben und Hinweise zur Infosichh**
ISBDSt (FF) DStLtr (Bl)	---	Vorgaben, Hinweise und Handlungsanweisungen im jeweiligen Zuständigkeitsbereich
ISB i.E. (FF) KtgtFhr / Kdr EinsStO (Bl) ISBEinsatz (Bt)		
ISBProj (FF) Ltr IPT / ProjLtr (Bl)		
ISBFW (FF) Ltr des entsprechenden Vorhabens		
ISBÜb (FF) Übungsleitende bzw. -leitender (Bl)		
Zuständiger ISBBtrb (FF) CISOBw (BI) ISBEinsatz (Mz bei Betroffenheit) betroffene ISBOrgBer (Bt) betroffene ISBProj (Bt)		

Abb. 8: Zusammenhang der Regelungen und Hinweise

316. Vorgaben und Hinweise sollen bei längerfristigem Fortbestehen des Anlasses über ein Jahr hinaus aktualisiert oder in mittel- bis langfristige Regelungen nach den Vorgaben der Zentralen Dienstvorschrift A-550/1 (siehe Bezug Anlage 11.15 (lfdNr. 60)) überführt werden.

317. Dezentrale Vorgaben und Hinweise müssen sich immer auf zentrale Vorgaben und Hinweise beziehen sowie diese konkretisieren bzw. präzisieren und sind durch die in der Abb. 8 aufgeführten Organisationselemente herauszugegeben. Einsatzspezifische Regelungen sind nur dann zu erstellen, wenn spezielle Umstände nur den Einsatz betreffen und diese speziellen Umstände durch vorhandene zentrale Vorgaben und Hinweise nicht hinreichend abgedeckt sind. Dezentrale Vorgaben und Hinweise

dürfen den vorhandenen zentralen Vorgaben und Hinweisen nicht widersprechen, können jedoch kurzfristig zu schaffende Übergangsregelungen berücksichtigen.

318. Die gemäß Abb. 8 durch CISOBw zu erstellenden Weisungen zur InfoSichh sind anlassbezogen als „Weisungen zur Informationssicherheit für die Bundeswehr“ jahresbezogen durchzunummerieren (z.B. Weisung zur InfoSichh in der Bw Nr. 01/2018). Diese Weisungen haben eine aus zeitlichere Sicht kurzfristigen Regelungscharakter, mit denen auf aktuelle Bedrohungen der InfoSichh mit dringlichem Regelungsbedarf bzw. sich schnell ändernde Sachverhalte zur InfoSichh unverzüglich reagiert werden kann. Sie werden durch CISOBw jährlich dahingehend überprüft, ob der Anlass für eine Weisung fortbesteht. Ggf. sind sie zu aktualisieren oder in eine bestehende Regelung gemäß der Zentralen Dienstvorschrift A-550/1 zu überführen. Alle aktuell gültigen Weisungen zur InfoSichh werden im Intranetauftritt http://infosichh.bundeswehr.org im Bereich „Fachinformationen / InfoSichhWsg“ bereitgestellt.

319. **Warnhinweise** des CSOCBw enthalten Informationen über Umstände, welche sich möglicherweise zu einem Informationssicherheitsvorkommnis entwickeln können und empfehlen bei Bedarf präventive Maßnahmen. **Advisories** des CSOCBw enthalten Informationen über bestehende Sicherheitslücken in Soft- und Hardware und empfehlen ein Vorgehen zum Reduzieren des Risikos oder Schließen der Sicherheitslücke.

320. Regelungen zur InfoSichh haben Gültigkeit in allen Anwendungsbereichen gemäß Abschnitt 4 dieser Zentralen Dienstvorschrift.

321. Bei IT-Betrieb und Aufgabenübernahme durch Dritte gelten die Bestimmungen gemäß Abschnitt 4.4.

3.4 Beratung und Unterstützung zur Informationssicherheit

322. Die DEUmilSAA

- berät die Verantwortlichen für InfoSichh in den Anwendungsbereichen F, W, P und V (siehe Nr. 402) in allen Angelegenheiten der InfoSichh und der IT-Risikominimierung,
- berät die für die Erstellung von InfoSichhKProj zuständigen Rollenträgerinnen und Rollenträger in allen Projektphasen,
- berät die für die Erstellung von InfoSichhKFW zuständigen Rollenträgerinnen und Rollenträger,
- akkreditiert IT vor Nutzungsbeginn gemäß Abschnitt 5.5 und
- zeichnet InfoSichhKProj (einschl. InfoSichhK für IT aus Infrastruktur- / Baumaßnahmen gemäß Abschnitt 4.5) bzw. InfoSichhKFW gemäß Abschnitt 6.3.6 und InfoSichhBef gemäß Nr. 645 mit.

323. Die ISBOrgBer unterstützen alle Verantwortlichen ihres OrgBer bei der Erstellung / Fortschreibung von dienststellen- / einsatzbezogenen InfoSichhK (InfoSichhKDSt), InfoSichhKFW und InfoSichh-Befehlen (InfoSichhBef).

324. Der bzw. die CISO Rüstung im BAAINBw berät die Leitung des BAAINBw und alle ProjLtr im OrgBer AIN in allen projekt- / programmbezogenen[54] Fragen zur InfoSichh inkl. des IT-RM.

325. Der bzw. die CISO Infrastruktur im BAIUDBw berät die Leitung des BAIUDBw und alle Verantwortlichen für Infra-Maßnahmen (siehe Nr. 435) in allen Fragen zur InfoSichh inkl. des IT-RM mit Bezug auf IT gemäß Abschnitt 4.5.

326. Die Regionalzentren des ZCSBw beraten alle DSt der Bw bei der Erstellung / Fortschreibung von InfoSichhKDSt sowie in allen weiteren Angelegenheiten der InfoSichh inkl. des IT-RM.

327. Das CSOCBw berät und unterstützt alle Dienststellen im GB BMVg sowie ISB, Personal aus dem IT-Betrieb und ausnahmsweise IT-Nutzer bzw. IT-Nutzerinnen oder Vertragspartner der Bw auf Anfrage fachlich bei der Erkennung, Bewertung und Meldung eines (möglichen) InfoSichhVork sowie ISB in allen weiteren Phasen der Behandlung von InfoSichhVork. Details hierzu sind im Abschnitt 8 geregelt.

328. Das APZBw berät die Projekt- und Dienststellenleitungen hinsichtlich der Umsetzung der Zentralen Dienstvorschrift A-962/1 VS-NfD „Abstrahlsicherheit“ (siehe Bezug Anlage 11.15 (lfdNr. 21)). Darüber hinaus sind durch das APZBw Infrastrukturvermessungen (Zonenvermessungen) und Vermessungen von IT durchzuführen.

329. Die NDA Germany und die Kryptobereichsleitstellen (KBL) der TSK beraten und unterstützen die Kryptomittel nutzenden DSt / EinsKtgt bei der Behandlung und beim Einsatz von Kryptomitteln auf Basis der Zentralen Dienstvorschrift A-961/1 VS-NfD „Kryptosicherheit in der Bundeswehr“, (siehe Bezug Anlage 11.15 (lfdNr. 20)) und verteilen nationale und internationale Kryptomittel. Weiterhin nimmt die NDA Germany die Aufgaben des COMSEC-Officer NATO gemäß SDIP 293/1 NATO RESTRICTED „Instructions for the control and safeguarding of NATO cryptomaterial“ (siehe Bezug Anlage 11.15 (lfdNr. 33)) wahr.

330. Das PZITSichhBw bzw. sonstige durch das BSI anerkannte und von der Bw beauftragte Prüfstellen evaluieren gemäß Abschnitt 5.1 IT und sprechen Zertifizierungs-, Zulassungs- bzw. Freigabeempfehlungen aus. Beratungs- und Prüfleistungen mit dem Ziel einer Zertifizierung (siehe Abschnitt 5.2), Zulassung (siehe Abschnitt 5.3) bzw. Anerkennung (siehe Abschnitt 5.4) von IT sind beim PZITSichhBw oder bei anerkannten Prüfstellen über die DEUmilSAA zu beantragen.

331. Im Rahmen des Materiellen Geheim- und Sabotageschutzes ist eine Beteiligung des MAD notwendig. Darüber hinaus berät der MAD auch bei allen anderen Fachfragen zu materiellen Absicherungsmaßnahmen. Eine Beratung durch das BAMAD ist durch die zuständigen Rollenträgerinnen und Rollenträger (Ltr IPT / ProjLtr, BAAINBw, DStLtr, Kontingentführer bzw. Kontigentführerin gemäß Nr. 407) für Projekte beim BAMAD und in allen anderen Fällen bei der regional zuständigen MAD-Stelle zu beantragen. Bei identifizierten Erkenntnissen und

[54] einschl. komplexe Dienstleistungen

Problemlösungen mit allgemeiner Bedeutung für die Projektrealisierung informiert das BAMAD den CISO Rüstung sowie den CISO Infrastruktur.

332. Zur Lösung von Grundsatzproblemen der InfoSichh, z. B. bei der Verarbeitung oder Übertragung von Informationen der Geheimhaltungsgrade VS-VERTRAULICH oder höher sowie vergleichbarer NATO- / EU-Einstufungen bzw. Einstufungen anderer Nationen, sonstiger überstaatlicher Organisationen oder „MISSION“[55], kann eine Beratung durch den MAD (ggf. im Benehmen mit dem BSI) erforderlich werden. Anträge hierzu sind durch den zuständigen Sicherheitsbeauftragten (SichhBeauftr) auf dem Dienstweg über den zuständigen bzw. die zuständige ISBOrgBer / ISBEinsatz / zuständigen ISBBtrb an den MAD[56] zu richten.

3.5 Überwachung der Informationssicherheit

3.5.1 Allgemeines

333. Die Überwachung dient der Aufrechterhaltung der InfoSichh und der Lagefeststellung zur InfoSichh in der durch die Bw genutzten und betriebenen IT. Sie besteht aus zentralen und dezentralen Anteilen. Die zentralen Anteile sind im Abschnitt 3.5.2, die dezentralen Anteile in den Abschnitten 3.5.3 und 7 beschrieben.

334. Die Lage der InfoSichh ist Teil der Lage IT und der Gesamtlage Cyber- und Informationsraum (CIR), die sich aus den Erkenntnissen von zentral und dezentral durchgeführten Überwachungsmaßnahmen zur InfoSichh sowie aus betriebsbezogenen Überwachungsmaßnahmen (Systemauditing, siehe Anlage 11.6.2.2) ergibt.

335. Alle während der Nutzung von IT relevanten Erkenntnisse aus den zentral und dezentral durchgeführten Überwachungsmaßnahmen sind dem bzw. der CSOCBw zu melden. Rollenträgerinnen und Rollenträger melden relevante Erkenntnisse zur InfoSichh von möglicher politischer oder organisationsbereichs- / einsatzübergreifender Bedeutung unverzüglich dem CSOCBw (E-Mail-Adresse CSOCBw@bundeswehr.org) unter nachrichtlicher Beteiligung des bzw. der CISOBw (E-Mail-Adresse CISOBw@bundeswehr.org) und CISO Ressort (E-Mail-Adresse BMVgCISORessort@bmvg.bund.de).

[55] „*MISSION*“ ist der Platzhalter für eine spätere konkrete Benennung und setzt eine sog. *Security Policy* für den beabsichtigten Einsatz voraus. Insofern ist z.B. MISSION SECRET keine gültige Einstufung, sondern z. B. NATO / ISAF SECRET oder NATO SECRET Releasable to ISAF.

[56] MADAmtEingang@bundeswehr.org (Kopie: KdoCIRFaeEntw-InfoSichh@bundeswehr.org)

3.5.2 Zentrale Überwachung der Informationssicherheit

3.5.2.1 Chief Information Security Officer Ressort und Chief Information Security Officer der Bundeswehr

336. Aufgrund der Weisungsbefugnis des bzw. der CISO Ressort (vgl. Nr. 302) und des bzw. der CISOBw (vgl. Nr. 303) können diese anlassbezogen InfoSichhIn (siehe Abschnitt 7.2) in allen Anwendungsbereichen gemäß Abschnitt 4.1 dieser Zentralen Dienstvorschrift durchführen (Inspektionsbefugnis) oder anordnen (Anordnungsbefugnis). Die Inspektionsbefugnis kann auch ohne Ankündigung ausgeübt werden. Sind bei der Inspektion personenbezogene Daten betroffen, sind die zuständigen ADSB zwingend in die Inspektion einzubeziehen. Der bzw. die CISOBw überwacht die InfoSichh in der Bw und bewertet die aktuelle Lage zur InfoSichh inkl. des IT-RM. Der bzw. die CISO Ressort verantwortet die Rolle des IT-Risikomanagers bzw. der IT-Risikomanagerin für das Ressort und der bzw. die CISOBw für die Bundeswehr.

3.5.2.2 Militärischer Abschirmdienst

337. Der MAD[57] ist unverzüglich über den bzw. die SichhBeauftr einzuschalten, wenn ein Hinweis auf extremistische / terroristische Bestrebungen oder sicherheitsgefährdende oder geheimdienstliche Tätigkeiten vorliegt (zum weiteren Vorgehen bei InfoSichhVork siehe Abschnitt 8.6).

3.5.2.3 Zentrum für Cyber-Sicherheit der Bundeswehr

338. Das ZCSBw

- unterstützt den bzw. die CISOBw bei der Durchführung anlassbezogener Überwachungsmaßnahmen,
- ist mit dem CSOCBw zuständig für die zentrale technische Überwachung der InfoSichh (siehe Nr. 342),
- ist mit dem CSOCBw zuständig für die technische Erfassung und das Führen der bundeswehrgemeinsamen Informationssicherheitslage (siehe Nr. 342),
- identifiziert (systemische) IT-Risiken als Beitrag zur Risikolandkarte,
- erarbeitet in der Abteilung Üprfg / Ustg den zentralen Prüfkatalog für InfoSichhIn auf Basis des IT-Grundschutzkataloges der Bw,
- führt mit den Regionalzentren InfoSichhIn (einschließlich der jährlichen Überprüfungen der Kryptoverwaltungen) in allen Anwendungsbereichen dieser Zentralen Dienstvorschrift durch (siehe Nr. 340),
- führt durch bzw. koordiniert mit dem bzw. der ISBGBW in der NDA Germany InfoSichhIn, InfoSichhPrfg und InfoSichhKtr bei der geheimschutzbereuten Wirtschaft und übt mit dem bzw. der

[57] Meldungen können unmittelbar an das BAMAD aber auch an die regionale MAD-Stellen erfolgen.

ISBGBW die Fachaufsicht Krypto / COMSEC gegenüber der geheimschutzbereuten Wirtschaft aus (siehe Nr. 346),

- führt mit der Prüforganisation des ZCSBw (die Incident Response Teams im CSOCBw, alle Regionalzentren (vgl. Nr. 340) und alle Schwachstellenanalyse-Teams) anlassbezogen InfoSichhPrfg in allen Anwendungsbereichen dieser Zentralen Dienstvorschrift durch[58],
- führt mit der Abteilung Üprfg / Ustg und den Regionalzentren technische Schwachstellenanalysen[59] (z.B. im Rahmen von Akkreditierungen gemäß Abschnitt 5.5) durch,
- führt mit dem CSOCBw und dem Regionalzentrum NORD auf Anforderung IT-forensische Untersuchungen (vgl. Nrn. 343 - 345) durch und
- führt mit den Penetration Test Teams in der Abteilung Üprfg / Ustg ggf. unter Beteiligung der RedTeams des Zentrums für Cyberoperationen (ZCO) erweiterte Überprüfungen der InfoSichh in allen DSt / EinsKtgt / EinsStO der Bw durch.

339. Technische Schwachstellenanalysen im Einsatz sind mit dem ISBEinsatz zu koordinieren. In besonders dringenden Fällen, z. B. bei identifizierten hohen Sicherheitsrisiken, kann der ISBEinsatz eine technische Schwachstellenanalyse unmittelbar bei ZCSBw unter nachrichtlicher Beteiligung CISOBw beantragen.

340. Die Inspektionsteams in den **Regionalzentren des ZCSBw** führen

- regelmäßig InfoSichhIn (siehe Abschnitt 7.2) in allen Anwendungsbereichen[60] gemäß Abschnitt 4.1 dieser Zentralen Dienstvorschrift sowie
- anlassbezogen InfoSichhPrfg (siehe Abschnitt 7.4) in allen DSt der Bw im In- und Ausland sowie im Einsatz[61]

durch (Ausnahmen siehe Nr. 349). Sind bei der Inspektion personenbezogene Daten betroffen, sind die zuständigen ADSB zwingend in die Inspektion einzubeziehen.

341. Die Prüforganisation des ZCSBw (vgl. Nr. 338) hat zur Umsetzung ihrer Zuständigkeiten im Rahmen von InfoSichhIn und InfoSichhPrfg eine fachliche Weisungsbefugnis[62] gegenüber den beteiligten Stellen in der Bw.

342. Das **CSOCBw** führt für den bzw. die CISOBw die bundeswehrgemeinsame Informationssicherheitslage. Zu deren technischer Erfassung baut CSOCBw ein Netzwerk unterschiedlicher Sensoren auf, um InfoSichh relevante Ereignisse zu detektieren und sowohl reaktive als auch präventive Gegenmaßnahmen ergreifen zu können. Weiterhin betreibt CSOCBw ein zentrales Security Information and Event Management System (SIEM) als ein zentrales Lagesystem. Das

58 Im Einsatz zusammen mit ISBEinsatz (vgl. Nr. 340).
59 Nicht für IT-Anteile des IT-SysBw, die sich in der Betriebsverantwortung der BWI befinden.
60 Mit Ausnahme von InfoSichhIn von SpezKr der Bw im Ausland (siehe Nr. 312).
61 Zusammen mit ISBEinsatz gemäß Nr. 312.
62 Davon unberührt bleibt die letzendliche Verantwortung und abschließende Weisungsbefugnis des bzw. der DStLtr gem. Nr. 447

CSOCBw gewährleistet mit dem Lage- und Überwachungszentrum (LÜZ) eine 24h / 7-Tage-Überwachung. Die technische Überwachung muss die zentralen Dienste und Anwendungen[63] der Bw und zentrale Komponenten der InfoSichh[64] mit einbeziehen. Betroffene Dienste und Anwendungen sind durch die Betriebsverantwortlichen nach Vorgaben des CSOCBw so zu konfigurieren, dass eine weitgehend automatisierte Erfassung der nötigen Protokollinformationen durch das zentrale Lagesystem ermöglicht wird. Das InfoSichh-Personal oder Überwachungseinrichtungen von Auftragnehmern (z. B. ISBAN, CERT eines vertraglich für IT-Betriebsaufgaben verpflichteten Unternehmens) sind über eine vertraglich festzulegende Kooperation mit dem CSOCBw in die Überwachung einzubeziehen.

343. Das **CSOCBw** ist die zentrale Stelle für die Erfassung und Koordinierung von InfoSichhVork im GB BMVg (siehe Abschnitt 8) und veranlasst evtl. notwendige Maßnahmen zum Schutz des IT-SysBw, zur Beweissicherung und ggf. zur IT-Notfall- / Krisenbewältigung.

344. Das **CSOCBw** stellt IT-forensische Fähigkeiten zur Verfügung[65], um während und in der Aufarbeitung / Bewertung von InfoSichhVork (siehe Abschnitt 8) schnell und effizient auf forensischen Ergebnissen aufbauende reaktive und präventive Gegenmaßnahmen ergreifen zu können (z. B. Anpassen zentraler Filter, der dynamische Einsatz von Sensoren und das zeitliche Einschränken / Deaktivieren von zentralen Diensten und / oder Sicherheitskomponenten). Bei erwarteten Einschränkungen des Betriebes oder Einsatzes von IT der Bw sind die Prozesse der A-960/15 „IT-Krisenmanagement in der Bundeswehr“ (siehe Bezug Anlage 11.15 (lfdNr. 47)) durchzuführen. Weiterhin stehen diese IT-forensischen Fähigkeiten auf Anforderung für die Unterstützung von disziplinaren und strafrechtlichen Ermittlungen zur Verfügung. Näheres dazu regelt die A-960/5 (siehe Bezug Anlage 11.15 (lfdNr. 59)).

345. Zur IT-forensischen Beweissicherung bei InfoSichhVork arbeitet das **CSOCBw** mit dem BAMAD oder Einrichtungen des Bundes (z. B. Bundesamt für Sicherheit in der Informationstechnik (BSI), Bundeskriminalamt (BKA)) und dem Regionalzentrum NORD des ZCSBw zusammen.

346. Der bzw. die **ISB Geheimschutzbetreute Wirtschaft** (ISBGBW) übt die Fachaufsicht Krypto / COMSEC gegenüber der geheimschutzbetreuten Wirtschaft (siehe Bezug Anlage 11.15 (lfdNr. 43)) derjenigen Unternehmen in der Bundesrepublik Deutschland aus, die Kryptomittel der Bw einsetzen. Hierzu initiiert, beauftragt und koordiniert er bzw. sie InfoSichhIn (siehe Abschnitt 7.2), InfoSichhKtr (siehe Abschnitt 7.3) oder InfoSichhPrfg (siehe Abschnitt 7.4) bezogen auf Krypto / COMSEC bei Unternehmen der geheimschutzbetreuten Wirtschaft in Absprache mit dem Bundesministerium für Wirtschaft und Energie und führt diese durch. Darüber hinaus führt er bzw. sie

63 z. B. Lotus Notes, Verzeichnisdienste, NuKomBw, HaFIS
64 z. B. Sicherheitsgateways an Netzübergängen in Fremdnetze
65 Im Regionalzentrum NORD des ZCSBw stehen zur Unterstützung des CSOCBw ebenfalls IT-forensische Fähigkeiten zur Verfügung, vgl. Nr. 342.

ggf. anlassbezogene InfoSichhIn und InfoSichhPrfg zur Aufrechterhaltung bzw. Wiederherstellung der Kryptosicherheit bei Unternehmen der geheimschutzbetreuten Wirtschaft durch.

3.5.3 Dezentrale Überwachung der Informationssicherheit

347. Die **ISBOrgBer** führen die aktuelle Lage zur InfoSichh ihres OrgBer und verantworten die Rolle des IT-Risikomanagers bzw. der IT-Risikomanagerin für ihren Zuständigkeitsbereich.

348. Der bzw. die **ISBEinsatz** ist verantwortlich für die einsatzspezifische Überwachung der InfoSichh, das Führen und Bewerten der aktuellen Informationssicherheitslage und verantwortet die Rolle des IT-Risikomanagers bzw. der IT-Risikomanagerin in seinem bzw. ihrem Zuständigkeitsbereich.

349. Der bzw. die **ISBBMVg** und der bzw. die **ISBMAD** führen regelmäßig InfoSichhIn (siehe Abschnitt 7.2) und anlassbezogen InfoSichhPrfg (siehe Abschnitt 7.4) in den DSt ihres Zuständigkeitsbereiches durch und verantworten die Rolle des IT-Risikomanagers bzw. der IT-Risikomanagerin in seinem bzw. ihrem Zuständigkeitsbereich.

350. Die **ISBDSt** bzw. **ISB i.E.** führen unregelmäßige InfoSichhKtr (siehe Abschnitt 7.3) in ihren DSt bzw. EinsKtgt / EinsStO durch und verantworten die Rolle des IT-Risikomanagers bzw. der IT-Risikomanagerin in seinem bzw. ihrem Zuständigkeitsbereich.

351. Die **ISBBtrb** arbeiten mit dem bzw. der ISBDSt, den ISBProj und anderen für IT-Btrb(Fü)Einr zuständigen ISB zusammen und sind für die Steuerung und Überwachung aller technischen InfoSichh-Maßnahmen für die im eigenen Zuständigkeitsbereich betriebenen IT-Services und Produkte verantwortlich. Sie überwachen ihre Systeme auf Basis der vorliegenden Informationen / Erkenntnisse bzgl. aller Aspekte der InfoSichh nach den Vorgaben des bzw. der CISOBw und unterstützen den bzw. die ISBDSt bzw. die Inspektionsteams der Regionalzentren des ZCSBw bei der Durchführung von InfoSichhIn, InfoSichhKtr und InfoSichhPrfg (siehe Abschnitt 7) zur Gewährleistung der InfoSichh inkl. des IT-RM im Betrieb im eigenen Zuständigkeitsbereich. Dabei sorgen sie für die Bereitstellung der ggf. erforderlichen Zugangs- / Zugriffsberechtigungen.

352. Bei Unternehmen, die Betriebsaufgaben für die Bw übernehmen, veranlasst bzw. erbringt der bzw. die **ISBAN** diese Unterstützungsleistungen (siehe Nr. 308).

353. Alle Stellen der dezentralen Überwachung melden ihre jeweiligen Lageerkenntnisse und Bewertungen als Lagebeitrag für die Gesamtlage an das CSOCBw.

4 Informationssicherheit in den Anwendungsbereichen

4.1 Anwendungsbereiche und Rollenträgerinnen und Rollenträger

401. Die im Rahmen des Informationssicherheitsmanagementprozesses (siehe Nr. 109, Abb. 1) durchzuführenden Aufgaben wie

- die Erstellung und Herausgabe von Regelungen,
- die Schutzbedarfsfeststellung,
- die Planung und Realisierung der technischen, organisatorischen, personellen und infrastrukturellen InfoSichh-Maßnahmen inkl. des IT-RM,
- die Akkreditierung sowie die Überwachung und Gewährleistung der InfoSichh durch InfoSichhIn, InfoSichhKtr und InfoSichhPrfg,
- das Meldewesen sowie die Behandlung von InfoSichhVork,
- das IT-Krisenmanagement in der Bw,
- das Hinwirken, über den zuständigen bzw. die zuständige ADSB, bei allen Systemen, auch bei Testsystemen, die PersDat verarbeiten, vor Inbetriebnahme auf Feststellung der eventuell notwendigen vorhandenen Datenschutz-Folgenabschätzung und Anmeldung im Verfahrensverzeichnis,
- das Nachsteuern von Maßnahmen und Regelungen sowie
- die Beratung, Sensibilisierung und Ausbildung der Verantwortlichen durch speziell hierfür ausgebildetes Personal

sind jeweils in unterschiedlicher Ausprägung in verschiedenen **Anwendungsbereichen** durchzuführen.

402. Diese Anwendungsbereiche sind

- Wehrtechnische Forschung & Technologie sowie sonstige Forschungsvorhaben, Erprobungen, Truppenversuche und Wehrtechnische Aufträge (F),
- Wissenschaftliche Unterstützung Nicht-Technisch (W),
- Projekte nach Customer Product Management (P),
- Infrastruktur- / Baumaßnahmen bzw. sonstige Vorhaben mit IT-Anteil (V),
- IT-Betrieb und Aufgabenübernahme durch Dritte (O),
- Sofortinitiativen für den Einsatz (Phasendokument „Fähigkeitslücke und Funktionale Forderung“) (S),
- Dienststellen (D),
- Einsatzkontingente und Einsatzstandorte (E) und
- Übungen (Ü).

403. Innerhalb dieser Anwendungsbereiche werden die Aufgaben durch **Rollenträgerinnen und Rollenträger** wahrgenommen. Dabei werden auch einige der in Abschnitt 3 eingeführten zentralen und dezentralen Organisationselemente der InfoSichh zu Rollenträgerinnen und Rollenträgern.

404. Die Anwendungsbereiche werden gekennzeichnet (z. B. „F“ für Forschungsvorhaben, „P“ für CPM-Projekte) und die Rollenträgerinnen und Rollenträger diesen zugeordnet (siehe Nr. 407). Die Kennzeichnungen der Anwendungsbereiche (F, W, P, V, O, S, D, E und Ü) finden sich im „Modulteil“ (Abschnitt 5 – 10) und im „Anlagenteil“ (Anlage 11) innerhalb der jeweiligen Abschnittsüberschriften wieder. Diesbezüglich nicht markierte Abschnittsüberschriften sind für alle Anwendungsbereiche relevant.

405. Alle Rollenträgerinnen und Rollenträger müssen die Vorgaben aus dem „Allgemeinen Teil“ (Abschnitt 1 – 4) dieser Zentralen Dienstvorschrift sowie die im „Modulteil“ (Abschnitt 5 – 10) und im „Anlagenteil“ (Anlage 11) entsprechend gekennzeichneten Abschnitte im Rahmen ihrer Zuständigkeit berücksichtigen und umsetzen.

406. Die Anlage 11.5 enthält für bestimmte Anwendungsbereiche Wegweiser in tabellarischer Form, der eine stichwortartige Übersicht über alle Tätigkeiten und die dafür zuständigen Rollenträgerinnen und Rollenträger bietet.

407. In der Abb. 9 werden alle Anwendungsbereiche aufgeführt und die Rollenträgerinnen und Rollenträger diesen Anwendungsbereichen zugeordnet. Zudem werden den Anwendungsbereichen Kennzeichen zugeordnet (z. B. „D“ für Dienststellen).

	Anwendungsbereiche								
	Wehrtechnische Forschung & Technologie sowie sonst. Forschungsvorhaben, Erprobungen, Truppenversuche und Wehrtechnische Aufträge	Wissenschaftliche Unterstützung Nicht-Technisch (WissUstg NT)	Projekte nach CPM	Infrastruktur- / Baumaßnahmen bzw. sonstige Vorhaben mit IT-Anteil	IT-Betrieb / Aufgabenübernahme durch Dritte	Sofortinitiativen für den Einsatz (FFF(S))	Dienststellen	Einsatzkontingente und Einsatzstandorte	Übungen
Anwendungsbereiche	**F**	**W**	**P**	**V**	**O**	**S**	**D**	**E**	**Ü**
Rollenträgerinnen und Rollenträger									
Verantwortliche von Vorhaben bzw. Projekten der Wehrtechnischen Forschung & Technologie sowie sonstiger Forschungsvorhaben, Erprobungen, Truppenversuche und Wehrtechnischen Aufträgen	**X**								
Verantwortliche von Vorhaben der Wissenschaftlichen Unterstützung nicht-technisch		**X**							
Ltr IPT	**X**		**X**			**X**			
Projektleiter / Projektleiterin	**X**	**X**	**X**		**X**	**X**			
Auftragnehmer	**X**	**X**	**X**	**X**	**X**	**X**			
ISBAN	**X**	**X**	**X**	**X**	**X**	**X**			
DEUmilSAA	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
NDA Germany	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**
APZBw	**X**		**X**	**X**	**X**	**X**	**X**	**X**	**X**
PZITSichhBw	**X**		**X**	**X**	**X**	**X**			
MAD	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
DStLtr / KtgtFhr / Kdr EinsStO			**X**	**X**	**X**	**X**	**X**	**X**	**X**
Ltr IT-Btrb(Fü)Einr							**X**	**X**	**X**

	Anwendungsbereiche								
	Wehrtechnische Forschung & Technologie sowie sonst. Forschungsvorhaben, Erprobungen, Truppenversuche und Wehrtechnische Aufträge	Wissenschaftliche Unterstützung Nicht-Technisch (WissUstg NT)	Projekte nach CPM	Infrastruktur- / Baumaßnahmen bzw. sonstige Vorhaben mit IT-Anteil	IT-Betrieb / Aufgabenübernahme durch Dritte	Sofortinitiativen für den Einsatz (FFF(S))	Dienststellen	Einsatzkontingente und Einsatzstandorte	Übungen
Anwendungsbereiche	**F**	**W**	**P**	**V**	**O**	**S**	**D**	**E**	**Ü**
Rollenträgerinnen und Rollenträger									
IT-Personal der DSt / des EinsKtgt							**X**	**X**	**X**
IT-Anwender der DSt / des EinsKtgt							**X**	**X**	**X**
Übungsleitende bzw. -leitender		**X**							**X**
CISO Ressort	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
CISOBw	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
CISO Rüstung			**X**			**X**			
CISO Infrastruktur				**X**	**X**		**X**		
CSOCBw					**X**		**X**	**X**	**X**
ISBOrgBer	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
ISBBMVg	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
ISBEinsatz				**X**	**X**	**X**		**X**	**X**
ISBBtrb			**X**		**X**	**X**	**X**	**X**	**X**
ISBMAD			**X**	**X**		**X**	**X**	**X**	
ISBDSt		**X**		**X**	**X**		**X**		**X**
ISB i.E. (ISB DEUEinsKtgt bzw. ISB EinsStO)				**X**	**X**	**X**		**X**	
ISBGBW	**X**	**X**	**X**		**X**		**X**	**X**	
ISBProj	**X**		**X**		**X**	**X**	**X**	**X**	**X**

	Anwendungsbereiche								
	Wehrtechnische Forschung & Technologie sowie sonst. Forschungsvorhaben, Erprobungen, Truppenversuche und Wehrtechnische Aufträge	Wissenschaftliche Unterstützung Nicht-Technisch (WissUstg NT)	Projekte nach CPM	Infrastruktur- / Baumaßnahmen bzw. sonstige Vorhaben mit IT-Anteil	IT-Betrieb / Aufgabenübernahme durch Dritte	Sofortinitiativen für den Einsatz (FFF(S))	Dienststellen	Einsatzkontingente und Einsatzstandorte	Übungen
Anwendungsbereiche	**F**	**W**	**P**	**V**	**O**	**S**	**D**	**E**	**Ü**
Rollenträgerinnen und Rollenträger									
ISBÜb		**X**							**X**
ISBFW	**X**	**X**							

Abb. 9: Rollenträgerinnen und Rollenträger mit Zuständigkeiten in den Anwendungsbereichen

4.2 Wehrtechnische Forschung & Technologie sowie sonstige Forschungsvorhaben, Erprobungen, Truppenversuche und Wehrtechnische Aufträge (F)

408. Für Vorhaben der wehrtechnischen Forschung & Technologie (F&T-Vorhaben) bzw. sonstige, z.B. wehrmedizinische Forschungs-[66] und Entwicklungsvorhaben, Erprobungen, Truppenversuche und Wehrtechnische Aufträge (WTA) mit prototypischer Realisierung von IT (dies schließt in Waffensysteme eingebettete IT mit ein), die Echtdaten verarbeiten oder übertragen muss, die an das IT-SysBw angebunden wird, die einen internationalem Bezug (z. B. wegen Verarbeitung / Übertragung von Informationen der NATO) hat oder die in bestehende bzw. in auftragsbezogen einzurichtende IT-Infrastruktur von DSt (z.B. Wehrtechnische / Wehrwissenschaftliche DSt) eingebunden werden muss, ist ein InfoSichhKFW gemäß Abschnitt 6.3.4 zu erstellen[67]. Der bzw. die Leitende des entsprechenden

[66] Dazu gehören insbesondere alle Forschungsvorhaben im Rahmen der Ressortforschung des BMVg.

[67] Für technische Erprobungen von Wehrmaterial, die bei WTD / WWD / MArs durchgeführt werden, sind durch den ISBProj frühzeitig in Abstimmung mit dem bzw. der betreffenden ISBFw InfoSichh-Maßnahmen aus dem InfoSichhKProj abzuleiten und in einem InfoSichhFW festzulegen. Entsprechend sind bei der Erteilung von WTA durch den Auftraggeber bereits im Auftrag InfoSichh-Maßnahmen zu definieren, welche bei der bearbeitenden DSt für den Zeitraum der Auftragsbearbeitung umzusetzen sind. Wenn absehbar ist, dass für die Umsetzung von InfoSichh-Maßnahmen bei der zu beauftragenden DSt Haushaltsmittel benötigt werden, so sind diese von dem bzw. der Leitenden frühzeitig einzuplanen.

Vorhabens ist für die InfoSichh des Vorhabens insgesamt, für die Erstellung des InfoSichhKFW und für die Umsetzung der darin dokumentierten InfoSichh-Maßnahmen verantwortlich. Zu seiner Unterstützung kann der bzw. die Leitende einen ISBFW bestellen, wobei zu beachten ist, dass die Rollen ISBDSt und ISBFW in diesem Anwendungsbereich nicht in Personalunion wahrgenommen werden dürfen. Das InfoSichhKFW ist gemäß Nr. 641 durch die DEUmilSAA mitzeichnen zu lassen.

409. Vor Beginn entsprechender Untersuchungen mit prototypischer Anbindung an das IT-SysBw ist die IT durch den Leitenden bzw. die Leitende des entsprechenden Vorhabens / Versuches analog zu den Vorgaben des Abschnitts 5.6.2 freizugeben und gemäß Abschnitt 5.5 durch die DEUmilSAA zu akkreditieren. Bei Erprobungen und WTA ist der bzw. die ISBDSt der betroffenen DSt des OrgBer AIN in diesen Akkreditierungsprozess einzubinden.

4.3 Wissenschaftliche Unterstützung Nicht-Technisch (W)

410. Unter dem Begriff „WissUstg NT“ wird die zielgerichtete Anwendung, Steuerung und Koordinierung der wissenschaftlichen Methoden Concept Development and Experimentation (CD&E), Modellbildung und Simulation (M&S), Operations Research (OR), Architektur (Arch) und Nicht Technische (NT) Studien verstanden. Wird bei Anwendung dieser Methoden prototypische IT realisiert, die Echtdaten verarbeiten und/oder übertragen muss, die an das IT-SysBw angebunden wird oder die einen internationalen Bezug (z. B. wegen Verarbeitung / Übertragung von Informationen der NATO) hat, ist ein InfoSichhKFW gemäß Abschnitt 6.3.4 zu erstellen. Der bzw. die Leitende des entsprechenden Vorhabens WissUstg NT ist für die InfoSichh des Vorhabens insgesamt, für die Erstellung des InfoSichhKFW und für die Umsetzung der darin dokumentierten InfoSichh-Maßnahmen verantwortlich. Zu seiner Unterstützung kann der bzw. die Leitende einen ISBFW bestellen. Das InfoSichhKFW ist gemäß Nr. 641 durch die DEUmilSAA mitzeichnen zu lassen.

411. Vor Beginn wissenschaftlicher Untersuchungen mit prototypischer Anbindung an das IT-SysBw ist die IT durch den Leitenden bzw. die Leitende des entsprechenden Vorhabens analog zu den Vorgaben des Abschnitts 5.6.2 freizugeben und gemäß Abschnitt 5.5 durch die DEUmilSAA zu akkreditieren.

4.4 Projekte nach Customer Product Management (P)

4.4.1 Allgemeines

412. Gemäß CPM (siehe Bezug Anlage 11.15 (lfdNr. 12)) ist InfoSichh Teil des Projektelementes “Informationssicherheit, IT-Architektur / -Standardisierung und Datenschutz“. Für Projekte ist grundsätzlich ein InfoSichhKProj zu erstellen.

413. Für IT, die ausschließlich querschnittliche InfoSichh-Funktionen erfüllt und nicht primär der Informationsverarbeitung dient (z. B. querschnittliche Kryptogeräte), kann ausnahmsweise mit

vorheriger Zustimmung der DEUmilSAA in Abstimmung mit dem CISO Rüstung auf die Erstellung eines InfoSichhKProj verzichtet werden.

414. Sofern das Projekt lediglich Haushaltsmittel für die Beschaffung querschnittlicher IT der DSt bereitstellt, entfällt die Erstellung eines InfoSichhKProj. Für die Dokumentation und die Herstellung der InfoSichh sind in diesem Fall die DSt (siehe Anwendungsbereich DSt (D), Nr. 451) verantwortlich. Hierzu sind den DSt vom Verantwortlichen für die Beschaffung oben genannter IT die hierzu notwendigen Informationen bereitzustellen.

4.4.2 Analysephase (Projektelement „Informationssicherheit, IT-Architektur / -Standardisierung und Datenschutz“ im Phasendokument „Fähigkeitslücke und Funktionale Forderung“)

415. Im Integrierten Planungsprozess und in der **Analysephase Teil 1** des CPM liegt die Verantwortung für die InfoSichh bei Projekten in Verantwortung BMVg Abt Plg beim bzw. bei der Ltr IPT im Planungsamt der Bundeswehr (PlgABw) bzw. bei Projekten in der Verantwortung BMVg Abt CIT beim bzw. bei der Ltr IPT im KdoCIR. Im CPM-Dokument „Fähigkeitslücke und Funktionale Forderung (FFF)“ ist hinsichtlich des Projektelementes “Informationssicherheit, IT-Architektur / -Standardisierung und Datenschutz“ für den Anteil der InfoSichh die Informationsstruktur mit Schutzbedarfsfeststellung gemäß Abschnitt 2.1 zu dokumentieren. Die Ltr IPT beteiligen hierzu frühzeitig die DEUmilSAA und bei der Festlegung der Informationsstruktur stets den zuständigen bzw. die zuständige ADSB[68]. Dieser bzw. diese prüft, ob PersDat (siehe Nr. 203) verarbeitet werden sollen und berät den bzw. die Ltr IPT bei der Bewertung hinsichtlich ihrer Zuordnung zu Schutzbereichen und ihres Schutzbedarfes sowie hinsichtlich der Prüfung der Rechtsgrundlage der Verarbeitung von PersDat sowie der eventuell notwendigen Datenschutz-Folgenabschätzung.

416. In der **Analysephase Teil 2** liegt die Verantwortung für die InfoSichh beim bzw. bei der Ltr IPT im BAAINBw. Dieser bzw. diese übernimmt damit die Rolle des bzw. der ISBProj, sofern er bzw. sie keinen bzw. keine ISBProj zur Unterstützung gemäß Abschnitt 5.7 bestellt. Die Aufgaben des bzw. der ISBProj sind im Abschnitt 9.6 beschrieben.

417. In der Analysephase Teil 2 sind InfoSichhKProj (siehe Abschnitt 6.3.2) als Anlagen zu den entsprechenden Lösungsvorschlägen[69] für das CPM-Dokument „Auswahlentscheidung (AWE)“ durch den bzw. die Ltr IPT zu erstellen. Die InfoSichhKProj sind gemäß Nr. 621 abzustimmen und durch die DEUmilSAA mitzeichnen zu lassen. Sie müssen u. a. folgende Punkte dokumentieren:

- den Geltungsbereich des InfoSichhKProj,
- das Einsatzspektrum des Systems,

[68] Dies sollte ein bzw. eine ADSB des Hauptnutzers sein. Dies ist im IPT festzulegen.
[69] Dies gilt auch für das Dokument FFF mit LV.

- die Informationsstruktur mit Schutzbedarfsfeststellung (siehe Abschnitt 2.1),
- die Strukturanalyse des Systems mit Angaben zur Systemarchitektur sowie zum Einsatzspektrum des Systems,
- Abhängigkeiten bzgl. der InfoSichh von und zu anderen Projekten wie Vorgaben aus anderen Projekten und Auswirkungen auf andere Projekte,
- die Notwendigkeit des Einsatzes zugelassener InfoSichh-Produkte gemäß Abschnitt 5.3,
- die Notwendigkeit einer Akkreditierung gemäß Abschnitt 5.5,
- Festlegung der Verpflichtungen gem. Art. 26 EU-DSGVO (siehe Bezug Anlage 11.15 (lfdNr. 65)),
- die Prüfung der Rechtsgrundlage der Datenverarbeitung von PersDat,
- in Abhängigkeit vom Schutzbedarf zutreffende Festlegungen für normalen Schutzbedarf sowie InfoSichh-Anforderungen bei hohem oder sehr hohem Schutzbedarf (siehe Anlage 11.3),
- relevante Bausteine und InfoSichh-Maßnahmen aus dem IT-Grundschutzkatalog der Bw in Abhängigkeit vom Schutzbedarf (soweit wie in der Analysephase 2 möglich),
- ggf. zusätzliche / alternative InfoSichh-Maßnahmen (siehe Abschnitt 2.2.2),
- die bereits bekannten Aspekte / InfoSichh-Maßnahmen für die IT-Notfallvorsorge,
- die für den Anteil InfoSichh des Projektelementes „Informationssicherheit, IT-Architektur / -Standardisierung und Datenschutz“ bereits bekannten Risiken (soweit wie möglich eine projektbezogene Risikoanalyse gemäß Abschnitt 6.2, unter Berücksichtigung des Einsatzumfeldes und der geplanten Systemarchitektur) sowie
- Vorgaben für die Fortschreibung.

Zur Struktur eines InfoSichhKProj siehe Anlage 11.7.1.

418. Die Ltr IPT prüfen frühzeitig die Notwendigkeit von **Zulassungen** (siehe Abschnitt 5.3), **Zertifizierungen** (siehe Abschnitt 5.2) bzw. **Anerkennungen** (siehe Abschnitt 5.4) für IT-Produkte im Projekt, stimmen die Rahmenbedingungen mit der DEUmilSAA ab und stellen entsprechende Anträge. Die notwendigen Ressourcen für Evaluierungsleistungen sind projektseitig einzuplanen.

4.4.3 Realisierungsphase

419. In der **Realisierungsphase** liegt die Verantwortung für die InfoSichh weiterhin beim bzw. bei der Ltr IPT im BAAINBw, der bzw. die ab dieser Phase zugleich ProjLtr ist. Er bzw. sie übernimmt damit die Rolle des bzw. der ISBProj, sofern er bzw. sie keinen bzw. keine ISBProj zur Unterstützung (siehe Abschnitt 5.7) bestellt. Die Aufgaben des bzw. der ISBProj sind im Abschnitt 9.6 beschrieben.

420. Aufbauend auf der ausgewählten Lösung der AWE ist das InfoSichhKProj fortzuschreiben. Basierend auf dieser Fortschreibung des InfoSichhKProj sind die Anforderungen zum Anteil InfoSichh des Projektelementes „Informationssicherheit, IT-Architektur / -Standardisierung und Datenschutz“ im Rahmen des Vergabeverfahrens in der Leistungsbeschreibung einzubringen. Die ProjLtr beteiligen hierzu weiterhin die DEUmilSAA.

421. Nach erfolgtem Vergabeverfahren sind die technischen InfoSichh-Maßnahmen umzusetzen. Das InfoSichhKProj muss die abschließend realisierten technischen InfoSichh-Maßnahmen dokumentieren. Abhängigkeiten bzgl. der InfoSichh von anderen Projekten und Auswirkungen auf andere Projekte sind mit den jeweils zuständigen Ltr IPT / ProjLtr abzustimmen und zu berücksichtigen.

422. Die im Projektverlauf erkannten InfoSichh-Risiken sind im InfoSichhKProj zu dokumentieren und zu bearbeiten. Sofern zugelassene Produkte eingesetzt und in den Zulassungsdokumenten des BSI Risiken benannt werden, sind diese Risiken ebenfalls in das Risikomanagement aufzunehmen.

423. Im Rahmen der Integrierten Nachweisführung ist die vollständige und korrekte Umsetzung der technischen InfoSichh-Maßnahmen zu prüfen. Die Durchführung der Prüfung ist durch den bzw. die Ltr IPT / ProjLtr zu bestätigen. Der Nachweis der Prüfung ist dem InfoSichhKProj als Anlage anzufügen.

424. Die ProjLtr beantragen frühzeitig vor Beginn der Nutzung eine ggf. erforderliche **Akkreditierung** (vgl. Nr. 520) der IT bei der DEUmilSAA (siehe Nr. 530).

425. Nach Abstimmung und Berücksichtigung der Mitzeichnung (siehe Nr. 620) setzt der bzw. die ProjLtr das finalisierte InfoSichhKProj in Kraft und übermittelt es an die Stellen gemäß Nr. 622.

426. Mit der **Genehmigung zur Nutzung** (GeNu) ist das Projekt durch den bzw. die ProjLtr freizugeben (**verfahrensbezogene Freigabe** gemäß Abschnitt 5.6.2).

427. Die Vorgaben für andere Projekte und für DSt / IT-Btrb(Fü)Einr und EinsKtgt sind den entsprechenden Rollenträgerinnen und Rollenträgern (DStLtr, Ltr IT-Btrb(Fü)Einr, KtgtFhr) rechtzeitig vor Nutzungs- bzw. Betriebsbeginn zu übergeben (siehe Nr. 622). Hierzu zählen auch ggf. notwendige Arbeitshilfen. Vor Beginn des Wirkbetriebes übergibt der bzw. die ProjLtr neben dem fertigen InfoSichhKProj die für den Betrieb und die Nutzung erforderliche technische Dokumentation an die o.g. Rollenträgerinnen und Rollenträger.

428. Die technische Kopplung von Komponenten, Systemen und Produkten bzw. die Nutzung von IT-Services hat immer unter Beachtung der InfoSichh zu erfolgen[70]. Die technische Kopplung hat in enger Abstimmung zwischen den jeweils zuständigen ISBProj unter Beteiligung der betroffenen ISBBtrb zu erfolgen, um die Aufnahme in bestehende Betriebsprozesse, vor allem aber die Konformität der InfoSichh mit anderen existierenden zentralen Vorgaben und Anforderungen zu gewährleisten, um die Robustheit, Verfügbarkeit und Stabilität der gekoppelten Komponenten, Systeme und Produkte nicht zu gefährden.

[70] Siehe Anlage 11.15 lfd-Nr. 61

4.4.4 Nutzungsphase

4.4.4.1 Allgemeines

429. Der bzw. die ProjLtr ist in der Nutzungsphase für die Gewährleistung, d. h. Herstellung, Aufrechterhaltung und Wiederherstellung der projektbezogenen und damit insbesondere der technischen InfoSichh verantwortlich. Er bzw. sie hat

- bei identifizierten Mängeln der technischen InfoSichh unter Abwägung der Schwere der Mängel die Freigabe (siehe Abschnitt 5.6) aufzuheben oder zeitlich zu befristen (siehe Abschnitt 5.6.5) und die Wiederherstellung der InfoSichh zu veranlassen,
- die Konfigurationskontrolle der durch ihn bzw. sie ausgelieferten IT zu übernehmen,
- im Rahmen des Obsoleszenzmanagements die Aktualität der eingesetzten Hardware und Software sicherzustellen,
- bei allen relevanten Änderungen (siehe Nr. 625) an der IT
  - + das InfoSichhKProj fortzuschreiben (siehe Abschnitt 6.3.2.3),
  - + das InfoSichhKProj durch die DEUmilSAA mitzeichnen zu lassen, spätestens im Rahmen der Re-Akkreditierung,
  - + die IT für die weitere Nutzung erneut freizugeben (siehe Abschnitt 5.6.4) und
  - + die DEUmilSAA hierüber zu unterrichten,
- die erforderlichen regelmäßig wiederkehrenden Maßnahmen zur Aufrechterhaltung der Zulassung(en) rechtzeitig einzuplanen und umzusetzen sowie
- eine ggf. erforderliche Re-Akkreditierung (siehe Abschnitt 5.5.8) der IT rechtzeitig bei der DEUmilSAA zu beantragen.

430. Existieren auf Basis des fortgeschriebenen InfoSichhKProj neue Vorgaben für andere Projekte und daraus resultierend für DSt / IT-Btrb(Fü)Einr und EinsKtgt, so sind diese sowie das fortgeschriebene InfoSichhKProj den entsprechenden Rollenträgerinnen und Rollenträgern (ProjLtr, DStLtr, Ltr IT-Btrb(Fü)Einr, KtgtFhr) rechtzeitig vor Nutzungs- bzw. Betriebsbeginn der Änderungen zu übergeben (vgl. Nr. 624).

431. Liegt für in der Nutzung befindliche IT kein InfoSichhKProj (siehe Abschnitt 6.3.2) vor, ist dieses nachträglich in Verantwortung des bzw. der ProjLtr zu erstellen. Soll auf die nachträgliche Erstellung ausnahmsweise verzichtet werden, ist die Zustimmung der DEUmilSAA einzuholen.

432. Bei Beendigung der Nutzung von IT sind die hierzu im InfoSichhKProj beschriebenen Maßnahmen (siehe Anlage 11.7.1) umzusetzen.

433. Dienststellen- und einsatzbezogene Aufgaben in der Nutzungsphase sind in den Anwendungsbereichen DSt (D) (siehe Abschnitt 4.8) und EinsKtgt und EinsStO (E) (siehe Abschnitt 4.9) beschrieben.

4.4.4.2 Übernahme von IT anderer Nationen / Streitkräfte

434. Soll IT anderer Nationen / Streitkräfte unverändert in die nationale Nutzung übernommen werden, so ist durch den bzw. die Ltr IPT die Informationssicherheitsdokumentation (InfoSichhDok) dieser IT auf Abweichungen zu den Vorgaben dieser Zentralen Dienstvorschrift zu prüfen[71]. Das Resultat der Prüfung sowie die InfoSichhDok ist der DEUmilSAA zur Bewertung vorzulegen. Sofern sich ergebende Abweichungen nicht beseitigen lassen, ist das daraus resultierende Risiko zu beschreiben und eine Entscheidung zur weiteren Vorgehensweise über die DEUmilSAA bei CISOBw herbeizuführen.

4.5 Infrastruktur- / Baumaßnahmen bzw. sonstige Vorhaben mit IT-Anteil (V)

435. Für IT, die aus Infrastruktur- / Baumaßnahmen finanziert wird oder sonstige Vorhaben, in denen IT-Anteile beschafft bzw. eingerüstet werden (z. B. Gebäudeverkabelung, Gebäudeautomation), ist der Abschnitt 4.4 durch die hierfür Verantwortlichen (im folgenden „Verantwortlicher für die Infra-Maßnahme“ genannt) sinngemäß anzuwenden. Durch den Bedarfsträger ist mindestens eine Informationsstruktur gemäß Abschnitt 2.1 zu erstellen und zu begründen. Daraus abgeleitet ist durch den Verantwortlichen für die Infra-Maßnahme ein InfoSichhK in Anlehnung an ein InfoSichhKProj (vgl. Abschnitt 6.3.2) zu erstellen und an die nutzenden DSt zu übergeben. Notwendige Abweichungen zu Struktur und Inhalt des InfoSichhK sind mit der DEUmilSAA frühzeitig abzustimmen. Sofern IT aus Infrastrukturmitteln beschafft wird, sind notwendige Abweichungen und Regelungen mit dem CISO Infrastruktur abzustimmen. Dieser führt eine Abstimmung mit CISOBw und der DEUmilSAA herbei.

4.6 IT-Betrieb und Aufgabenübernahme durch Dritte (O)

4.6.1 Übernahme von IT-Betriebsverantwortung

436. Bei der Übernahme der IT-Betriebsverantwortung durch einen Dritten und der Nutzung dieser IT durch den GB BMVg sind grundsätzlich die Bestimmungen dieser Zentralen Dienstvorschrift einschließlich weiterer Zentraler Dienstvorschriften zur InfoSichh sowie weiterer konkretisierender zentraler und dezentraler Durchführungsbestimmungen und Hinweise zur InfoSichh anzuwenden. Diese Regelungen, datenschutzrechtliche Aspekte gemäß EU-DSGVO (siehe Bezug Anlage 11.15 (lfdNr. 65)) und BDSG (siehe Bezug Anlage 11.15 (lfdNr. 2)) sowie die Aufgabenabgrenzung zu den für InfoSichh Verantwortlichen in der Bw (siehe Nr. 311f. sowie Abschnitt 9) sind daher bei der Vertragsgestaltung zu berücksichtigen. Der Auftragnehmer benennt hierzu einen bzw. eine ISBAN gemäß Nr. 308.

[71] Zu Vorgaben zur Anbindung an das IT-SysBw vgl. B1-960/0-7000 (siehe Bezug Anlage 11.15 (lfdNr. 61))

437. Auf Seiten der Bw ist ein bzw. eine ProjLtr zu benennen. Der bzw. die ProjLtr übernimmt damit die Rolle des bzw. der ISBProj, sofern er bzw. sie keinen bzw. keine ISBProj zur Unterstützung gemäß Abschnitt 5.7 bestellt hat. Die Aufgaben des bzw. der ISBProj sind im Abschnitt 9.6 beschrieben.

438. Die InfoSichh-Maßnahmen sind in einem InfoSichhK zu dokumentieren, das in Anlehnung an die Struktur eines InfoSichhKProj zu erstellen ist (siehe Abschnitt 6.3.2). Der Baustein "Outsourcing" aus dem IT-Grundschutzkatalog der Bw ist dabei zu berücksichtigen. Dieses InfoSichhK ist durch die DEUmilSAA gemäß Nr. 621 mitzeichnen zu lassen.

439. Der Vertrag muss dem Auftraggeber das Recht zusichern, die Wirksamkeit der InfoSichh-Maßnahmen und die InfoSichh-Maßnahmen für das unmittelbare Einsatzumfeld der IT auch während der Nutzung kurzfristig und ggf. mit geeigneter Unterstützung des Auftragnehmers zu überprüfen. Vor Beginn der Nutzung ist die IT gemäß Abschnitt 5.5 durch die DEUmilSAA zu akkreditieren und durch den bzw. die ProjLtr gemäß Abschnitt 5.6.2 freizugeben.

Bereits bestehende Verträge sollen diesbezüglich angepasst werden.

4.6.2 Übernahme von Aufgabenbereichen

440. Übernimmt ein Dritter[72] (z. B. ein Auftragnehmer) – mit von ihm selbst betriebener IT – Aufgabenbereiche für die Bw, müssen notwendige Zugriffe von dieser IT auf Datenbestände / Informationen im IT-SysBw über ein Sicherheitsgateway (siehe Begriffsbestimmungen in Anlage 11.11) geführt werden. Eine notwendige Zulassung des Sicherheitsgateways regelt Abschnitt 5.3.4.

441. Für den ggf. in der Verantwortung des Dritten liegenden Anteil des Sicherheitsgateways sind die Bestimmungen zur InfoSichh der Bw, des BSI und ggf. der NATO / EU anzuwenden und bei der Vertragsgestaltung zu berücksichtigen. Darüber hinaus sind bei der Vertragsgestaltung datenschutzrechtliche Aspekte der Auftragsdatenverarbeitung gemäß Art. 28 EU-DSGVO (siehe Bezug Anlage 15 (lfdNr. 65)) zu berücksichtigen.

442. Die zur Anbindung (u.a. am Sicherheitsgateway) erforderlichen InfoSichh-Maßnahmen sind in einem InfoSichhK zu dokumentieren. Das Konzept ist gemäß Nr. 621 mitzeichnen zu lassen.

Sofern Daten der Bw auf der durch den Dritten betriebenen IT verarbeitet werden, ist in den Fällen gemäß Nr. 520 eine Akkreditierung durch die DEUmilSAA ggf. in Zusammenarbeit mit anderen Akkreditierungsstellen (z.B. BMWi) erforderlich.

Dem Auftraggeber muss vertraglich das Recht eingeräumt werden, die Wirksamkeit der InfoSichh-Maßnahmen kurzfristig und sofern notwendig mit geeigneter Unterstützung des Dritten zu prüfen.

[72] Andere Bundesressorts, die IT-Dienstleistungen für die Bundeswehr erbringen, gelten nicht als Dritte.

Vor Beginn der Nutzung ist eine Registrierung und Freigabe zur Inbetriebnahme des Sicherheitsgateways gemäß Anlage 11.2.11 erforderlich.

Bereits bestehende Verträge sollen diesbezüglich angepasst werden.

4.7 Sofortinitiativen für den Einsatz (Phasendokument „Fähigkeitslücke und Funktionale Forderung“) (S)

443. Bei unvorhersehbar dringendem Einsatzbedarf sind im CPM-Dokument „Fähigkeitslücke und Funktionale Forderung (Sofortinitiative) (FFF(S))“ durch den bzw. die Ltr IPT die Informationsstruktur (siehe Abschnitt 2.1) mit dem Schutzbedarf (siehe Abschnitt 2.1.3) zu dokumentieren. Ist in der Informationsstruktur PersDat vorgesehen, beteiligt der bzw. die Ltr IPT bei der Festlegung der Informationsstruktur den zuständigen bzw. die zuständige ADSB[73].

444. Der bzw. die Ltr IPT ist für die InfoSichh verantwortlich und muss sicherstellen, dass vor Nutzung der IT auf Basis des identifizierten Schutzbedarfes mindestens die grundlegenden InfoSichh-Maßnahmen im Rahmen eines vorläufigen InfoSichhKProj (siehe Abschnitt 6.3.2) dokumentiert und umgesetzt sind. Dieses ist gemäß Nr. 621 durch die DEUmilSAA mitzeichnen zu lassen. Für die nachträgliche Erstellung des InfoSichhKProj und der Nachsteuerung von InfoSichh-Maßnahmen ist der bzw. die Ltr IPT verantwortlich. Zu seiner Unterstützung kann der bzw. die Ltr IPT einen bzw. eine ISB bestellen. Für die im Einsatz genutzte IT ist im Rahmen der nachträglichen Erstellung des endgültigen InfoSichhKProj in den Fällen gemäß Nr. 520 eine Akkreditierung erforderlich.

445. Vor Beginn der Nutzung ist mindestens eine vorläufige Freigabe gemäß Abschnitt 5.6.5 zu erteilen.

4.8 Dienststellen (D)

446. DSt umfassen auch Schiffe und Boote sowie vergleichbare zivile und militärische Organisationseinheiten der Bw. Weitere Detaillierungen legen die OrgBer fest.

447. Der bzw. die DStLtr

- ist verantwortlich für die InfoSichh inkl. IT-RM in der DSt. Diese Verantwortung verbleibt auch mit der Bestellung eines bzw. einer ISBDSt bei ihm bzw. ihr,
- bestellt einen bzw. eine ISBDSt und einen stellvertretenden / eine stellvertretende ISBDSt zu seiner bzw. ihrer Unterstützung (siehe Abschnitt 5.7 „Bestellung“ und Abschnitt 9.7 „Aufgabenbeschreibung“), sofern die Aufgaben nicht selbst übernommen werden,
- setzt das InfoSichhK der DSt (InfoSichhKDSt, siehe Abschnitt 6.3.3) in Kraft,

[73] Dies sollte ein bzw. eine ADSB des Hauptnutzers sein. Dies ist im IPT festzulegen.

- erteilt die Freigabe zur Nutzung für die in der DSt genutzte bzw. betriebene IT in Form der operationellen Freigabe gemäß Abschnitt 5.6.3 (vor Beginn der ersten Nutzung) oder als Freigabe in der Nutzung gemäß Abschnitt 5.6.4 (wenn IT in der Nutzung durch den bzw. die Ltr IPT / ProjLtr erneut freigegeben wurde) oder als vorläufige Freigabe gemäß Abschnitt 5.6.5 (in dringenden Fällen nach einer Risikobewertung),
- beantragt ggf. notwendige Akkreditierungen (siehe Nrn. 520 und 530) bzw. Re-Akkreditierungen (siehe Abschnitt 5.5.8),
- unterstützt das ZCSBw bei der Durchführung von InfoSichhIn (siehe Abschnitt 7.2), InfoSichhPrfg (siehe Abschnitt 7.4) und bei der Einbringung von Sensoren zur Erfassung der InfoSichh-Lage sowie
- veranlasst InfoSichhKtr (siehe Abschnitt 7.3) zur Überwachung der InfoSichh in der eigenen bzw. in nachgeordneten DSt.

Weiterhin ist der bzw. die DStLtr verantwortlich für die

- Erstellung und Fortschreibung des InfoSichhKDSt (siehe Abschnitt 6.3.3),
- Herstellung, Gewährleistung und ggf. Wiederherstellung der InfoSichh durch Umsetzung bzw. Gewährleistung aller personellen, infrastrukturellen und organisatorischen InfoSichh-Maßnahmen aus den InfoSichhKProj für die DSt (sind zur Umsetzung Baumaßnahmen erforderlich, so ist nach der Bereichsvorschrift C1-1810/0-6000 VS-NfD (siehe Bezug Anlage 11.15 (lfdNr. 24)) und der Bereichsdienstvorschrift C-1800/121 „Infrastrukturbearbeitung“ (siehe Bezug Anlage 11.15 (lfdNr. 25)), zu verfahren),
- Meldung technischer Mängel der InfoSichh auf dem Dienstweg an den bzw. die Ltr IPT / ProjLtr,
- Maßnahmen zur IT-Notfallvorsorge in seiner bzw. ihrer DSt gem. Notfallmanagementkonzept bzw. Notfallhandbuch der Liegenschaft (siehe Nr. 128) und nach den Vorgaben des BtrbZ IT-SysBw,
- Sensibilisierung und Ausbildung im Rahmen der InfoSichh (siehe Abschnitt 10) für das IT-Personal und die IT-Anwender der DSt und
- Meldung von InfoSichhVork der DSt nach den Vorgaben des Abschnitts 8.

Im Falle unterschiedlicher Sichtweisen von InfoSich und Datenschutz liegt die abschließende Entscheidung bei dem bzw. der DStLtr.

448. Der bzw. die bestellte ISBDSt muss dem bzw. der bestellenden DStLtr unterstellt[74] sein.

449. Unter Berücksichtigung von übergreifenden wirtschaftlichen, örtlichen oder einsatzspezifischen Aspekten und im Einvernehmen mit den betroffenen DStLtr kann ein bzw. eine ISBDSt bestellt werden, der bzw. die für die Wahrnehmung der Aufgaben in mehreren DSt zuständig ist. Die Bestellung des bzw. der ISBDSt erfolgt in diesem Fall vom bzw. von der DStLtr der nächsten gemeinsam vorgesetzten DSt. Einzelheiten hierzu regeln die OrgBer.

[74] In militärischen DSt truppendienstliche Unterstellung.

450. In DSt mit umfangreicher oder komplexer fachspezifischer IT-Ausstattung oder DSt, die stark disloziert sind, können für Organisationseinheiten (z. B. Abteilung, Referat, Dezernat, Sachgebiet, Team) Informationssicherheitsgehilfen (InfoSichhGeh) des bzw. der ISBDSt bestellt werden. Sie arbeiten dem bzw. der ISBDSt in allen Belangen der InfoSichh zu und nehmen ihre Aufgaben (siehe Abschnitt 9.10) nebenamtlich wahr. Einzelheiten hierzu regeln die ISBOrgBer.

451. Für IT,

- die aus einem Projekt zur Beschaffung querschnittlicher IT stammt (siehe Nr. 414),
- die keinem CPM-Projekt (siehe Abschnitt 4.4) bzw. Vorhaben gemäß der Abschnitte 4.2, 4.3 und 4.5 oder einer Sofortinitiative für den Einsatz (siehe Abschnitt 4.7) zuzuordnen ist oder
- für die kein InfoSichhK vorliegt, aber in der DSt betrieben wird,

sind die Informationsstruktur (siehe Abschnitt 2.1) und alle daraus resultierenden InfoSichh-Maßnahmen (ggf. auch InfoSichh-Anforderungen gemäß Anlage 11.2 und Anlage 11.3) im InfoSichhKDSt zu dokumentieren (siehe Nr. 628) und umzusetzen. Umfang und Inhalt der zu erstellenden Anteile sind im Vorfeld und ggf. während der Erstellung mit dem zuständigen Regionalzentrum des ZCSBw, bei IT gemäß Abschnitt 4.5 zudem mit CISO Infrastruktur, abzustimmen. In diesen Fällen ist der bzw. die DStLtr auch für die Umsetzung und Gewährleistung der technischen InfoSichh-Maßnahmen verantwortlich.

Die IT ist gemäß Nr. 520 zu akkreditieren.

452. Der bzw. die ADSB ist bei der Erstellung / Fortschreibung des InfoSichhKDSt zu beteiligen.

453. Das IT-Personal ist durch den jeweils zuständigen bzw. die jeweils zuständige ISBDSt zur InfoSichh gemäß Anlage 11.2.8[75] zu belehren und zu verpflichten.

Die IT-Anwender sowie das IT-Personal sind über die für die DSt geltenden InfoSichh-Bestimmungen gemäß Anlage 11.2.8[75] durch den bzw. die ISBDSt zu belehren.

454. Betreibt eine DSt IT, ist die DSt auch eine IT-BtrbEinr und der bzw. die DStLtr für die Durchführung des IT-Betriebes verantwortlich. Zu seiner bzw. ihrer Unterstützung bestellt der bzw. die DStLtr einen ISBBtrb[76]. Der bzw. die ISBBtrb arbeitet diesbezüglich mit dem bzw. der ISBDSt und den zuständigen ISBProj unter Beteiligung der betroffenen ISBBtrb anderer IT- Btrb(Fü)Einr zusammen. In diesem Fall ist der bzw. die DStLtr verantwortlich für die

- Gewährleistung der betrieblichen InfoSichh in der DSt nach Freigabe der IT durch den jeweiligen bzw. die jeweilige Ltr IPT / ProjLtr (siehe Abschnitt 5.6.2),
- Umsetzung der für den IT-Betrieb relevanten technischen InfoSichh-Maßnahmen der InfoSichhKProj,

[75] Insbesondere die Anlage 11.2.8 lfdNr. 26 (z.B. Cyber Hygiene Check Up) ist zu beachten.
[76] In IT-BtrbEinr kann der bzw. die ISBBtrb in Personalunion mit dem bzw. der ISBDSt der betreibenden DSt bestellt werden.

- Festlegung ggf. abweichender oder zusätzlicher und konkretisierender technischer InfoSichh-Anforderungen und -Maßnahmen, die dem bzw. der Ltr IPT / ProjLtr mitzuteilen und mit der Fortschreibung des InfoSichhKProj zu bestätigen sind,
- Unterstützung aller mit Inspektions-, Kontroll- und Prüfaufgaben beauftragten Stellen und für Bereitstellung der ggf. erforderlichen Zugangs- / Zugriffsberechtigungen sowie
- Durchführung von Notfallübungen für IT in seiner bzw. ihrer Zuständigkeit (Richtwert: alle 2 Jahre).

4.9 Einsatzkontingente und Einsatzstandorte (E)

455. EinsKtgt umfassen auch Kontingente im Einsatzgebiet, Schiffe und Boote sowie vergleichbare Organisationseinheiten der Bw. Weitere Detaillierungen legt das EinsFüKdoBw fest.

456. Zur Herstellung, Überwachung, Gewährleistung und Wiederherstellung der InfoSichh bei Einsätzen gelten grundsätzlich die Vorgaben dieser Zentralen Dienstvorschrift. Besonderheiten können sich ergeben aufgrund

- unterschiedlicher Verfahren und Mittel zur Informationsverarbeitung und -übertragung in der NATO, in der EU, in anderen Nationen und in sonstigen überstaatlichen Organisationen sowie aufgrund organisationsbereichsspezifischer Anwendungen,
- der geografischen sowie klimatischen Bedingungen im Einsatzgebiet,
- der Mitnutzung von angemieteten kommerziellen Übertragungswegen zwischen Inland und Einsatzgebiet sowie innerhalb des Einsatzgebietes,
- der Mitnutzung von offenen Übertragungswegen zum Zwecke der Truppenbetreuung (z. B. Übergänge in öffentliche Netze der Bundesrepublik Deutschland bzw. in das öffentliche Netz im Einsatzgebiet) und
- der spezifischen Gefährdungssituation des jeweiligen Einsatzes, z. B. durch gegnerische Informationsoperationen.

457. Im Einsatzgebiet kommen IT und IT in Waffensystemen zum Einsatz, für die bereits gültige InfoSichhKProj (siehe Abschnitt 6.3.2) vorliegen. Eine Anpassung der InfoSichhKDSt (siehe Abschnitt 6.3.3) an die örtlichen Gegebenheiten ist in der Regel erforderlich. Bereits im Vorfeld von Einsätzen müssen daher nach Möglichkeit die InfoSichhKDSt einsatzbezogen adaptiert werden[77]. Bei Kontingentwechsel ist das vorhandene (standort- bzw. einsatzbezogene) InfoSichhK zu prüfen und ggf. fortzuschreiben.

458. Bei Abweichungen gegenüber den InfoSichhKProj für die im EinsStO / EinsKtgt genutzte / betriebene IT in Bezug auf die Umsetzung von Vorgaben bzw. das Einsatzszenario ist die DEUmilSAA zu unterrichten. Eine Entscheidung der DEUmilSAA zur Akkreditierung dieser IT erfolgt im Einzelfall auf Basis einer Risikobewertung (siehe Nr. 462).

[77] In Abhängigkeit von den örtlichen Gegebenheiten zu einem standortbezogenen InfoSichhk.

459. Beim EinsFüKdoBw sind durch dessen Befehlshaber bzw. Befehlshaberin ein bzw. eine ISBEinsatz und ein Stellvertreter bzw. eine Stellvertreterin (stv. ISBEinsatz) gemäß Abschnitt 5.7 zu bestellen[78]. Die Aufgaben des bzw. der ISBEinsatz sind im Abschnitt 9.3 beschrieben.

460. Änderungen der InfoSichh-Maßnahmen[79] sind im Einzelfall, aufgrund der Besonderheiten des Einsatzes, durch den Kontingentführer bzw. die Kontingentführerin (KtgtFhr) bzw. den Kommandeur bzw. die Kommandeurin (Kdr) EinsStO zu bewerten und in Abstimmung mit dem EinsFüKdoBw (ISBEinsatz) festzulegen und in den entsprechend adaptierten InfoSichhKDSt zu dokumentieren. Gleiches gilt für die Kommunikation zwischen der Bundesrepublik Deutschland und dem Einsatzgebiet. Entsprechende Regelungen trifft das EinsFüKdoBw.

461. Der bzw. die KtgtFhr oder Kdr EinsStO

- ist verantwortlich für die InfoSichh inkl. IT-RM im EinsKtgt / EinsStO. Diese Verantwortung verbleibt auch mit der Bestellung eines bzw. einer ISB i.E. (ISB DEUEinsKtgt bzw. ISB EinsStO) bei ihm bzw. ihr,
- bestellt einen bzw. eine ISB i.E. (ISB DEUEinsKtgt bzw. ISB EinsStO) zur Unterstützung (siehe dazu Abschnitt 5.7 „Bestellung“ und Abschnitt 9.7 „Aufgabenbeschreibung“), der dem bzw. der ISBEinsatz fachlich unterstellt ist und ihn bzw. sie in allen Belangen der InfoSichh im Einsatz berät,
- setzt das bzgl. einsatzspezifischer Belange fortgeschriebene InfoSichhKDSt (siehe Abschnitt 6.3.3) in Kraft,
- erteilt die Freigabe zur Nutzung für die in seinem bzw. ihrem EinsKtgt / EinsStO genutzte bzw. betriebene IT in Form der operationellen Freigabe gemäß Abschnitt 5.6.3 (vor Beginn der ersten Nutzung) oder als Freigabe in der Nutzung gemäß Abschnitt 5.6.4 (wenn IT in der Nutzung durch den bzw. die Ltr IPT / ProjLtr erneut freigegeben wurde) oder als vorläufige Freigabe gemäß Abschnitt 5.6.5 (in dringenden Fällen nach einer Risikobewertung),
- unterstützt das ZCSBw bei der Durchführung von InfoSichhIn (siehe Abschnitt 7.2), InfoSichhPrfg (siehe Abschnitt 7.4) und bei der Einbringung von Sensoren zur Erfassung der InfoSichh-Lage sowie
- veranlasst InfoSichhKtr (siehe Abschnitt 7.3) im eigenen bzw. nachgeordneten Bereich.

462. Weiterhin ist der bzw. die KtgtFhr / Kdr EinsStO verantwortlich für die

- Fortschreibung des InfoSichhKDSt (siehe Abschnitt 6.3.3.3) bzgl. der Einsatzbelange,
- Herstellung bzw. Wiederherstellung der InfoSichh durch Umsetzung bzw. Gewährleistung aller personellen, infrastrukturellen, organisatorischen und der für den IT-Betrieb relevanten technischen InfoSichh-Maßnahmen aus den InfoSichhKProj für die in seinem bzw. ihrem EinsStO / EinsKtgt

[78] Siehe Fußnote 47.

[79] Gilt für organisatorische, personelle, infrastrukturelle sowie die für den IT-Betrieb relevanten technischen InfoSichh-Maßnahmen, sofern die Betriebsverantwortung nicht bei einem Dritten liegt. Liegt die Betriebsverantwortung bei einem Dritten gemäß Abschnitt 4 (z. B. BWI), ist eine Abstimmung herbeizuführen. Sind technische InfoSichh-Maßnahmen betroffen, ist eine Abstimmung mit dem bzw. der jeweils verantwortlichen Ltr IPT / ProjLtr herbeizuführen.

genutzte / betriebene IT (sind zur Umsetzung Baumaßnahmen erforderlich, so ist nach der Bereichsvorschrift C1-1810/0-6000 VS-NfD (siehe Bezug Anlage 11.15 (lfdNr. 24)) und der Bereichsdienstvorschrift C-1800/121 „Infrastrukturbearbeitung“ (siehe Bezug Anlage 11.15 (lfdNr. 25)) zu verfahren),

- Festlegung ggf. zusätzlicher und konkretisierender technischer InfoSichh-Anforderungen und -Maßnahmen, die vom bzw. von der Ltr IPT / ProjLtr bei der Fortschreibung des betroffenen InfoSichhKProj zu bestätigen sind,
- Erstellung einer Risikobewertung, sofern bei den Maßnahmen Abweichungen gegenüber dem InfoSichhKProj erforderlich sind oder die in seinem bzw. ihrem EinsStO / EinsKtgt genutzte / betriebene IT außerhalb des im InfoSichhKProj beschriebenen Einsatzszenarios betrieben wird. Diese Risikobewertung ist über die bzw. den Ltr IPT / ProjLtr an die DEUmilSAA zwecks Entscheidung bzgl. der Akkreditierung dieser IT weiterzuleiten,
- Maßnahmen zur IT-Notfallvorsorge am EinsStO nach den Vorgaben des Risikomanagers bzw. der Risikomanagerin im EinsFüKdoBw bzw. nach operationellen Vorgaben,
- Sensibilisierung im Rahmen der InfoSichh (siehe Abschnitt 10.2) für das IT-Personal und die IT-Anwender seines bzw. ihres EinsKtgt / EinsStO und
- Meldung von InfoSichhVork des EinsKtgt / EinsStO nach den Vorgaben des Abschnitts 8.

463. Das IT-Personal ist durch den jeweils zuständigen bzw. die jeweils zuständige ISB i.E. zur InfoSichh gemäß Anlage 11.2.8 zu belehren und zu verpflichten.

Die IT-Anwender sowie das IT-Personal sind über die für das EinsKtgt / den EinsStO geltenden InfoSichh-Bestimmungen gemäß Anlage 11.2.8 durch den bzw. die ISB i.E. zu belehren.

464. Sofern der EinsStO bzw. das EinsKtgt über ein NOC i.E. verfügt, beauftragt der bzw. die KtgtFhr / Kdr EinsStO einen Leiter bzw. eine Leiterin NOC i.E. (Ltr NOC i.E.) mit der Durchführung von IT-Betriebsaufgaben. Zu seiner bzw. ihrer Unterstützung bestellt der bzw. die KtgtFhr / Kdr EinsStO einen bzw. eine ISBBtrb für die NOC i.E.[80]

465. Der bzw. die Ltr NOC i.E.

- ist – nach Freigabe der IT durch den jeweiligen bzw. die jeweilige Ltr IPT / ProjLtr und KtgtFhr / Kdr EinsStO (siehe Abschnitt 5.6.2 und 5.6.3) – für die Gewährleistung der für den IT-Betrieb relevanten technischen InfoSichh aller nutzenden EinsStO verantwortlich,
- arbeitet mit dem oder den zuständigen ISBProj unter Beteiligung der betroffenen ISBBtrb zusammen,
- meldet technische Mängel der InfoSichh auf dem Dienstweg an den bzw. die ISBEinsatz sowie dem bzw. der zuständigen Ltr IPT / ProjLtr,

[80] Der bzw. die ISBBtrb kann in Personalunion mit dem bzw. der ISB i.E. bestellt werden.

- unterstützt alle mit Inspektions-, Kontroll- und Prüfaufgaben beauftragten Stellen und sorgt für die Bereitstellung der ggf. erforderlichen Zugangs- / Zugriffsberechtigungen und
- trifft Maßnahmen zur IT-Notfallvorsorge im NOC i.E., macht Vorgaben zur IT-Notfallvorsorge auf Basis der Vorgaben des Risikomanagers bzw. der Risikomanagerin im EinsFüKdoBw oder des bzw. der KtgtFhr / Kdr EinsStO für die nutzenden EinsStO sowie operationeller Vorgaben und führt Notfallübungen für IT in seiner bzw. ihrer Zuständigkeit durch (Richtwert: einmal pro Kontingent).

466. Unter Berücksichtigung von übergreifenden, wirtschaftlichen und örtlichen Aspekten und im Einvernehmen mit den betroffenen DStLtr kann ein bzw. eine ISB i.E. bestellt werden, der bzw. die für die Wahrnehmung der Aufgaben in mehreren EinsStO zuständig ist. Die Bestellung des bzw. der ISB i. E. erfolgt in diesem Fall vom bzw. von der KtgtFhr des EinsKtgt. Eine mögliche Personalunion des bzw. der ISB i.E. mit dem bzw. der ISBBtrb (siehe Nr. 464) ist hierbei zu beachten. Einzelheiten regelt ISBEinsatz.

4.10 Übungen (Ü)

467. Voraussetzung für die Teilnahme einer DSt an nationalen oder internationalen Übungen[81] mit ihrer IT ist ein Informationssicherheitsbefehl (InfoSichhBef, siehe Abschnitt 6.3.5). Das nationale übungskoordinierende Kommando regelt die Zuständigkeit für die Bestellung des ISB Übung (ISBÜb) und die Erstellung des InfoSichhBef. Der InfoSichhBef muss die Bestellung eines bzw. einer ISBÜb (dieser bzw. diese kann in Personalunion mit dem bzw. der ISBDSt der übungsleitenden DSt bestellt werden) berücksichtigen. Der InfoSichhBef ist gemäß Nr. 645 durch die DEUmilSAA mitzeichnen zu lassen.

468. Sollen während der Übung PersDat verarbeitet werden, ist der bzw. die ADSB der für die Übung verantwortlichen DSt bei der Erstellung des InfoSichhBef zu beteiligen. Die Regelungen zur Akkreditierung (siehe Abschnitt 5.5) finden auch bei Übungen Anwendung (siehe Nr. 530).

[81] Vergleiche A-229/2 VS-NfD „Übungswesen der Bundeswehr“ (siehe Anlage 11.15 (lfdNr. 62)).

5 Informationssicherheitsverfahren

5.1 Evaluierung von Informationssicherheits-Produkten

501. Eine **Evaluierung** ist eine formale Prüfung mit Bewertung eines InfoSichh-Produktes durch eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannte Prüfstelle. Ziel der Evaluierung ist die Feststellung, ob das Produkt die in den „Sicherheitszielen“ (sogenannten Security Targets) vorgegebenen Sicherheitseigenschaften und damit das erwartete Vertrauen in die Wirksamkeit der implementierten InfoSichh-Funktionen erfüllt.

Die Evaluierung von InfoSichh-Produkten erfolgt nach international anerkannten Kriterien (z. B. nach den „Common Criteria“ (CC, siehe http://www.commoncriteriaportal.org) oder in bestimmten Ausnahmefällen den „Information Technology Security Evaluation Criteria“ (ITSEC)).

Nach erfolgreicher Evaluierung wird dem Produkt die entsprechende Sicherheitseigenschaft bescheinigt. Eine darüber hinaus gehende formelle Bestätigung von Sicherheitseigenschaften wird im Rahmen einer **Zertifizierung** (siehe Abschnitt 5.2) oder einer **Zulassung** (siehe Abschnitt 5.3) erteilt.

502. Das Prüfzentrum für IT-Sicherheit in der Bundeswehr (PZITSichhBw bei der Wehrtechnischen Dienststelle 81 (WTD 81)) ist eine vom BSI anerkannte Prüfstelle und kann neben weiteren, vom BSI anerkannten kommerziellen Prüfstellen Evaluierungen für den GB BMVg durchführen.

5.2 Zertifizierung von Informationssicherheits-Produkten

503. Die **Zertifizierung** von InfoSichh-Produkten ist ein international harmonisiertes Verfahren für die formelle Bestätigung von Evaluierungsergebnissen (Zertifikat; zur Evaluierung siehe Abschnitt 5.1).

Zur Evaluierung mit dem Ziel einer Zertifizierung (z. B. nach „Common Criteria“ (CC)), siehe Abschnitt 5.1.

504. Für die Bundesrepublik Deutschland erteilt ausschließlich das BSI entsprechende Zertifikate. Die Bundesrepublik Deutschland hat sich aber im Rahmen des sogenannten „Common Criteria Mutual Recognition Agreement (CC-MRA)“ verpflichtet, Zertifikate anderer Nationen / Länder in Deutschland (Ausnahmebereich: nationale Sicherheit, z. B. Schutz von VS) anzuerkennen. Dadurch wird die Mehrfach-Zertifizierung des gleichen Produktes in verschiedenen Staaten vermieden, wenn die Zertifikate auf ITSEC oder CC beruhen.

5.3 Zulassung von Informationssicherheits-Produkten

5.3.1 Allgemeines

505. Die **Zulassung** ist eine formale Genehmigung für die Verwendung von InfoSichh-Produkten zur Verarbeitung und Übertragung von staatlich geschützten Verschlusssachen (VS, siehe Nr. 202).

506. Für die Verarbeitung und / oder Übertragung von VS ist die Verwendung zugelassener InfoSichh-Produkte im GB BMVg verbindlich (siehe auch Abschnitt 5.3.4).

5.3.2 Zuständigkeiten

507. Die nationale Zulassungsbehörde für InfoSichh-Produkte in Deutschland ist das BSI. Zulassungsbehörde für InfoSichh-Produkte der NATO ist das „NATO Military Committee (NAMILCOM)“ mit der „Military Committee Communication and Information Systems Security and Evaluation Agency (SECAN)“ als zuständige Evaluierungsstelle. Die Zulassungsbehörde für InfoSichh-Produkte der EU ist das „EU Infosec Office“. Die Evaluierungen werden von den Sicherheitsbehörden bestimmter hierfür durch das EU Infosec Office autorisierter EU-Mitgliedstaaten durchgeführt bzw. veranlasst.

508. Zulassungen von InfoSichh-Produkten, mit denen amtlich als Verschlusssache eingestufte bzw. geheim zu haltende Informationen verarbeitet oder übertragen werden können, werden in Deutschland durch das BSI erteilt. Dies kann z.B. in Form einer allgemeinen Zulassung oder einer Freigabeempfehlung geschehen (zu den Begriffsbestimmungen siehe Anlage 11.11). Dem BMVg bleibt es gemäß Begründung zum BSI-Gesetz (siehe Bezug Anlage 11.15 (lfdNr. 7)) unbenommen, für seinen GB für die Verarbeitung und Übertragung von Informationen eigene informationstechnische Sicherheitsvorkehrungen zu ergreifen bzw. Systeme oder Komponenten zu entwickeln, zu prüfen, zu bewerten und zuzulassen.

509. Zulassungen von InfoSichh-Produkten für die Verarbeitung und Übertragung von VS werden durch den bzw. die CISO Ressort auf Basis von Sicherheitsnachweisungen durch Evaluierungen (siehe Abschnitt 5.1) ausschließlich für die Verwendung im GB BMVg erteilt.

510. Zulassungen von InfoSichh-Produkten, mit denen eingestufte NATO-Informationen verarbeitet oder übertragen werden können, dürfen nur durch das BSI (bis NATO CONFIDENTIAL) oder NAMILCOM (alle NATO-Einstufungen) erteilt werden.

511. Zulassungen von InfoSichh-Produkten, mit denen eingestufte EU-Informationen verarbeitet oder übertragen werden können, dürfen nur durch das BSI (bis EU CONFIDENTIAL in nationalen Systemen) oder dem Rat der Europäischen Union (alle EU-Einstufungen) oder dessen Generalsekretär (bis EU-CONFIDENTIAL) erteilt werden.

5.3.3 Antragstellung (P, V, S)

512. Anträge auf Zulassung oder Verlängerung einer Zulassung eines InfoSichh-Produktes sind durch den bzw. die Ltr IPT / ProjLtr oder den Verantwortlichen bzw. die Verantwortliche für die Infra-Maßnahme an die DEUmilSAA zu richten. Der Antrag ist im Intranetauftritt http://infosichh.bundeswehr.org im Bereich „Produkte / Zulassungen“ eingestellt.

513. Der finanzielle und zeitliche Aufwand für Evaluierungen ist in den Projekten bzw. Vorhaben rechtzeitig und ggf. unter Beteiligung fachlich geeigneter Stellen (z. B. Prüfstellen) durch den bzw. die Ltr

IPT / ProjLtr oder den Verantwortlichen bzw. die Verantwortliche für die Infra-Maßnahme zu berücksichtigen. Eine nachträgliche Berücksichtigung kann zu erheblichen Kostensteigerungen, Verzögerungen oder zum Scheitern des Projektes bzw. Vorhabens führen.

5.3.4 Zulassungspflichtige Informationssicherheits-Produkte (P, V, S)

514. Zulassungspflichtig sind Produkte mit InfoSichh-Funktionen zur Verwendung für VS zur

1. Herstellung von Schlüsselmitteln,
2. Verschlüsselung (Kryptierung) bzw. zur kryptographischen Unterstützung,
3. Löschung oder Vernichtung von VS-Datenträgern,
4. Abstrahlsicherheit,
5. Sicherung von Übertragungsleitungen und
6. Trennung von Netzen mit unterschiedlichen maximalen Einstufungen der verarbeiteten VS.

Die Nummern 3 bis 6 gelten nicht für VS-NfD eingestufte VS.

Nummer 6 gilt jedoch sowohl

- bei einem Sicherheitsgefälle, d.h. wenn in beiden Netzen unterschiedlich hoch eingestufte Informationen (z.B. GEHEIM bzw. VS-NfD) verarbeitet werden, als auch
- bei der Informationsraumtrennung, d.h. wenn ein Netz im deutschen Informationsraum mit einem Netz eines anderen Informationsraums (z.B. NATO, EU bzw. anderer Nationen, sonstiger überstaatlicher Organisationen oder von Missionen) verbunden wird, und nicht sämtliche deutsch eingestuften Informationen für den anderen Informationsraum bestimmt sind[82].

5.4 Anerkennung von Zulassungen, die durch NATO- oder EU-Mitgliedstaaten ausgesprochen wurden (P, V, S)

515. Eine **Anerkennung** ist die formale Genehmigung für die Verwendung von InfoSichh-Produkten für die Verarbeitung / Übertragung nationaler Informationen der Einstufung VS-NfD.

516. Eine Anerkennung kann ein **InfoSichh**-Produkt im Einzelfall dann erhalten, wenn dieses in Deutschland mangels ausreichend vorliegender oder bereitgestellter Dokumentation weder evaluierbar noch zulassungsfähig ist, jedoch eine Zulassung durch die National Communication Security Authority (NCSA) des NATO- bzw. EU-Mitgliedstaates hat, in dem das Produkt entwickelt und evaluiert wurde. Eine Anerkennung wird durch CISOBw auf Basis der Dokumente analog zum Zulassungsantrag (siehe Nr. 512) im Benehmen mit dem BSI ausgesprochen.

517. Eine Anerkennung für ein Produkt bezieht sich **immer** auf

- das festgelegte Einsatzspektrum (d. h. die Verwendungsart) und

[82] Sonderform eines Sicherheitsgefälles.

- einen aktuell zugelassenen Konfigurationsstand.

Die Anerkennung erlischt bei Änderung des Einsatzspektrums, des Konfigurationsstandes bzw. bei Ablauf oder Aufhebung der zugrunde liegenden Zulassung des NATO- bzw. EU-Mitgliedstaates (siehe Nummer 516).

518. Rahmenbedingungen für die Verwendung anerkannter InfoSichh-Produkte für den Schutz von deutschen VS sind den durch CISOBw zu erstellenden Behandlungshinweisen zu entnehmen und in den jeweiligen produktspezifischen Anerkennungsdokumenten auf Basis einer Risikobetrachtung zu beschreiben.

5.5 Akkreditierung

5.5.1 Allgemeines

519. Unter Akkreditierung wird ein Prüfungs- und Genehmigungsverfahren von IT unter Leitung der zuständigen Akkreditierungsstelle verstanden.

520. Eine Akkreditierung im GB BMVg ist grundsätzlich für sämtliche IT durchzuführen, mindestens jedoch für jede IT, die

- Informationen der Einstufung „VS-NUR FÜR DEN DIENSTGEBRAUCH“ oder höher sowie vergleichbare NATO- / EU-Einstufungen bzw. Einstufungen anderer Nationen, sonstiger überstaatlicher Organisationen oder „MISSION“[83],
- PersDat SB 3[84] und / oder
- SSI mit einem sehr hohen Schutzbedarf der Vertraulichkeit

verarbeitet und / oder überträgt.

521. Die Akkreditierung betrifft die folgenden Anwendungsbereiche gemäß Abschnitt 4:

- Wehrtechnische Forschung & Technologie sowie sonstige Forschungsvorhaben, Erprobungen, Truppenversuche und Wehrtechnische Aufträge (siehe Nr. 409),
- Projekte nach CPM gemäß Nr. 424 und 429,
- Infrastruktur- / Baumaßnahmen bzw. sonstige Vorhaben mit IT-Anteil gemäß Nr. 435 i.V.m. Nrn. 424 und 429,
- IT-Betrieb und Aufgabenübernahme durch Dritte gemäß Nr. 438 bzw. 444,
- Sofortinitiativen für den Einsatz (FFF(S)) gemäß Nr. 444 ausschließlich im Rahmen der nachträglichen Erstellung des endgültigen InfoSichhKProj,

[83] „MISSION“ ist der Platzhalter für eine spätere konkrete Benennung und setzt eine sog. *Security Policy* für den beabsichtigten Einsatz voraus. Insofern ist z.B. MISSION SECRET keine gültige Einstufung, sondern z. B. NATO / ISAF SECRET oder NATO SECRET Releasable to ISAF.

[84] Für Medizinprodukte, die nach Erlass dieser Vorschrift beschafft und installiert werden.

- DSt, sofern dort IT gemäß Nr. 451 zum Einsatz kommt,
- EinsKtgt und EinsStO im Rahmen einer Einzelfallentscheidung auf Basis einer Risikobewertung gemäß Nr. 458 und 462 und
- Übungen gemäß Nr. 468 und 645.

Umfang und Tiefe der Akkreditierungsprüfung (siehe Abschnitt 5.5.5) werden durch die Akkreditierungsstelle festgelegt.

522. Der Prozess der Akkreditierung endet bei positivem Abschluss mit einer Akkreditierungsbescheinigung gemäß Anlage 11.8.7. Diese ist grundsätzlich drei Jahre[85] gültig. Ausnahmen sind mit der DEUmilSAA abzustimmen. Sie gilt

- für eine festgelegte Einsatzumgebung[86],
- für eine festgelegte technische Konfiguration,
- für eine definierte Informationsstruktur (siehe Abschnitt 2.1) und
- bis zu einem eventuellen Entzug durch die zuständige Akkreditierungsstelle (siehe Nr. 552).

523. Die nationale Methodik und Systematik des Akkreditierungsprozesses entspricht der Vorgehensweise der NATO / EU. Hierdurch wird erreicht, dass die Ergebnisse der nationalen Akkreditierung auch im Bündniskontext und multinational anerkannt bzw. eingebracht werden können.

5.5.2 Zuständigkeiten

524. Verantwortlich für die Akkreditierung von IT in der Bundesrepublik Deutschland ist als oberste nationale Security Accreditation Authority (SAA) und National Security Authority (NSA) das Bundesministerium des Innern (BMI). Ausführendes Organ des BMI für diese Aufgabe ist das Bundesamt für Sicherheit in der Informationstechnik (BSI).

525. In Deutschland hat das BMI als nationale SAA die Aufgabe für alle Akkreditierungsangelegenheiten im GB BMVg auf die DEUmilSAA übertragen (siehe Bezug Anlage 11.15 (lfdNr. 39)).

526. Die DEUmilSAA ist für die Akkreditierung der IT gemäß Nr. 520 zuständig.

527. Multinationale IT fällt in den Verantwortungsbereich der SAAs mehrerer Nationen oder multinationaler Organisationen. In diesem Fall vertritt die DEUmilSAA die nationalen Interessen ggf. mit Unterstützung der Regionalzentren[87] des ZCSBw.

Die Vorgehensweise zur Akkreditierung multinationaler Anbindungen wird einvernehmlich zwischen den SAAs der beteiligten Nationen und multinationalen Organisationen geregelt.

[85] Für Medizinprodukte 5 Jahre
[86] Hierunter werden auch verlegbare Systeme verstanden, deren Umgebung in einem festgelegten Rahmen wechselt.
[87] Dies betrifft die Sachgebiete "Unterstützung DEUmilSAA Nord bzw. West" der RegZ NORD bzw. WEST.

5.5.3 Aufgaben der Deutschen militärischen Security Accreditation Authority

528. Die DEUmilSAA erfüllt im Rahmen der Akkreditierung folgende Aufgaben:

- Durchführen von Akkreditierungen und Re-Akkreditierungen.
- Mitwirken beim Abschluss von Akkreditierungsvereinbarungen mit internationalen Partnern.
- Prüfen der Umsetzung von mit internationalen Partnern getroffenen Akkreditierungsvereinbarungen.
- Mitwirken bei der Harmonisierung nationaler und multinationaler Regelungen zur Akkreditierung von IT.
- Vertreten der deutschen Position in internationalen / multinationalen Gremien zur Akkreditierung (Security Accreditation Boards).
- Zusammenarbeiten mit SAAs anderer Nationen / überstaatlicher Organisationen bei
  + externen Anbindungen und
  + IT im Verantwortungsbereich mehrerer SAA.
- Beraten in allen Phasen des CPM von Projekten, Vorhaben und Dienststellen hinsichtlich der anzuwendenden nationalen und multinationalen Regelungen in Bezug auf Akkreditierungen.
- Prüfen und Mitzeichnen aller InfoSichhKProj, aller InfoSichhKFW und von InfoSichhBef gemäß Nr. 645 (vergleiche Abschnitt 6.3.1).
- Erstellen von Akkreditierungsbescheinigungen.
- Weiterleiten internationaler Akkreditierungsbescheinigungen.

529. Die DEUmilSAA ist jederzeit berechtigt, Einsicht in die für ihre Aufgabenerfüllung relevanten InfoSichh-Dokumente zu nehmen.

5.5.4 Beantragung einer Akkreditierung

530. Der bzw. die Verantwortliche für die IT (z. B. Ltr IPT, ProjLtr, Übungsleitende bzw. -leitender, DStLtr) beantragt die Akkreditierung (bzw. die Re-Akkreditierung gemäß Abschnitt 5.5.8) zeitgerecht vor der Nutzung bzw. Inbetriebnahme bei der DEUmilSAA. Er bzw. sie informiert darüber den CISO Rüstung bzw. wenn es sich um IT aus Infrastrukturmitteln handelt den CISO Infrastruktur.

5.5.5 Durchführung der Akkreditierung

531. Die Federführung für die Durchführung einer Akkreditierung liegt bei der DEUmilSAA. Diese trifft die Entscheidung über Umfang, Tiefe und Ablauf der Prüfung auf Basis nationaler und internationaler Vorgaben zur Akkreditierung.

532. Der Akkreditierungsprozess besteht aus folgenden Schritten:

- Prüfung der InfoSichhDok durch die DEUmilSAA (weitere Vorgaben zur InfoSichhDok sind dem Abschnitt 5.5.6 zu entnehmen),

- Überprüfung der in der InfoSichhDok beschriebenen InfoSichh-Maßnahmen auf ihre Umsetzung in der IT (die möglichen Ergebnisse sind dem Abschnitt 5.5.7 zu entnehmen) und
- Ausstellung einer Akkreditierungsbescheinigung gemäß Anlage 11.8.7 bzw. eines sogenannten „Statement of Compliance (SoC)“ gemäß Nr. 544 nach erfolgreich abgeschlossener Prüfung durch die DEUmilSAA.

533. Die Akkreditierungsprüfung erfolgt auf Basis eines vom Verantwortlichen für die IT vorzulegenden und von der DEUmilSAA zu genehmigenden Akkreditierungsplanes. Die Akkreditierungsprüfung beinhaltet die Mitzeichnung des entsprechenden InfoSichhK bzw. InfoSichhBef. Bei der Akkreditierung von IT gemäß Nr. 451 sind die im InfoSichhKDSt beschriebenen InfoSichh-Maßnahmen Gegenstand der Überprüfung.

534. Der bzw. die Verantwortliche für die IT koordiniert zeitgerecht mit der DEUmilSAA den Zeitraum der Prüfung. Die Durchführung der Prüfung erfolgt unter der Leitung der DEUmilSAA. Je nach Umfang und Tiefe der Prüfung wird die DEUmilSAA unterstützt durch ein Prüfteam des ZCSBw, das PZITSichhBw oder eine andere geeignete Institution.

535. Nach erfolgreich abgeschlossener Prüfung durch die DEUmilSAA erfolgt die Ausstellung einer Akkreditierungsbescheinigung gemäß Anlage 11.8.7 bzw. eines sogenannten „Statement of Compliance (SoC)[88]“ gemäß Nr. 544. Die möglichen Ergebnisse einer Akkreditierungsprüfung sind dem Abschnitt 5.5.7 zu entnehmen.

5.5.6 Dokumentation

5.5.6.1 Allgemeines

536. Voraussetzung einer erfolgreichen Akkreditierung von IT ist das bzw. der durch die DEUmilSAA mitgezeichnete InfoSichhK bzw. InfoSichhBef (siehe Abschnitt 6.3) und der Nachweis der Umsetzung der darin beschriebenen InfoSichh-Maßnahmen.

537. Bei der Dokumentation von NATO- / EU- oder multinationaler IT sind grundsätzlich die nachfolgend aufgeführten, von der NATO / EU gemäß NATO „INFOSEC Management Directive for Communication and Information Systems (CIS)“ (siehe Bezug Anlage 11.15 (lfdNr. 31), dort Abschnitt IV) multinational geforderten Dokumente in englischer Sprache zu erstellen. Dokumente für IT der Bw, mit denen Informationen mit NATO-Einstufung verarbeitet bzw. übertragen wird, können in Englisch oder Deutsch erstellt werden. Einzelheiten sind systembezogen mit der DEUmilSAA abzusprechen.

[88] Bestätigung der Einhaltung der Vorgaben der internationalen Organisation in der nationalen IT.

5.5.6.2 Community Security Requirement Statement (CSRS)

538. Ein CSRS wird zur Beschreibung von IT benötigt, das sich auf mehrere, örtlich getrennte Teilsysteme (z. B. ein WAN) erstreckt. Die InfoSichh der einzelnen Teile wird jeweils in einem SSRS (siehe Nr. 539) beschrieben.

5.5.6.3 System-Specific Security Requirement Statement (SSRS)

539. Das SSRS beschreibt die InfoSichh der zu akkreditierenden IT. Es beschreibt das System allgemein, die InfoSichh-Anforderungen, Sicherheitsumgebung (das IT-Umfeld), InfoSichh-Maßnahmen sowie die Administration der InfoSichh.

5.5.6.4 System Interconnection Security Requirement Statement (SISRS)

540. Das SISRS beschreibt die InfoSichh der Verbindung zweier Systeme. Es wird erforderlich, wenn die Beschreibung der InfoSichh der Systeme nicht im CSRS oder SSRS enthalten ist, z. B. bei Anbindung nach erfolgter Akkreditierung. Es enthält grundsätzlich die gleichen Angaben wie ein SSRS (siehe Nr. 539).

5.5.6.5 Security Operating Procedures (SecOps)

541. Die SecOps sind eine Beschreibung aller umgesetzten InfoSichh-Maßnahmen. Sie können unverändert zum InfoSichhKDSt genommen werden, es bedarf keiner Übersetzung.

5.5.6.6 Security Test & Evaluation Plan (ST&E Plan)

542. Der ST&E Plan beinhaltet die erforderlichen Prüfmaßnahmen, die zum Nachweis der Umsetzung der InfoSichh-Maßnahmen durchzuführen sind. Hierzu gehört die Überprüfung der personellen, infrastrukturellen, organisatorischen und technischen InfoSichh-Maßnahmen (einschl. der Maßnahmen zur Abstrahlsicherheit gemäß Zentraler Dienstvorschrift A-962/1 VS-NfD „Abstrahlsicherheit“ (siehe Bezug Anlage 11.15 (lfdNr. 21)).

5.5.7 Mögliche Ergebnisse einer Akkreditierung

5.5.7.1 Vollständige Akkreditierung (ATO = Approval to Operate)

543. Werden bei der Prüfung keine oder nur geringfügige Mängel bzgl. der InfoSichh festgestellt, so dass ausschließlich tolerierbare Risiken verbleiben, erstellt die DEUmilSAA eine Akkreditierungsbescheinigung über eine vollständige Akkreditierung an den Verantwortlichen bzw. die Verantwortliche für die IT (z. B. Ltr IPT / ProjLtr). Diese ist in der Regel maximal drei Jahre gültig.

544. Soll nationale IT an internationale IT angeschlossen werden, erstellt die DEUmilSAA gleichzeitig ein sogenanntes SoC, welches die Einhaltung der Vorgaben der internationalen Organisation in der nationalen IT bestätigt.

5.5.7.2 Eingeschränkte Akkreditierung (IATO = Interim Approval to Operate)

545. Werden bei der Prüfung Mängel bzgl. der InfoSichh festgestellt, die zu Risiken führen, die nur temporär aber nicht dauerhaft tolerierbar sind, kann die DEUmilSAA nur eine eingeschränkte, mit Auflagen versehene Akkreditierung ausstellen (Interim Approval to Operate, IATO).

546. Die Gültigkeit einer IATO wird durch die DEUmilSAA festgelegt. Sie beträgt maximal zwölf Monate und ist einmal um maximal zwölf Monate verlängerbar. Eine weitere Verlängerung der IATO durch die DEUmilSAA ist nur in Einzelfällen und nur mit Zustimmung des bzw. der CISOBw möglich. Innerhalb der Laufzeit dieser zweiten Verlängerung muss durch eine erneute Prüfung eine vollständige Akkreditierung erreicht werden, ansonsten ist gemäß Nr. 547 zu verfahren. Der Weiterbetrieb ohne eine Akkreditierung bzw. IATO durch die DEUmilSAA stellt ein InfoSichhVork dar (siehe Abschnitt 8).

5.5.7.3 Keine Akkreditierung

547. Werden bei der Prüfung Mängel bzgl. der InfoSichh festgestellt, die zu nicht tolerierbaren Risiken führen, wird keine Akkreditierung ausgesprochen. Im Prüfbericht werden nach Möglichkeit neben der Beschreibung der Mängel auch Vorschläge zu deren Abstellung aufgezeigt.

5.5.7.4 Genehmigung zum Testen (AfT = Approval for Testing)

548. Im Verlauf des Akkreditierungsprozesses kann die DEUmilSAA auf Anfrage eine Genehmigung zum Testen (Approval for Testing, AfT) von IT erteilen. Ein AfT kann erforderlich sein, wenn z. B. die noch nicht akkreditierte IT in Anbindung an bereits akkreditierte IT getestet werden soll.

549. Ein AfT ist zeitlich auf ein Minimum zu beschränken und ist grundsätzlich nur für zu verarbeitende / übertragende Informationen bis zur Einstufung VS-NfD (bzw. vergleichbar) zulässig. In begründeten Ausnahmefällen können nach Genehmigung der DEUmilSAA auch Informationen mit höheren Geheimhaltungsgraden verarbeitet und / oder übertragen werden.

5.5.8 Re-Akkreditierung

550. Eine Re-Akkreditierung wird erforderlich bei

- Änderung der Informationsstruktur (siehe Abschnitt 2.1), die eine Änderung der InfoSichh-Maßnahmen erforderlich macht,
- wesentlichen Änderungen in den InfoSichh-Anforderungen, die durch die umgesetzten InfoSichh-Maßnahmen nicht erfüllt werden,
- Änderung der Einsatzumgebung, z.B. aufgrund gravierender Änderungen der betrieblichen Umgebung bzw. des IT-Umfeldes,
- Änderung der technischen Konfiguration, z. B. bei gravierenden Änderungen der systemspezifischen Hardware oder Software (Betriebssoftware, InfoSichh-Software),
- neuen externen Anbindungen,

- Auftreten einer gravierenden InfoSichh-Lücke[89] (siehe Nr. 818),
- gravierenden Änderungen der systemspezifischen Hardware oder Software (Betriebssoftware, InfoSichh-Software),
- gravierenden Änderungen der betrieblichen Umgebung bzw. des IT-Umfeldes,
- negativen Erkenntnissen aus einer InfoSichhIn bezogen auf das akkreditierte System (siehe Nr. 715),
- Ablauf der Gültigkeit der Akkreditierungsbescheinigung sowie
- Entzug durch die DEUmilSAA (siehe Abschnitt 5.5.9).

551. Die verantwortlichen Rollenträgerinnen und Rollenträger in den Anwendungsbereichen (z.B. ProjLtr / DStLtr) melden Änderungen unter Vorlage des aktualisierten InfoSichhK zeitgerecht an die DEUmilSAA. Diese prüft die Dokumentation und entscheidet, ob und in welchem Umfang eine Re-Akkreditierung erforderlich ist. Die in Nutzung befindliche akkreditierte IT kann grundsätzlich in Abstimmung mit der DEUmilSAA (siehe hierzu auch Abschnitt 5.5.9) bis zum Abschluss der Re-Akkreditierung weiter betrieben werden.

5.5.9 Entzug der Akkreditierung

552. In folgenden Fällen kann die Akkreditierung durch die DEUmilSAA entzogen werden:

- bei nicht tolerierbaren Risiken der InfoSichh und / oder
- nach einem schwerwiegenden InfoSichhVork (Meldung gemäß Abschnitt 8.4) und Bewertung durch die DEUmilSAA und / oder
- nach entsprechender Intervention eines beteiligten Bündnispartners (z. B. Entzug der Akkreditierung durch einen Bündnispartner).

553. Die betroffene IT darf dann grundsätzlich nicht weiter betrieben werden. Der CISOBw ist zu beteiligen.

Sofern hierdurch Kernführungsfähigkeiten der Bw bzw. einsatzrelevante IT betroffen sind, greifen die Prozesse gemäß A-960/15 „IT-Krisenmanagement in der Bundeswehr“ (siehe Bezug Anlage 11.15 (lfdNr. 47)).

[89] D. h. die Vertraulichkeit von Informationen der Einstufung VS - VERTRAULICH oder höher, einschließlich vergleichbarer NATO- / EU-Einstufungen bzw. Einstufungen anderer Nationen, sonstiger überstaatlicher Organisationen oder „MISSION“) ist gefährdet. Im Rahmen des IT-Grundschutzes und der Miltärischen Sicherheit wird der Begriff Sicherheitslücke genutzt.

5.6 Freigabe zur Nutzung

5.6.1 Allgemeines

554. Jede IT (zur Begriffsbestimmung „Informationstechnik“ siehe Anlage 11.11) ist aus Sicht der InfoSichh freizugeben. Diese Freigabe erteilt

- vor der ersten Nutzung der bzw. die Ltr IPT / ProjLtr oder der bzw. die Verantwortliche für die Infra-Maßnahme oder der bzw. die Verantwortliche von Vorhaben der Wehrtechnischen Forschung & Technologie sowie sonstiger Forschungsvorhaben, Erprobungen, Truppenversuchen und Wehrtechnischen Aufträgen bzw. Vorhaben der WissUstg NT für die gesamte IT des Projektes / Vorhabens (**verfahrensbezogene Freigabe** gemäß Abschnitt 5.6.2) und im Anschluss
- vor der ersten Nutzung für die IT seines bzw. ihres Zuständigkeitsbereiches der bzw. die DStLtr oder der bzw. die KtgtFhr ggf. in Abstimmung mit dem bzw. der Ltr der zuständigen IT-Btrb(Fü)Einr (**operationelle Freigabe** gemäß Abschnitt 5.6.3) und
- in der Nutzung der bzw. die zuständige Ltr IPT / ProjLtr (**Freigabe in der Nutzung**) nach Vorliegen der Gründe gemäß Abschnitt 5.6.4

mit dem Musterformular aus der Anlage 11.8.1.

555. Mit diesen Freigaben wird bestätigt, dass die IT selbst sowie das IT-Umfeld die geforderten InfoSichh-bezogenen Eigenschaften aufweist, d. h. alle im jeweiligen InfoSichhKProj bzw. InfoSichhKFW geforderten InfoSichh-Maßnahmen wurden durch die zuständigen Rollenträgerinnen und Rollenträger umgesetzt.

556. Verantwortlich für die Umsetzung der

- **technischen** InfoSichh-Maßnahmen ist der bzw. die Ltr IPT / ProjLtr oder der bzw. die Verantwortliche für die Infra-Maßnahme oder der bzw. die Verantwortliche von Vorhaben der Wehrtechnischen Forschung & Technologie sowie sonstiger Forschungsvorhaben, Erprobungen, Truppenversuchen und Wehrtechnischen Aufträgen bzw. Vorhaben der WissUstg NT und
- **personellen**, **organisatorischen** und **infrastrukturellen** InfoSichh-Maßnahmen ist der bzw. die DStLtr / KtgtFhr jeweils für den Anteil der in seinem / ihrem Zuständigkeitsbereich genutzten IT.

557. Freigaben sind durch die zuständigen Rollenträgerinnen und Rollenträger grundsätzlich unbefristet zu erteilen. Unter bestimmten Voraussetzungen kann eine **vorläufige Freigabe** erteilt werden (siehe Abschnitt 5.6.5). Ohne Freigabe darf IT nicht betrieben werden.

558. Soll die IT als Ganzes oder in Teilbereichen nicht mehr genutzt werden, sind die jeweiligen Freigaben durch die zuständigen Rollenträgerinnen und Rollenträger (siehe Nr. 554) aufzuheben.

559. Wird während der Nutzung von IT festgestellt, dass

- geforderte InfoSichh-Maßnahmen nicht umgesetzt sind oder

- InfoSichh-Lücken (siehe auch InfoSichhVork in Abschnitt 8, insbesondere Nr. 806) bestehen,

sind die zuständigen Rollenträgerinnen und Rollenträger (siehe Nr. 554) sofort über den Sachverhalt zu informieren. Sie entscheiden anhand einer Risikobewertung, ob die Freigabe eingeschränkt (vorläufige Freigabe gemäß Abschnitt 5.6.5) oder aufgehoben werden muss.

Ergänzend ist die DEUmilSAA zu informieren.

560. Freigaben sind aufzuheben, wenn

- die Akkreditierung durch die DEUmilSAA entzogen wurde (siehe Abschnitt 5.5.9) oder
- schwere Mängel der technischen InfoSichh identifiziert wurden und das verbleibende Risiko nicht tolerierbar ist.

5.6.2 Verfahrensbezogene Freigabe (P, V, O, S, F, W,)

561. Die verfahrensbezogene **Freigabe** ist durch den bzw. die Ltr IPT / ProjLtr oder den bzw. die Verantwortliche für die Infra-Maßnahme nach Durchführung entsprechender Prüfungen vor Nutzungsbeginn des Projektes bzw. Vorhabens mit dem Musterformular gemäß Anlage 11.8.1 zu erteilen. Für CPM-Projekte erfolgt die verfahrensbezogene Freigabe in Verbindung mit der „Genehmigung zur Nutzung – GeNu“, die auch eine Aussage zur InfoSichh (Stand InfoSichhKProj, Umsetzung der InfoSichh-Maßnahmen, Akkreditierung) enthalten muss.

Für Vorhaben der wehrtechnische Forschung & Technologie sowie sonstige Forschungsvorhaben, Erprobungen, Truppenversuche und Wehrtechnische Aufträge oder Vorhaben der WissUstg NT ist – wenn ein InfoSichhKFW gemäß Nr. 408 bzw. Nr. 410 zu erstellen ist – ebenfalls eine verfahrensbezogene Freigabe, wie oben beschrieben, durch den Verantwortlichen bzw. die Verantwortliche für das Vorhaben zu erteilen.

562. Voraussetzungen für eine verfahrensbezogene Freigabe sind

- das Vorliegen eines aktuellen und erlassenen InfoSichhK,
- bei Verarbeitung von PersDat das Vorliegen eines aktuellen und erlassenen Datenschutz-Konzeptes, der Sammelerfassung im Verfahrensverzeichnis und erforderlichenfalls einer Datenschutz-Folgenabschätzung, welches in der Verantwortung des bzw. der zuständigen ADSB beigestellt wird,
- die Umsetzung aller darin geforderten technischen InfoSichh-Maßnahmen sowie
- der positive Abschluss einer **Akkreditierung** gemäß Abschnitt 5.5 (d. h. eine gültige Akkreditierungsbescheinigung gemäß Anlage 11.8.7 liegt vor).

563. Die jeweils zuständigen ISB (ISBProj, ISBFW) prüfen die Umsetzung dieser InfoSichh-Maßnahmen im Rahmen der Integrierten Nachweisführung oder vergleichbarer Prüfungen. Dazu können Prüfungen und Bewertungen beim PZITSichhBw unter Beteiligung CISO Rüstung bzw. CISO Infrastruktur beantragt werden. Bei positivem Ergebnis der Prüfung empfehlen sie den jeweils

zuständigen Rollenträgerinnen und Rollenträgern (vgl. Abschnitt 4.1) die verfahrensbezogene Freigabe.

564. Bei Abnahme- und Einsatzprüfungen von Projekten, die einen sehr hohen Schutzbedarf bezogen auf die Vertraulichkeit von VS haben (siehe Abschnitt 2.1.3), wirkt das BAMAD im Rahmen seines gesetzlichen Auftrages zum Geheimschutz mit (siehe Bezug Anlage 11.15 (lfdNr. 4)). Anträge hierzu sind an das BAMAD[90] unter nachrichtlicher Beteiligung der DEUmilSAA zu richten.

565. Bei Einschränkungen hinsichtlich der Umsetzung notwendiger InfoSichh-Maßnahmen und daraus resultierenden nicht dauerhaft tolerierbaren Risiken kann eine vorläufige Freigabe gemäß Abschnitt 5.6.5 erteilt werden.

566. Die Ltr IPT / ProjLtr oder der bzw. die Verantwortliche für die Infra-Maßnahme oder der bzw. die Verantwortliche Vorhaben der Wehrtechnischen Forschung & Technologie sowie sonstiger Forschungsvorhaben, Erprobungen, Truppenversuchen und Wehrtechnischen Aufträgen bzw. Vorhaben der WissUstg NT stellen den DStLtr / KtgtFhr den Freigabebescheid als Voraussetzung der operationellen Freigabe vor Beginn der Nutzung zur Verfügung.

567. Wird eine verfahrensbezogene Freigabe aufgehoben (siehe Nr. 560), sind neben den DStLtr / KtgtFhr auch CISOBw, DEUmilSAA, CISO Rüstung und CISO Infrastruktur zu informieren.

568. Die der Freigabe zugrundeliegende Konfiguration ist durch die Ltr IPT / ProjLtr, die Verantwortlichen für die Infra-Maßnahme oder die Verantwortlichen für Vorhaben der wehrtechnischen Forschung & Technologie sowie sonstige Forschungsvorhaben, Erprobungen, Truppenversuche und Wehrtechnische Aufträge oder für Vorhaben der WissUstg NT unter Konfigurationskontrolle zu nehmen. Abweichungen vom freigegebenen Konfigurationsstand unterliegen einer erneuten Freigabe (Freigabe in der Nutzung gemäß Abschnitt 5.6.4).

5.6.3 Operationelle Freigabe (D, E)

569. Der bzw. die zuständige DStLtr (siehe Abschnitt 4.8) oder KtgtFhr (siehe Abschnitt 4.9) erteilt vor Beginn der Nutzung von IT in seiner bzw. ihrer DSt / seinem bzw. ihrem EinsKtgt die **operationelle Freigabe** mit dem Musterformular gemäß Anlage 11.8.1.

570. Voraussetzungen für eine operationelle Freigabe sind

- das Vorliegen aktueller und erlassener InfoSichhKProj oder InfoSichhKFW,
- die Dokumentation aller darin geforderten dienststellenbezogenen InfoSichh-Maßnahmen im dienststellen- / einsatzbezogenen InfoSichhK (siehe Abschnitt 6.3.3),
- die Umsetzung aller darin geforderten personellen, infrastrukturellen und organisatorischen InfoSichh-Maßnahmen in der DSt / im EinsKtgt,

[90] MADAmtEingang@bundeswehr.org

- die Freigabe zur Nutzung durch
  - + den bzw. die Ltr IPT / ProjLtr (siehe Abschnitt 5.6.2) mit dem CPM-Dokument „Genehmigung zur Nutzung – GeNu“ gemäß CPM (siehe Bezug Anlage 11.15 (lfdNr. 12)) bzw. dem Dokument gemäß Anlage 11.8.1 oder
  - + den bzw. die Verantwortliche für die Infra-Maßnahme mit dem Dokument gemäß Anlage 11.8.1 oder
  - + den bzw. die Verantwortliche von Projekten bzw. Vorhaben der Wehrtechnischen Forschung & Technologie sowie sonstiger Forschungsvorhaben, Erprobungen, Truppenversuchen und Wehrtechnischen Aufträgen bzw. Vorhaben der WissUstg NT mit dem Dokument gemäß Anlage 11.8.1 sowie
- bei Bedarf der positive Abschluss einer **Akkreditierung** gemäß Abschnitt 5.5 (bzw. Re-Akkreditierung gemäß Abschnitt 5.5.8) (d. h. eine gültige Akkreditierungsbescheinigung gemäß Anlage 11.8.7 liegt vor).

571. Die ISBDSt / ISB i.E. prüfen die Umsetzung der personellen, infrastrukturellen und organisatorischen InfoSichh-Maßnahmen und empfehlen dem bzw. der DStLtr oder KtgtFhr bei positivem Ergebnis die operationelle Freigabe. Bei Einschränkungen hinsichtlich der Umsetzung notwendiger InfoSichh-Maßnahmen und daraus resultierenden nicht dauerhaft tolerierbaren Risiken kann eine vorläufige Freigabe gemäß Abschnitt 5.6.5 erteilt werden.

572. Wird eine operationelle Freigabe aufgehoben (siehe Nr. 560), sind neben dem bzw. der betroffenen ProjLtr auch CISOBw, DEUmilSAA, CISO Rüstung und CISO Infrastruktur zu informieren.

573. Betreibt die DSt / der EinsStO selber IT, ist die Umsetzung der für den IT-Betrieb relevanten technischen InfoSichh-Maßnahmen durch die DSt / das EinsKtgt ebenfalls zu prüfen.

5.6.4 Freigabe in der Nutzung (P, V, O, S, F, W, D, E)

574. In der Nutzung ist die IT aus verfahrensbezogener und im Anschluss daran aus operationeller Sicht (siehe Abschnitte 5.6.2 und 5.6.3) erneut freizugeben, wenn

- eine Fortschreibung des InfoSichhKProj (siehe Abschnitt 6.3.2) vorgenommen wurde,
- eine vorläufige (siehe Abschnitt 5.6.5) in eine unbefristete Freigabe gewandelt werden soll,
- die verfahrensbezogene Freigabe (siehe Abschnitt 5.6.2) aktualisiert wurde oder
- erhebliche Änderungen / Ergänzungen an der IT (z. B. an der Hardware- oder Softwarekonfiguration, d. h. Änderungen des durch den bzw. die ProjLtr freigegebenen Konfigurationsstandes) vorgenommen wurden.

575. Ggf. muss eine erneute **Akkreditierung** (Re-Akkreditierung gemäß Abschnitt 5.5.8) erfolgen.

576. Die Ltr IPT / ProjLtr, die Verantwortlichen für die Infra-Maßnahme oder die Verantwortlichen für Vorhaben der Wehrtechnischen Forschung & Technologie sowie sonstiger Forschungsvorhaben,

Erprobungen, Truppenversuchen und Wehrtechnischen Aufträgen bzw. Vorhaben der WissUstg NT stellen den DStLtr / KtgtFhr den Freigabebescheid als Voraussetzung der erneuten operationellen Freigabe vor Beginn der Inbetriebnahme der Änderung zur Verfügung.

5.6.5 Vorläufige Freigabe (P, V, O, S, F, W, D, E)

577. Die zuständigen Rollenträgerinnen und Rollenträger (siehe Nr. 554) können nach einer Risikobewertung eine zeitlich befristete **vorläufige Freigabe** erteilen, wenn

- die Voraussetzungen für eine unbefristete Freigabe gemäß der Abschnitte 5.6.2, 5.6.3 oder 5.6.4 nicht erfüllt werden **und**
- das verbleibende Risiko temporär tolerierbar ist und
- die DEUmilSAA gemäß Abschnitt 5.5.7.2 bei Bedarf (Nr. 520) zumindest eine eingeschränkte Akkreditierung erteilt bzw. der vorläufigen Freigabe unter Auflagen zugestimmt hat.

Ergibt die Bewertung, dass die Risiken auch temporär nicht tolerierbar sind, darf keine vorläufige Freigabe zur Nutzung erteilt werden.

578. DSt oder EinsKtgt informieren umgehend die betroffenen Ltr IPT / ProjLtr, die Verantwortlichen für die Infra-Maßnahme oder die Verantwortlichen für Vorhaben der Wehrtechnischen Forschung & Technologie sowie sonstiger Forschungsvorhaben, Erprobungen, Truppenversuchen und Wehrtechnischen Aufträgen bzw. Vorhaben der WissUstg NT über den zuständigen bzw. die zuständige ISBOrgBer oder ISBEinsatz unter Beteiligung CISOBw, wenn sie eine vorläufige Freigabe oder keine Freigabe wegen nicht tolerierbarer Risiken erteilt haben.

Ltr IPT / ProjLtr, die Verantwortlichen für die Infra-Maßnahme oder die Verantwortlichen für Vorhaben der Wehrtechnischen Forschung & Technologie sowie sonstiger Forschungsvorhaben, Erprobungen, Truppenversuchen und Wehrtechnischen Aufträgen bzw. Vorhaben der WissUstg NT informieren umgehend alle betroffenen DSt / EinsKtgt sowie CISOBw und die DEUmilSAA, wenn sie wegen nicht tolerierbarer Risiken keine vorläufige Freigabe erteilen können oder eine vorläufige Freigabe aufheben (siehe Nr. 560).

579. Die vorläufige Freigabe und ggf. damit verbundene Auflagen sind im betreffenden InfoSichhK und im Freigabedokument (siehe Anlage 11.8.1) zu dokumentieren. Sie darf grundsätzlich für maximal ein Jahr erteilt werden. Im Ausnahmefall ist eine Verlängerung der vorläufigen Freigabe nach Abstimmung mit CISOBw um max. ein weiteres Jahr zulässig.

580. Die zuständigen Rollenträgerinnen und Rollenträger (siehe Nr. 554) leiten unverzüglich alle erforderlichen Maßnahmen ein, um die Voraussetzungen für eine unbefristete Freigabe zu schaffen. Eine unbefristete Freigabe darf erst nach erneuter Überprüfung und Mängelabstellung erteilt werden.

5.7 Bestellung von Informationssicherheitsbeauftragten und Informationssicherheitsgehilfen

5.7.1 Allgemeines

581. Zum bzw. zur ISB sind grundsätzlich Offiziere oder vglb. Beamte bzw. Beamtinnen / Tarifbeschäftigte zu bestellen.

582. In DSt oder EinsKtgt / EinsStO ab der Ebene Brigade / Flottille / Bundesoberbehörde **oder** die eine Kryptoverwaltung betreiben **oder** die IT nutzen bzw. betreiben, die Informationen verarbeitet oder überträgt, die in mindestens einem Grundwert den **Schutzbedarf „sehr hoch“** hat[91], müssen ein hauptamtlicher[92] bzw. eine hauptamtliche ISBDSt oder ISB i.E. **und** ein hauptamtlicher Stellvertreter bzw. eine Stellvertreterin bestellt werden[93]. Dies gilt ebenso für solche DSt, deren IT-Landschaft wesentlich durch technisch-wissenschaftliche IT und Anwendungen geprägt ist. In DSt bzw. EinsKtgt / EinsStO mit einer Kryptoverwaltung sind grundsätzlich Offiziere oder vglb. Beamte / Tarifbeschäftigte zu bestellen. Ist in DSt bzw. EinsKtgt / EinsStO mit einer Kryptoverwaltung die Bestellung von Offizieren oder vergleichbar (siehe Nr. 581) aufgrund der dortigen Dienstpostenbesetzung nicht möglich, kann der bzw. die CISOBw eine Ausnahmegenehmigung für die Bestellung von Portepee-Unteroffizieren oder vglb. Beamte / Tarifbeschäftigte im Rahmen der NATO-Vorgaben (siehe Bezug Anlage 11.15 (lfdNr. 33), dort Chapter 3, Section III) erteilen.

583. In DSt oder EinsKtgt / EinsStO, die keine Kryptoverwaltung betreiben, bestellt der bzw. die DStLtr oder KtgtFhr / Kdr EinsStO grundsätzlich einen bzw. eine ISB für die Dienststelle (ISBDSt, siehe Abschnitt 3.2.3) sowie einen stellvertretenden bzw. eine stellvertretende ISBDSt, sofern er bzw. sie die Aufgaben nicht selbst übernimmt. Die Bestellung von Portepee-Unteroffizieren oder Beamten bzw. Beamtinnen / Arbeitnehmern bzw. Arbeitnehmerinnen in vergleichbarer Besoldungs- / Entgeltgruppe (TVöD) ist zulässig, sofern kein Personal nach Nr. 581 zur Verfügung steht.

584. Eine zusätzliche bzw. parallele Verwendung von InfoSichh-Personal in Bereichen mit Administratortätigkeiten oder mit Veranlassung solcher Tätigkeiten (z.B. als Bestellberechtigter für IT-Services oder Zugriffsrechte), die Rechte beinhalten, die zu einer Selbstkontrolle führen, ist nicht zulässig. Dies ist bei der Festlegung des Umfanges des IT-Personals zu berücksichtigen.

585. Ist die Position des bzw. der ISBDSt / ISB i.E. und / oder dessen Vertreter bzw. deren Vertreterin in DSt / EinsKtgt / EinsStO mit Verpflichtung zur Bestellung eines bzw. einer hauptamtlichen ISB nicht besetzt und können diese z. B. aufgrund fehlender Voraussetzungen nicht sofort

[91] Ist mindestens eines der drei Kriterien erfüllt, ist ein bzw. eine hauptamtliche ISB und ein hauptamtlicher Stellvertreter bzw. eine hauptamtliche Stellvertreterin zu bestellen.
[92] Hauptamtlich im Sinne dieser Zentralen Dienstvorschrift bedeutet, dass eine der Hauptaufgaben im ODP / ATK die Wahrnehmung der Aufgabe InfoSichh sein soll.
[93] Gilt nicht für die OrgBer Militärseelsorge und Rechtspflege.

wiederbesetzt werden, so ist durch den bzw. die DStLtr oder KtgtFhr / Kdr EinsStO bei dem bzw. der CISOBw auf dem Dienstweg ein Antrag auf Ausnahmegenehmigung zu stellen und der bzw. die DStLtr oder KtgtFhr / Kdr EinsStO hat die Aufgaben bis zur Bestellung eines bzw. einer ISB selbst wahrzunehmen. Ausnahmegenehmigungen für DSt oder EinsKtgt / EinsStO, die eine Kryptoverwaltung betreiben, sind unzulässig[94].

586. Zur Gewährleistung einer unabhängigen Überwachung ist Nr. 301 zu beachten. Die ISB haben in der Wahrnehmung ihrer Aufgaben ein direktes Vortragsrecht bei dem bzw. der für die InfoSichh verantwortlichen Vorgesetzten (siehe Abschnitt 5.7.4).

5.7.2 Voraussetzungen (F, W, P, V, O, D, E, Ü)

587. Aufgaben der InfoSichh dürfen nur von qualifiziertem Personal wahrgenommen werden. ISBOrgBer, ISBEinsatz, ISBDSt, ISBBtrb, ISBProj, ISBFW, ISB i.E., ISBÜb und ISBGBW sowie deren Vertreterin bzw. Vertreter und Gehilfen (siehe Nr. 450) dürfen erst bestellt werden, wenn

- sie an der entsprechenden Ausbildung gemäß Abschnitt 10.1 zum / zur ISB bzw. InfoSichhGeh mit Erfolg teilgenommen haben,
- die Ermächtigung zum Zugang zu VS (soweit erforderlich) nach Zentraler Dienstvorschrift A-1130/2 VS-NfD „Militärische Sicherheit in der Bundeswehr – Verschlusssachen“, Abschnitt 16.1 „Ermächtigungen“ (siehe Bezug Anlage 11.15 (lfdNr. 15)) erteilt wurde,
- eine Verpflichtungserklärung gemäß Anlage 11.8.6 unterzeichnet ist und
- eine Kryptobescheinigung gemäß Zentraler Dienstvorschrift A-1130/2 VS-NfD „Militärische Sicherheit in der Bundeswehr - Verschlusssachen“, Abschnitt 16.3, Nr. 1607 (siehe Bezug Anlage 11.15, lfdNr. 15) soweit erforderlich[95] vorliegt.

588. War der bzw. die vorgesehene ISB länger als fünf Jahre nicht als InfoSichh-Personal[96] eingesetzt, hat er bzw. sie vor einer erneuten Bestellung wieder an einem Lehrgang für ISB (siehe Abschnitt 10.1) erfolgreich teilzunehmen.

[94] Abweichend dazu kann auf dem Dienstweg für schwimmende Einheiten und Einsatzkontingente i.E. eine Ausnahmegenehmigung beim CISOBw beantragt werden.
[95] Erforderlich ist diese auch, wenn der bzw. die ISB im unmittelbaren Bereich zwar keine Kryptomittelverwaltung zu kontrollieren, diese Kontrollen aber im unterstellten Bereich durchzuführen hat.
[96] Oder bisher: IT-Sicherheitspersonal

5.7.3 Ausnahmen für Informationssicherheitsbeauftragte Organisationsbereich / Einsatz / Dienststelle / Betrieb / Projekt / Forschung und Wissenschaft / Geheimschutzbetreute Wirtschaft, Übung und Informationssicherheitsgehilfen (F, W, P, V, O, D, E, Ü)

589. Sind für den Zeitpunkt der Aufgabenübernahme noch nicht alle Bestellungsvoraussetzungen gegeben, ist für ISB vorab eine Ausnahmegenehmigung für die Wahrnehmung der Aufgaben[97] bei dem bzw. der CISOBw auf dem Dienstweg einzuholen. Ausnahmegenehmigungen für InfoSichhGeh erteilen die ISBOrgBer.

590. Ausnahmegenehmigungen sind befristet zu erteilen und dürfen nur erteilt werden, wenn

- entsprechende Grundkenntnisse der InfoSichh bei dem betreffenden Personal vorliegen,
- die Voraussetzungen gemäß Nr. 587, mit Ausnahme der Ausbildung zum bzw. zur ISB, vorliegen,
- eine Unterstützung durch den bzw. der ISB der vorgesetzten DSt möglich ist[98] und
- mindestens eine Lehrgangsanforderung / -beantragung für den fehlenden Lehrgang nachgewiesen wird.

591. Genehmigte Ausnahmen sind durch die Bestellenden mit dem entsprechend ausgefüllten Bestellungsvordruck gemäß Anlage 11.8.4 zu dokumentieren.

592. CISOBw führt aktuelle Übersichten über Ausnahmegenehmigungen für ISB.

5.7.4 Zuständigkeiten für Bestellungen (F, W, P, V, O, D, E, Ü)

593. Die Zuständigkeiten für die Bestellung von ISB sind zusammenfassend folgender Abb. 10 zu entnehmen:

Funktion	**Bestellung durch**	**hauptamtlich**[92]
CISO Ressort	Staatssekretär / Staatssekretärin für Planung, Ausrüstung, Informationstechnik und Nutzung	Nein
CISOBw	Staatssekretär / Staatssekretärin für Planung, Ausrüstung, Informationstechnik und Nutzung	Nein
ISBBMVg	Staatssekretär / Staatssekretärin für Administration	Ja
ISBOrgBer	Regelung durch die OrgBer	Ja
ISBMAD	Präsident / Präsidentin / Amtschef / Amts-chefin des BAMAD	Ja

[97] Ausgenommen ist die Entlastung des Kryptoverwalters bzw. der Kryptoverwalterin – diese Aufgabe hat der bzw. die ISB der vorgesetzten DSt durchzuführen.
[98] Dies gilt nur für ISBDSt und ISB i.E.

Funktion	**Bestellung durch**	**hauptamtlich**[92]
CISO Rüstung	Präsident / Präsidentin BAAINBw	Ja
CISO Infrastruktur	Präsident / Präsidentin BAIUDBw	Ja
ISBDSt	DStLtr[99]	fallbezogen gemäß Abschnitt 5.7.1
ISBGBW	Kdr ZCSBw	Ja
ISBProj	Ltr IPT / ProjLtr	projektbezogen
ISBFW	Ltr des Vorhabens	vorhabenbezogen
ISBEinsatz	Befehlshaber / Befehlshaberin EinsFüKdoBw	Ja
ISB i.E.	KtgtFhr / Kdr EinsStO	einsatzbezogen[100]
ISBÜb	DStLtr übungsleitende DSt	übungsbezogen[101]
ISBBtrb	DStLtr bzw. Ltr der jeweiligen IT-Betr(Fü)Einr	Ja[102]

Abb. 10: Bestellung von CISO und ISB

5.7.5 Dokumentation (F, W, P, V, D, E, Ü)

594. Die Bestellung zum bzw. zur ISB oder InfoSichhGeh erfolgt schriftlich mit den Formularen gemäß Anlage 11.8.4 und für ISBDSt / ISB i.E. zusätzlich in Verbindung mit der Dienstanweisung gemäß Anlage 11.8.5.

595. Eine Ausfertigung der Bestellung des bzw. der ISB oder InfoSichhGeh erhalten

- der bzw. die CISOBw,
- das ZCSBw,
- der bzw. die zuständige ISBOrgBer,
- der bzw. die ISB der vorgesetzten DSt / ISBEinsatz für ISB i.E. (InfoSichhDok),
- der bzw. die Sicherheitsbeauftragte der DSt / des EinsFüKdoBw (Absicherungshandakte),
- der bzw. die ISBDSt / ISB i.E. (InfoSichhDok),
- von DSt mit einer Kryptoverwaltung die Kryptobereichsleitstelle der Teilstreitkraft und
- der Kryptoverwalter bzw. die Kryptoverwalterin (Handakte).

[99] Dies kann bei Bestellung eines bzw. einer ISBDSt für mehrere DSt gemäß Abschnitt 4.8, Nr. 449 auch der bzw. die DStLtr der nächsten gemeinsamen DSt sein.
[100] kann in Personalunion mit dem bzw. der ISBDSt der kontingentführenden DSt bestellt werden
[101] kann in Personalunion mit dem bzw. der ISBDSt der übungsleitenden DSt bestellt werden
[102] In IT-BtrbEinr kann der bzw. die ISBBtrb in Personalunion mit dem bzw. der ISBDSt der betreibenden DSt bestellt werden.

596. Die Unterlagen über die Bestellung des bzw. der ISB und deren Stellvertreter oder InfoSichhGeh sind vom bzw. von der ISB der vorgesetzten DSt und vom bzw. von der Sicherheitsbeauftragten der DSt nach deren Aufhebung fünf Jahre aufzubewahren. Die Bestellungsunterlagen für ISB i.E. sind nach Auflösung der EinsKtgt im EinsFüKdoBw für die Dauer von fünf Jahren nachzuweisen. Die Frist beginnt mit der Aufhebung der Bestellung. Die Bestellungsunterlagen sind nach Ablauf der Aufbewahrungsfrist gemäß Zentraler Dienstvorschrift A-1130/2 VS-NfD „Militärische Sicherheit in der Bundeswehr – Verschlusssachen“ (siehe Bezug Anlage 11.15 (lfdNr. 15)) zu vernichten.

6 Dokumentation

6.1 Informationssicherheitsdokumentation

6.1.1 Dienststellen- / einsatzbezogene Informationssicherheitsdokumentation (D, E)

601. Der bzw. die ISBDSt / ISB i.E. führt eine aktuelle Informationssicherheitsdokumentation (InfoSichhDok) für die DSt bzw. das EinsKtgt bzw. den EinsStO. Diese enthält:

- die für die DSt / das EinsKtgt / den EinsStO relevanten Auszüge der InfoSichhKProj[103] und der InfoSichhKFW (in der Regel die durch die DSt / das EinsKtgt / den EinsStO umzusetzenden InfoSichh-Maßnahmen der InfoSichhK),
- das InfoSichhK der DSt / des EinsKtgt / des EinsStO,
- die InfoSichhBef für Übungen der DSt für noch nicht abgeschlossene InfoSichhVork, die während der Übung auftraten,
- die InfoSichhIn-Berichte mindestens der letzten beiden InfoSichhIn sowie die Kontroll- / Prüfberichte sowie ggf. die Dokumentation der Mängelbeseitigung,
- sonstige für die DSt / das EinsKtgt / den EinsStO relevante Berichte und Vorgänge zur InfoSichh,
- die für die DSt / das EinsKtgt / den EinsStO relevanten zentralen und dezentralen Vorgaben und Hinweise zur InfoSichh (vgl. Nr. 315), z. B. InfoSichh-Weisungen des bzw. der CISOBw oder Vorgaben, Hinweise und Handlungsanweisungen des bzw. der zuständigen ISBOrgBer bzw. Weisungen / Hinweise des bzw. der ISBEinsatz,
- alle für die DSt / das EinsKtgt / den EinsStO relevanten aktuellen Freigaben zur Nutzung (siehe Abschnitt 5.6) mit den erforderlichen Akkreditierungsbescheinigungen gemäß Anlage 11.8.7,
- Bestellungen des InfoSichh-Personals für den eigenen Zuständigkeitsbereich,
- Verpflichtungserklärungen für den eigenen Zuständigkeitsbereich,
- Kryptoermächtigungen für den eigenen Zuständigkeitsbereich,
- Ausnahmegenehmigungen für
  - + Bestellungen,
  - + Netzübergänge (siehe Anlage 11.2.11) sowie
  - + Nutzung privater IT zu dienstlichen Zwecken (siehe Anlage 11.2.1, Nr. 3) und
- eine Übersicht über die gemeldeten InfoSichhVork der letzten drei Jahre.

602. Ein Muster für die InfoSichhDok ist Anlage 11.8.2 zu entnehmen.

[103] Soweit vorhanden als importierbare Datei für das Grundschutzwerkzeug

603. Die InfoSichhDok ist bei Auflösung / Umstrukturierung an die im Organisationsbefehl zur Auflösung / Umstrukturierung vorgesehene Dienststelle zu übergeben. Sofern keine Regelung getroffen wurde, ist die Entscheidung CISOBw einzuholen.

6.1.2 Projekt- / vorhabenbezogene Informationssicherheitsdokumentation (F, W, P, V, O, S)

604. Der bzw. die ISB in den Anwendungsbereichen (F, W, P, V, O und S gemäß Nr. 402) führt eine aktuelle InfoSichhDok für sein Projekt bzw. Vorhaben. Diese enthält:

- das InfoSichhK mit den umzusetzenden Maßnahmen,
- die InfoSichhIn-Berichte mindestens der letzten beiden InfoSichhIn sowie die Kontroll- / Prüfberichte sowie ggf. die Dokumentation der Mängelbeseitigung,
- Abnahmeprotokolle der technischen InfoSichh-Maßnahmen,
- sonstige für das Projekt bzw. Vorhaben relevante Berichte und Vorgänge zur InfoSichh,
- für die InfoSichh relevante Konfigurationsunterlagen,
- die für das Projekt bzw. Vorhaben relevanten zentralen und dezentralen Vorgaben und Hinweise zur InfoSichh (vgl. Nr. 315), z. B. InfoSichh-Weisungen des bzw. der CISOBw oder Vorgaben, Hinweise und Handlungsanweisungen des bzw. der zuständigen ISBBtrb,
- alle für das Projekt bzw. Vorhaben relevanten aktuellen Freigaben; für Projekte nach CPM in Verbindung mit der GeNu (siehe Abschnitt 5.6),
- erforderliche Akkreditierungsbescheinigungen gemäß Anlage 11.8.7,
- für eingesetzte InfoSichh-Produkte die relevanten aktuellen Zulassungen bzw. Anerkennungen,
- Bestellung des InfoSichh-Personals für den eigenen Zuständigkeitsbereich,
- Verpflichtungserklärungen für den eigenen Zuständigkeitsbereich,
- Kryptoermächtigungen für den eigenen Zuständigkeitsbereich,
- eine Übersicht über die gemeldeten InfoSichhVork,
- Bei IT-Betrieb oder Aufgabenübernahme durch Dritte (Anwendungsbereich O) die für die InfoSichh relevanten Anteile des Vertrages sowie eine Liste der relevanten Ansprechpartner für InfoSichh beim Auftragnehmer (AN), das Dokument mit der Zusicherung zur Überprüfung von InfoSichh-Maßnahmen beim AN und die Dokumentation der durchgeführten Überprüfungen.

6.2 Risikoanalyse – Dokumentation des verbliebenen Risikos

605. Die Durchführung einer Ergänzenden Sicherheitsanalyse mit folgender Risikoanalyse (vgl. Anlage 11.1.10) im Rahmen der Erstellung oder Fortschreibung der InfoSichhK (z.B. Projekt, DSt / EinsKtgt) bzw. der Umsetzung der InfoSichh-Maßnahmen ist in Anlehnung an den IT-Grundschutz des BSI immer dann erforderlich, wenn

- hoher oder sehr hoher Schutzbedarf für mindestens einen der Grundwerte (Nr. 111) festgestellt wurde (siehe Nr. 207) und die in dieser Zentralen Dienstvorschrift hierfür festgelegten InfoSichh-Anforderungen und -Maßnahmen (siehe Anlage 11.3.2) im IT-Grundschutzkatalog der Bw (siehe Anlage 11.1.2) nicht ausreichen bzw. für den entsprechenden Grundwert in dieser Vorschrift keine InfoSichh-Anforderungen bzw. -Maßnahmen festgelegt sind,
- bei Relevanz der Gewährleistungsziele (siehe Nr. 112) in dieser Zentralen Dienstvorschrift keine InfoSichh-Anforderungen bzw. -Maßnahmen festgelegt sind,
- die betrachtete IT erkennbare bzw. bekannte Schwachstellen enthält, die das Wirksamwerden einer Gefährdung besonders begünstigen bzw. die weitere Gefährdungen beinhalten, die im Baustein gemäß IT-Grundschutz nicht berücksichtigt sind,
- mit den existierenden Bausteinen des IT-Grundschutzes des BSI und den ergänzenden InfoSichh-Anforderungen und -Maßnahmen dieser Zentralen Dienstvorschrift (siehe Anlagen 11.2 und 11.3) im IT-Grundschutzkatalog der Bw (siehe Anlage 11.1.2) die betrachtete IT nicht hinreichend abgebildet (modelliert) werden kann,
- IT in Einsatzszenarien betrieben wird, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind,
- gemäß der Schutzbedarfskategorie in der Informationsstruktur (siehe Abschnitt 2.1) geforderte InfoSichh-Anforderungen (siehe Anlage 11.3.2) durch eingesetzte Produkte oder umzusetzende InfoSichh-Maßnahmen nicht vollständig erfüllt werden können. In diesem Fall ist die Ergänzende Sicherheitsanalyse mit folgender Risikoanalyse (vgl. Anlage 11.1.10) nur bezogen auf nicht vollständig erfüllbare InfoSichh-Anforderungen und damit verbundene Risiken durchzuführen, siehe auch Abschnitt 2.2.2,
- gemäß der Schutzbedarfskategorie in der Informationsstruktur (siehe Abschnitt 2.1) umzusetzende InfoSichh-Maßnahmen des IT-Grundschutz des BSI und gemäß Anlage 11.3.2 nicht angewendet bzw. umgesetzt werden können. In diesem Fall ist die Ergänzende Sicherheitsanalyse mit folgender Risikoanalyse (vgl. Anlage 11.1.10) nur bezogen auf nicht anwend- / umsetzbare InfoSichh-Maßnahmen und damit verbundene Risiken durchzuführen, siehe auch Abschnitt 2.2.2. (**Anmerkung:** Die Durchführung einer Risikoanalyse für diesen Fall ist jedoch nicht erforderlich, wenn eine InfoSichh-Maßnahme nicht zutrifft. Nicht zutreffend ist z. B. eine InfoSichh-Maßnahme, die sich konkret auf ortsfeste Gebäudeinfrastruktur bezieht und nur dort umsetzbar ist, der Betrachtungsgegenstand jedoch z. B. ein Fahrzeug ist) oder
- InfoSichh-Maßnahmen noch nicht vollständig umgesetzt sind.

606. Nach der Risikoanalyse festgestellte Risiken sind hinsichtlich ihrer Tolerierbarkeit zu bewerten und zu dokumentieren. Die Ergebnisse der Risikoanalyse sind den Schutzbedarfsverantwortlichen (siehe Nr. 301) zur Stellungnahme zuzuleiten. Die Entscheidung, ob ein Risiko tolerierbar ist, treffen die jeweils zuständigen Verantwortlichen (z. B. Ltr IPT / ProjLtr / DStLtr / KtgtFhr / Kdr EinsStO). Die DEUmilSAA bzw. das zuständige Regionalzentrum im ZCSBw können beratend hinzugezogen werden.

607. Nicht tolerierbare Risiken sind mit zusätzlichen bzw. alternativen InfoSichh-Maßnahmen (siehe Abschnitt 2.2.2) durch die jeweils Verantwortlichen (z. B. Ltr IPT / ProjLtr / DStLtr) zu beseitigen (siehe auch Anlage 11.1.10.5). In besonders dringenden Fällen entscheidet der bzw. die zuständige Verantwortliche in Abstimmung mit dem bzw. der CISOBw und dem Supply Manager bzw. der Supply Managerin bzw. bei einsatzwichtiger IT der bzw. die KtgtFhr / Kdr EinsStO in Abstimmung mit dem bzw. der CISOBw und nach Rücksprache mit dem bzw. der Ltr NOC i.E. und dem Risikomanager bzw. der Risikomanagerin im EinsFüKdoBw über eine befristete Inbetriebnahme bzw. einen befristeten **Weiterbetrieb** der IT.

608. Es ist zu prüfen, ob die Dokumentation zur Ergänzenden Sicherheitsanalyse mit folgender Risikoanalyse (vgl. Anlage 11.1.10) als VS gemäß Zentraler Dienstvorschrift A-1130/2 VS-NfD „Militärische Sicherheit in der Bundeswehr – Verschlusssachen“ (siehe Bezug Anlage 11.15 (lfdNr. 15)) einzustufen ist.

609. Bei akkreditierten Systemen (siehe Abschnitt 5.5) ist die DEUmilSAA zu beteiligen. Bei hohen Risiken für die InfoSichh sind die Vorgaben gemäß Nr. 801ff. zu beachten.

610. Eine Methodik zur Durchführung von Risikoanalysen ist in der Anlage 11.1.10 beschrieben.

611. Bei Verarbeitung von PersDat ist ggf. eine Datenschutz-Folgenabschätzung in Verantwortung des bzw. der zuständigen ADSB durchzuführen (siehe Bezug Anlage 11.15 (lfdNr. 10)).

6.3 Informationssicherheitskonzepte / -befehle – Geltungsbereiche und Zuständigkeiten

6.3.1 Allgemeines

612. InfoSichhK sind nach ihrem Geltungsbereich in

- InfoSichhKProj, (siehe Abschnitt 6.3.2),
- InfoSichhKDSt, (siehe Abschnitt 6.3.3) und
- InfoSichhK für Wehrtechnische Forschung & Technologie sowie sonstige Forschungsvorhaben, Erprobungen, Truppenversuche und Wehrtechnische Aufträge, WissUstg NT (InfoSichhKFW, siehe Abschnitt 6.3.4)

zu unterscheiden[104].

Darüber hinaus gibt es – in militärischen DSt als Dokumentation der InfoSichh während Übungen – **Informationssicherheitsbefehle** (InfoSichhBef, siehe Abschnitt 6.3.5).

613. InfoSichhK müssen insbesondere

[104] Für die Anwendungsbereiche P, V, O und S (siehe Nr. 402) sind InfoSichhKProj, für D und E InfoSichhKDSt, für F und W InfoSichhKFW und für Ü InfoSichhBef zu erstellen.

- die jeweilige IT,
- die Informationsstruktur (siehe Abschnitt 2.1) unter Beachtung der Vorgaben und Hilfestellungen in der Anlage 11.4),
- das Einsatzspektrum,
- Q
- den Umfang der zu protokollierenden Ereignisse und deren Sicherheitsauditing (Auditingkonzept, siehe auch Anlage 11.6),
- die zu erfüllenden InfoSichh-Anforderungen bzw. umzusetzenden -Maßnahmen unter Berücksichtigung der Anlagen 11.1.2, 11.2 und 11.3 sowie
- bei Bedarf eine Risikoanalyse (siehe Abschnitt 6.2) einschließlich der Bewertung verbleibender Risiken

dokumentieren. Sie sind vor Inkraftsetzung fallbezogen abzustimmen bzw. mitzeichnen zu lassen. Näheres hierzu regeln die folgenden Abschnitte. Inhalte und Mitzeichnung von InfoSichhBef regelt Abschnitt 6.3.5.

614. InfoSichhK sind mindestens einmal jährlich auf ihre Aktualität zu prüfen. Dabei ist auch die Angemessenheit und Wirksamkeit der InfoSichh-Maßnahmen zu bewerten. Bei Bedarf ist das InfoSichhK fortzuschreiben (siehe hierzu Abschnitte 6.3.2.3 und 6.3.3.3).

615. InfoSichhK / InfoSichhBef sind durch den Verantwortlichen bzw. die Verantwortliche für die Erstellung in Kraft zu setzen.

616. Die Vorgaben zur InfoSichh von relevanten Projekten in der Bw, anderer Ressorts, der NATO, der EU, anderer Nationen oder von sonstigen überstaatlichen Organisationen, die in der Bw genutzt werden sollen oder zu denen es Berührungspunkte zu eigenen Projekten gibt, sind im Rahmen der InfoSichhKProj zu bewerten und geeignet zu berücksichtigen (siehe auch Abschnitt 4.4.4.2).

6.3.2 Projektbezogenes Informationssicherheitskonzept (P, V, O, S)

617. Für die Anwendungsbereiche Infrastruktur- / Baumaßnahmen bzw. sonstige Vorhaben mit IT-Anteil (V), IT-Betrieb und Aufgabenübernahme durch Dritte (O) und Sofortinitiativen für den Einsatz (S) ist dieser Abschnitt 6.3.2 sinngemäß anzuwenden.

6.3.2.1 Allgemeines

618. Das InfoSichhKProj beschreibt die technischen, personellen, infrastrukturellen und organisatorischen InfoSichh-Maßnahmen (einschl. Maßnahmen zur IT-Notfallvorsorge) zum Schutz der mit der jeweiligen IT zu verarbeitenden / übertragenden Informationen vor Verlust oder Beeinträchtigung der Grundwerte (siehe Nr. 111) bzw. bzgl. Einhaltung relevanter Gewährleistungsziele (siehe Nr. 112).

619. Bei der Realisierung von Projekten, die Informationen der Geheimhaltungsgrade VS-VERTRAULICH oder höher sowie vergleichbare NATO- / EU-Einstufungen bzw. Einstufungen anderer Nationen, sonstiger überstaatlicher Organisationen oder „MISSION“[105] verarbeiten oder übertragen, ist darüber hinaus das BAMAD im Rahmen seines gesetzlichen Mitwirkungsauftrages zum Geheimschutz bei der Erstellung von InfoSichhKProj beratend zu beteiligen. Anträge hierzu sind an das BAMAD unter nachrichtlicher Beteiligung der DEUmilSAA zu richten.

620. Aufbau, Form und Inhalt des InfoSichhKProj sind Anlage 11.7.1 bzw. der Arbeitshilfe zur Erstellung von InfoSichhKProj (siehe Anlage 11.1.1, Nr. 2) zu entnehmen.

6.3.2.2 Zuständigkeiten

621. InfoSichhKProj sind durch den bzw. die Ltr IPT / ProjLtr der DEUmilSAA zur Mitzeichnung vorzulegen. Der bzw. die Ltr IPT / ProjLtr beteiligt bei Einsatzbezug den bzw. die ISBEinsatz.

622. Bei Projekten, in denen PersDat verarbeitet bzw. gespeichert werden, berät die DEUmilSAA den bzw. die Ltr IPT / ProjLtr zu IT-relevanten Aspekten des Datenschutzes.

623. Der bzw. die Ltr IPT / ProjLtr stellt den DStLtr / KtgtFhr / Kdr EinsStO die durch diese umzusetzenden Vorgaben gemäß des durch ihn bzw. sie in Kraft gesetzten InfoSichhKProj zur Verfügung[106]. DStLtr / KtgtFhr / Kdr EinsStO übernehmen diese dienststellen- / einsatzbezogenen Vorgaben in das InfoSichhKDSt. Des Weiteren stellt der bzw. die Ltr IPT / ProjLtr das in Kraft gesetzte InfoSichhKProj der bzw. dem CISO Rüstung, der bzw. dem CISO Infrastruktur sowie der DEUmilSAA als Referenzdokument vor Beginn der Nutzung zur Verfügung.

624. Die Nrn. 621 bis 623 gelten auch für die Fortschreibung von InfoSichhKProj.

6.3.2.3 Fortschreibung

625. Das InfoSichhKProj ist in der Verantwortung des bzw. der zuständigen Ltr IPT / ProjLtr bei folgenden projektrelevanten Änderungen fortzuschreiben:

- wesentliche technische Änderungen an der IT (z. B. aufgrund Anschluss der IT anderer Projekte, Produktverbesserungen bzw. -änderungen wie z.B. zusätzliche Funktionalitäten),
- Änderungen der Informationsstruktur (siehe Abschnitt 2.1), z. B. bezüglich der Informationskategorie oder des Schutzbedarfes der zu verarbeitenden / übertragenden Informationen (solche Änderungen erfordern eine entsprechende Überarbeitung aller Abschnitte des InfoSichhKProj),
- FCPVOS

[105] „MISSION“ ist der Platzhalter für eine spätere konkrete Benennung und setzt eine sog. *Security Policy* für den beabsichtigten Einsatz voraus. Insofern ist z.B. MISSION SECRET keine gültige Einstufung, sondern z. B. NATO / ISAF SECRET oder NATO SECRET Releasable to ISAF.

[106] Form und Inhalt der bereitzustellenden Vorgaben sind der Arbeitshilfe zur Erstellung von projektbezogenen InfoSichhK (siehe Nr 2 in der Anlage 11.1.1) zu entnehmen

- Gesetzes- oder Vorschriftenänderungen (einschließlich Änderungen / Ergänzungen des IT-Grundschutzkatalogs der Bw oder ergänzender Anforderungen gemäß Anlagen 11.2 oder 11.3),
- Änderung des Einsatzspektrums der IT,
- Änderungen der möglichen Gefährdungen,
- erkannte Schwachstellen in der IT oder in ihrem Umfeld, die das Wirksamwerden einer Gefährdung begünstigen,
- Infrastrukturmaßnahmen, die die physikalische / technische Umgebung der IT betreffen oder verändern oder
- Anpassung / Änderung von CPM-Dokumenten, sofern technische Anteile der IT verändert werden.

626. Weitere anlassbezogene Gründe für die Fortschreibung des InfoSichhKProj sind im InfoSichhKProj zu dokumentieren.

6.3.3 Dienststellen- / einsatzbezogenes Informationssicherheitskonzept (D, E)

6.3.3.1 Allgemeines

627. Dieser Abschnitt gilt auch für die Erstellung von InfoSichhK für EinsKtgt / EinsStO. Der Begriff „einsatz- oder kontingentbezogenes InfoSichhK“ wird jedoch nicht verwendet.

628. Das InfoSichhKDSt dokumentiert alle in der DSt / im EinsKtgt / EinsStO umzusetzenden technischen, personellen, infrastrukturellen und organisatorischen InfoSichh-Maßnahmen (einschließlich Maßnahmen zur IT-Notfallvorsorge) zum Schutz der Informationen vor Verlust oder Beeinträchtigung der Grundwerte (siehe Nr. 111) bzw. bzgl. Einhaltung relevanter Gewährleistungsziele (siehe Nr. 112) aus den InfoSichhKProj bzw. InfoSichhKFW für die DSt / das EinsKtgt und die dort genutzte IT.

629. Aus den InfoSichhK der in der DSt / dem EinsKtgt betriebenen bzw. genutzten IT (z.B. InfoSichhKProj) werden die für die DSt / das EinsKtgt relevanten InfoSichh-Maßnahmen – dokumentiert im jeweiligen InfoSichhKProj bzw. InfoSichhKFW – als Vorgabe[107] übernommen. Die organisatorischen, personellen und infrastrukturellen sowie – falls die IT in der DSt / dem EinsKtgt betrieben wird – die technischen InfoSichh-Maßnahmen sind projekt- / vorhabenübergreifend vor dem Hintergrund der dienststellen- / einsatzbezogenen Gegebenheiten zu harmonisieren sowie anschließend in das InfoSichhKDSt zu übernehmen und umzusetzen. Nr. 451 ist zu beachten.

630. Für die Erstellung des InfoSichhKDSt werden folgende Eingangsdokumente / Angaben benötigt:

[107] Soweit vorhanden als importierbare Datei für das Grundschutzwerkzeug

- InfoSichhK der in der DSt / dem EinsKtgt / dem EinsStO genutzten bzw. betriebenen IT bzw. die Auszüge mit den Vorgaben für die DSt / das EinsKtgt / den EinsStO (d. h. insbesondere die Vorgaben für die InfoSichhKDSt), mit Ausnahme der Fälle gemäß Nr. 451,
- Übersicht über die in der DSt / im EinsKtgt / im EinsStO genutzte bzw. betriebene IT einschließlich deren Aufstellungsort und
- Vorschriften und Regelungen zur InfoSichh.

631. InfoSichhKDSt sind bedarfsbegründende Unterlagen für militärische und zivile Bedarfsforderungen zur Umsetzung von InfoSichh-Maßnahmen.

632. Aufbau und Struktur des InfoSichhKDSt mit Angaben zu den wesentlichen Inhalten sind Anlage 11.7.3 bzw. der Arbeitshilfe zur Erstellung von InfoSichhKDSt (siehe Anlage 11.1.1, Nr. 2) zu entnehmen.

6.3.3.2 Zuständigkeiten

633. Verantwortlich für die Erstellung und Inkraftsetzung des InfoSichhKDSt ist der bzw. die DStLtr / KtgtFhr / Kdr EinsStO.

634. InfoSichhKDSt sind bei Bedarf durch die ISB der vorgesetzten DSt, den bzw. die ISBEinsatz oder den zuständigen bzw. die zuständige ISBOrgBer auf Grundlage dieser Zentralen Dienstvorschrift zu prüfen. Diese Festlegung gilt auch für Fortschreibungen. Einzelheiten regeln die OrgBer.

6.3.3.3 Fortschreibung

635. InfoSichhKDSt sind bei Änderungen, die die InfoSichh betreffen, fortzuschreiben, z. B. bei:

- Fortschreibungen der InfoSichhKProj bzw. InfoSichhKFW, die Auswirkungen auf die DSt / das EinsKtgt / den EinsStO haben, in denen das Projekt bzw. Vorhaben genutzt / betrieben wird,
- Änderungen der IT-Ausstattung der DSt / des EinsKtgt / des EinsStO mit Auswirkung auf die InfoSichh,
- Einführung neuer IT (z. B. aus CPM-Projekten, Infrastruktur- / Baumaßnahmen und sonstige Vorhaben mit IT-Anteil, Sofortinitiativen für den Einsatz, Übernahme von IT anderer Nationen / Streitkräfte),
- Änderungen / Ergänzungen des IT-Grundschutzkatalogs der Bw,
- Änderung der möglichen Gefährdungen (z. B. bei Umzug oder Auftragsänderung der DSt / des EinsKtgt) oder
- Infrastrukturmaßnahmen (z. B. Umbau).

636. Bis zur Fortschreibung des InfoSichhKDSt sind informationssicherheitsrelevante Vorgänge in der DSt / dem EinsKtgt / dem EinsStO in der durch den bzw. die ISBDSt bzw. durch den bzw. die ISB

i.E. zu führenden dienststellenbezogenen / einsatzbezogenen InfoSichhDok (siehe Abschnitt 6.1.1) festzuhalten.

6.3.4 Informationssicherheitskonzept Forschung und Wissenschaft (F, W)

6.3.4.1 Allgemeines

637. Das InfoSichhKFW beschreibt die technischen, personellen, infrastrukturellen und organisatorischen InfoSichh-Maßnahmen (jedoch ohne Maßnahmen zur IT-Notfallvorsorge) zum Schutz der mit der jeweiligen IT zu verarbeitenden / übertragenden Informationen vor Verlust der Grundwerte (siehe Nr. 111) und bzgl. Relevanz der Gewährleistungsziele (siehe Nr. 112).

638. Die InfoSichhKFW sind inhaltlich in Anlehnung an einen InfoSichhBef zu erstellen (siehe Abschnitt 6.3.5). Ein Muster hierfür mit den Angaben zu den wesentlichen Inhalten ist Anlage11.8.8 zu entnehmen.

639. Das InfoSichhKFW ist frühzeitig vor Beginn des jeweiligen Vorhabens mit der DEUmilSAA – insbesondere hinsichtlich Umfang und Inhalt der zu erstellenden Abschnitte – abzustimmen. Die DEUmilSAA berät die Leitenden des jeweiligen Vorhabens bei der Erstellung des InfoSichhKFW.

640. Bei der Durchführung von Vorhaben, die Informationen der Geheimhaltungsgrade VS-VERTRAULICH oder höher sowie vergleichbare NATO- / EU-Einstufungen bzw. Einstufungen anderer Nationen, sonstiger überstaatlicher Organisationen oder „MISSION“[108] verarbeiten oder übertragen, ist darüber hinaus das BAMAD im Rahmen seines gesetzlichen Mitwirkungsauftrages zum Geheimschutz bei der Erstellung von InfoSichhKFW beratend zu beteiligen. Anträge hierzu sind an das BAMAD unter nachrichtlicher Beteiligung der DEUmilSAA zu richten.

6.3.4.2 Zuständigkeiten

641. Ist im Rahmen von Vorhaben der Wehrtechnischen Forschung & Technologie sowie sonstiger Forschungsvorhaben, Erprobungen, Truppenversuchen und Wehrtechnischen Aufträgen oder von Vorhaben der Wissenschaftlichen Unterstützung nicht-technisch die Erstellung eines InfoSichhKFW erforderlich (siehe hierzu Nrn. 408 und 410), ist hierfür der bzw. die Leitende des jeweilige Vorhabens verantwortlich.

642. InfoSichhKFW sind der DEUmilSAA zur Mitzeichnung vorzulegen. Die ISB der betroffenen OrgBer sind hierbei zu beteiligen. Die DEUmilSAA erarbeitet eine Stellungnahme zum InfoSichhKFW insbesondere im Hinblick auf eine ggf. erforderliche Akkreditierung. Der bzw. die Leitende eines entsprechenden Vorhabens informiert die DEUmilSAA unmittelbar, falls er bzw. sie beabsichtigt, von

[108] „MISSION“ ist der Platzhalter für eine spätere konkrete Benennung und setzt eine sog. *Security Policy* für den beabsichtigten Einsatz voraus. Insofern ist z.B. MISSION SECRET keine gültige Einstufung, sondern z. B. NATO / ISAF SECRET oder NATO SECRET Releasable to ISAF.

den Empfehlungen der Stellungnahme abzuweichen. Nach Abstimmung setzt der bzw. die Leitende des entsprechenden Vorhabens das InfoSichhKFW in Kraft.

643. Die Leitenden stellen das durch sie in Kraft gesetzte InfoSichhKFW den vorhabendurchführenden DSt vor Beginn der Vorhabendurchführung zur Verfügung.

6.3.5 Informationssicherheitsbefehl (Ü)

6.3.5.1 Allgemeines

644. Der Informationssicherheitsbefehl (InfoSichhBef, siehe auch Nr. 467) muss die Informationsstruktur gemäß Abschnitt 2.1 sowie mindestens Aussagen

- zum Informationsraum (siehe Begriffsbestimmungen in der Anlage 11.11),
- zu den infrastrukturellen und organisatorischen Absicherungsmaßnahmen am Übungsort,
- zur eingesetzten IT (einschl. Aussagen zu ihrer Vernetzung) und
- zu den jeweiligen Schnittstellen bei geplanter Kopplung von IT

enthalten und die Bestellung eines bzw. einer ISBÜb berücksichtigen. Als Anlage zum InfoSichhBef sind die InfoSichhKProj (siehe Abschnitt 6.3.2) bzw. InfoSichhKFW (siehe Abschnitt 6.3.4) der einzusetzenden IT aufzunehmen bzw. zu referenzieren. Ein Muster für Aufbau und Struktur des InfoSichhBef mit Angaben zu den wesentlichen Inhalten ist Anlage 11.8.8 zu entnehmen.

6.3.5.2 Zuständigkeiten

645. InfoSichhBef sind durch den Übungsleitenden bzw. die Übungsleitende zu erstellen und herauszugeben.

646. InfoSichhBef sind der DEUmilSAA über den bzw. die ISBOrgBer / ISBEinsatz der übungsleitenden DSt zur Mitzeichnung vorzulegen, wenn es sich um

- Übungen unter Einsatz von IT außerhalb der im jeweiligen InfoSichhKProj bzw. InfoSichhKFW beschriebenen Einsatzszenarien oder
- Übungen mit internationalem Bezug (z. B. wegen Verarbeitung / Übertragung von Informationen der NATO)

handelt. Die in diesen Übungen verwendete IT ist gemäß Nr. 520 zu akkreditieren.

Die DEUmilSAA legt fest, ob zusätzlich eine Mitprüfung durch einzelne ISBOrgBer oder den bzw. die ISBEinsatz erforderlich ist und informiert die jeweiligen ISBOrgBer / ISBEinsatz über diese Entscheidung.

647. InfoSichhBef organisationsbereichs- / einsatzspezifischer Übungen, die nicht unter die in Nr. 645 aufgezählten Übungen fallen, sind durch den bzw. die ISBOrgBer / ISBEinsatz mitzuzeichnen. Einzelheiten hierzu regeln die OrgBer / das EinsFüKdoBw.

6.3.6 Zuständigkeiten für die Erstellung / Inkraftsetzung und Abstimmung / Mitzeichnung von Informationssicherheitskonzepten sowie Informationssicherheitsbefehlen (Zusammenfassung)

648. Zusammenfassend werden die Zuständigkeiten für die Erstellung / Inkraftsetzung und Abstimmung / Mitzeichnung von InfoSichhK sowie InfoSichhBef dargestellt. Die Beteiligungsrechte der Gleichstellungsbeauftragten bleiben dabei unberührt.

Anwendungsbereich	Verantwortliche für Erstellung und Inkraftsetzung	Fallunter-scheidung	Abstimmung mit (A) / Mitzeichnung durch (M)
CPM-Projekte, Sofortinitiativen für den Einsatz, IT-Betrieb und Aufgabenübernahme durch Dritte	Ltr IPT / ProjLtr	–	DEUmilSAA (M) EinsFüKdoBw (A) (gemäß Abschnitt 6.3.2.2)
Infrastruktur- / Baumaß-nahmen bzw. sonstige Vorhaben mit IT-Anteil	Verantwortliche(r) für Infra-Maßnahmen	–	Inhalte gemäß Abstimmung mit der DEUmilSAA (M) (vgl. Abschnitt 4.5)
Dienststellen / Einsatzkontingente	DStLtr / KtgtFhr / Kdr EinsStO	–	Gemäß Regelung der OrgBer / EinsFüKdoBw (A) (gemäß Abschnitt 6.3.3.2)
Vorhaben der Wehrtechnischen Forschung & Technologie sowie sonstige Forschungsvorhaben, Erprobungen, Truppenversuche und Wehrtechnische Aufträge oder Vorhaben der Wissenschaftlichen Unterstützung nicht-technisch; jeweils mit einer prototypischen Realisierung	Leitender / Leitende des jeweiligen Vorhabens	–	DEUmilSAA (M) (gemäß Abschnitt 6.3.4.2)

Anwendungsbereich	Verantwortliche für Erstellung und Inkraftsetzung	Fallunter-scheidung	Abstimmung mit (A) / Mitzeichnung durch (M)
Übungen	Übungsleitende bzw. -leitender	OrgBer- / Einsatz-spezifisch	ISBOrgBer / ISBEinsatz[109] (M) ggf. DEUmilSAA (M) (gemäß Abschnitt 6.3.5.2)
		OrgBer- / Einsatz-übergreifend	DEUmilSAA (M) ggf. ISBOrgBer / ISBEinsatz[109] (M) (gemäß Abschnitt 6.3.5.2)
		Internationa-ler Bezug	DEUmilSAA(M) ggf. ISBOrgBer / ISBEinsatz (M) (gemäß Abschnitt 6.3.5.2)

Abb. 11: Zuständigkeiten zur Erstellung und Mitzeichnung von InfoSichhK / InfoSichhBef

6.4 Berichte zur Informationssicherheit (D)

649. Der bzw. die CISOBw erstellt einen jahresbezogenen Bericht zur Lage der InfoSichh in der Bw und gibt diesen bis zum 31. März des Folgejahres heraus.

650. In den Berichten zur Lage der InfoSichh sind Aussagen zum Stand und zum Bedarf an InfoSichh-Ausbildung in den OrgBer bzw. für den Einsatz aufzunehmen.

651. Die ISBOrgBer, der bzw. die ISBEinsatz, der bzw. die CISO Rüstung, der bzw. die CISO Infrastruktur und ZCSBw erarbeiten jahresbezogene Beiträge zum Bericht gemäß Nr. 649 im Rahmen ihrer Aufgaben und ihres Zuständigkeitsbereiches bis zum 15. Februar eines jeden Jahres. ISBBMVg legt seinen bzw. ihren Beitrag BMVg CIT II 2, ISBMAD BMVg R II 5 vor. Alle anderen legen ihre jahresbezogenen Beiträge dem bzw. der CISOBw unter nachrichtlicher Beteiligung BMVg CIT II 2 vor.

[109] Bei Übungen der Spezialkräfte der Bundeswehr ist auch die Mitzeichnung des bzw. der ISBEinsSpezKr erforderlich

7 Dezentrale Überwachung der Informationssicherheit

7.1 Allgemeines

701. Die dezentrale Überwachung der InfoSichh wird als Maßnahme der präventiven Fachaufsicht durch **InfoSichhIn** (siehe Abschnitt 7.2) und **InfoSichhKtr** (siehe Abschnitt 7.3) gewährleistet. Bei entsprechenden Hinweisen auf InfoSichhVork (siehe Abschnitt 8) wird die Überwachung durch eine **InfoSichhPrfg** (siehe Abschnitt 7.4) anlassbezogen erweitert.

Die Erkenntnisse aus den Überwachungsmaßnahmen dürfen nicht für die Leistungskontrolle von Bediensteten verwendet werden.

702. Im Rahmen von InfoSichhIn, InfoSichhKtr und InfoSichhPrfg darf das durchführende Personal nur auf Systemdateien, Metainformationen (z. B. Dateiname, Speicherdatum, Dateigröße) und Protokoll- / Auditingdaten lesend zugreifen. Dazu ist eine Freischaltung der Accounts der IT-Anwender weder notwendig, noch vorgesehen. Müssen im Rahmen von InfoSichhIn, InfoSichhKtr und InfoSichhPrfg Protokoll- und Auditingdaten von IT ausgewertet werden, die durch Dritte betrieben werden (siehe Abschnitt 4.6.1), so sind diese beim Betreiber vor der Prüfung über CSOCBw anzufordern. Bei der Auswertung von Protokoll- und Auditingdaten ist die Rahmendienstvereinbarung über die Protokollierung informationstechnischer Systeme (siehe Bezug Anlage 11.15 (lfdNr. 40)) zu berücksichtigen.

703. Sofern PersDat ab SB 2 bei der Durchführung von InfoSichhIn, InfoSichhKtr und InfoSichhPrfg betroffen sind, ist der bzw. die jeweils zuständige ADSB des zu prüfenden Anwendungsbereiches (Nr. 402) hinzuzuziehen. Die Einsichtnahme in dienstlich erhobene PersDat ist nur durch den zuständigen / die zuständige ADSB oder den bzw. die ADSB der vorgesetzten DSt bzw. des vorgesetzten EinsKtgt zulässig. Dies gilt bereits bei Einsichtnahme in Metainformationen, Protokoll- und Auditingdaten.

704. Sofern VS ab der Einstufung VS-VERTRAULICH oder höher sowie vergleichbare NATO- / EU-Einstufungen bzw. Einstufungen anderer Nationen, sonstiger überstaatlicher Organisationen oder „MISSION“[110] betroffen sind, ist der bzw. die für den jeweiligen Anwendungsbereich (siehe Nr. 402) zuständige SichhBeauftr hinzuzuziehen.

705. Die Einsichtnahme in IT-Anwenderdaten, die sich im Gewahrsam bzw. Mitgewahrsam des IT-Anwenders bzw. der IT-Anwenderin befinden, ist nur mit Einwilligung des IT-Anwenders bzw. der IT-Anwenderin zulässig. Die Einwilligung soll dokumentiert werden. Eine Nichteinwilligung darf nicht zu Lasten des IT-Anwenders bzw. der IT-Anwenderin gehen. Gewahrsam bzw. Mitgewahrsam an Dateien

[110] „MISSION“ ist der Platzhalter für eine spätere konkrete Benennung und setzt eine sog. *Security Policy* für den beabsichtigten Einsatz voraus. Insofern ist z.B. MISSION SECRET keine gültige Einstufung, sondern z. B. NATO / ISAF SECRET oder NATO SECRET Releasable to ISAF.

oder Datenträgern auf dienstlich genutzten APC ist in jedem Fall dann gegeben, wenn diese etwa durch ein persönliches Passwort des IT-Anwenders bzw. der IT-Anwenderin gegen Zugriffe Dritter (ausgenommen Zugriffsrechte von Systemadministratoren) geschützt sind. Weiter besteht ein rechtlich schützenswerter Gewahrsam, wenn die Nutzung des APC mit Genehmigung des Dienstherrn für die Tätigkeit in einer Funktion erfolgt, deren Inhalte einem besonderen Schutz unterliegen und an deren Geheimhaltung auch gegenüber dem Dienstherrn ein berechtigtes Interesse besteht (z. B. Nutzung für vertrauliche Angelegenheiten der Personalvertretung).

Liegt eine Einwilligung des IT-Anwenders bzw. der IT-Anwenderin zur Einsichtnahme in diesen Fällen nicht vor, bedarf die Einsichtnahme bzw. die Durchsuchung grundsätzlich einer richterlichen Anordnung.

Bei Verdacht auf eine Straftat / ein Dienstvergehen ist vor weiteren Maßnahmen zur Durchsuchung, Sicherstellung bzw. Beschlagnahme der bzw. die Disziplinarvorgesetzte zu informieren. Zum weiteren Vorgehen für eine Durchsuchung ist die Arbeitshilfe „Rechtliche Aspekte für die Durchsuchung von IT“ zur A-960/5 „Behandlung von Informationssicherheitsvorkommnissen und Unterstützung von disziplinaren und strafrechtlichen Ermittlungen“, Abschnitt 4.1, Nr. 7 (siehe Bezug Anlage 11.15 (lfdNr. 59)) zu beachten. Zur Tatort- und Beweismittelsicherung ist der Leitfaden „Beweisermittlung / -sicherung“ zur A-960/5 „Behandlung von Informationssicherheitsvorkommnissen und Unterstützung von disziplinaren und strafrechtlichen Ermittlungen“, Abschnitt 4.2, Nr. 3 (siehe Bezug Anlage 11.15 (lfdNr. 59)) zu beachten. Zur Unterstützung von disziplinaren und strafrechtlichen Ermittlungen ist die A-960/5 „Behandlung von Informationssicherheitsvorkommnissen und Unterstützung von disziplinaren und strafrechtlichen Ermittlungen“, Abschnitt 3 (siehe Bezug Anlage 11.15 (lfdNr. 59)) zu beachten.

706. Der bzw. die Verantwortliche für die InfoSichh im überprüften Anwendungsbereich (siehe Nr. 402) veranlasst die notwendigen Maßnahmen zur Abstellung von Mängeln, die im Rahmen der Überwachungsmaßnahmen bekannt geworden sind.

707. Erkenntnisse von grundsätzlicher und / oder übergreifender Bedeutung sind auf dem Dienstweg unter Beteiligung des bzw. der betroffenen ISBOrgBer / ISBEinsatz an den CISOBw zu melden und von diesem bzw. dieser bei Bedarf dem bzw. der CISO Ressort im BMVg zu melden.

708. ISBDSt / ISB i.E., SichhBeauftr und ADSB unterrichten sich rechtzeitig gegenseitig über ihre geplanten Prüfungen / Kontrollen. Die jeweiligen Prüfungen sollen gemeinsam durchgeführt werden.

709. Wenn aufgrund festgestellter InfoSichh-Mängel ein Hinweis auf extremistische / terroristische Bestrebungen oder sicherheitsgefährdende oder geheimdienstliche Tätigkeiten vorliegt, ist der MAD unverzüglich über den bzw. die SichhBeauftr einzuschalten (siehe auch Nr. 821f.).

7.2 Informationssicherheitsinspektionen

7.2.1 Allgemeines

710. InfoSichhIn sind regelmäßige oder anlassbezogene (z. B. vor Beginn eines Einsatzes oder bei Häufung von InfoSichhVork in einer DSt) Überprüfungsmaßnahmen, die auf der Grundlage aller in den jeweiligen Anwendungsbereichen (siehe Nr. 402) umzusetzenden und im jeweiligen InfoSichhK (siehe Abschnitt 6.3) dokumentierten InfoSichh-Maßnahmen und zur Überprüfung der Einhaltung der Regelungen zur InfoSichh bzw. zur Kryptosicherheit durchgeführt werden. Sie geben einen Überblick zum Umsetzungsstand von InfoSichh-Maßnahmen und über die Einhaltung der Vorschriften zur InfoSichh im jeweiligen Anwendungsbereich.

711. Für die Durchführung von InfoSichhIn gilt:

- Anwendungsbereiche D, E und Ü (vgl. Nr. 402):
  - Für InfoSichh-Maßnahmen, die in der DSt / dem EinsKtgt gemäß InfoSichhKDSt, InfoSichhKFW bzw. InfoSichhBef (auch auf Grund von Vorgaben anderer InfoSichhK wie z.B. InfoSichhKProj) umzusetzen sind, sind diese Maßnahmen auf Umsetzung zu prüfen und dazu die Prüffragen aus dem zentralen Prüfkatalog für InfoSichhIn (siehe Nr. 338) zu Grunde zu legen.
  - Muss die DSt / das EinsKtgt darüber hinaus InfoSichh-Maßnahmen umsetzen für die keine Prüffragen verankert sind (z. B. für höheren Schutzbedarf als „normal“ gemäß Anlage 11.3), sind diese ebenfalls auf Umsetzung zu prüfen.
- Anwendungsbereiche F, W, P, V, O und S (vgl. Nr. 402):
  - Für InfoSichh-Maßnahmen, die das Projekt bzw. das Vorhaben gemäß InfoSichhKProj bzw. InfoSichhKFW umzusetzen hat, sind diese Maßnahmen auf Umsetzung zu prüfen und dazu die Prüffragen aus dem zentralen Prüfkatalog für InfoSichhIn (siehe Nr. 338) zu Grunde zu legen.
  - Muss das Projekt bzw. das Vorhaben darüber hinaus InfoSichh-Maßnahmen umsetzen für die keine Prüffragen verankert sind (z. B. für höheren Schutzbedarf als „normal“ gemäß Anlage 11.3), sind diese ebenfalls auf Umsetzung zu prüfen.

7.2.2 Zuständigkeiten

712. InfoSichhIn führen durch:

- die **Regionalzentren des ZCSBw** in allen Anwendungsbereichen (siehe Nr. 402) dieser Zentralen Dienstvorschrift (mit Ausnahme der folgenden Strichaufzählungen), in den EinsKtgt und EinsStO unter Beteiligung des ISBEinsatz,
- der bzw. die **ISBBMVg** im BMVg,
- der bzw. die **ISBMAD** in den Dienststellen des MAD,

- der bzw. die **ISBEinsatzSpezKr** in Einsätzen von SpezKr der Bw im Ausland in Abstimmung mit ZCSBw sowie
- der bzw. die **ISBGBW** oder von ihm bzw. ihr beauftragte Dritte in den Unternehmen der geheimschutzbetreuten Wirtschaft, die Kryptogeräte der Bw nutzen.

713. Die Befugnis zur Veranlassung oder Durchführung von InfoSichhIn haben zusätzlich zu den Durchführenden gem. Nr. 712 jederzeit der bzw. die

- **CISO Ressort** in allen Anwendungsbereichen (siehe Nr. 402) dieser Zentralen Dienstvorschrift sowie im BMVg,
- **CISOBw** in allen Anwendungsbereichen (siehe Nr. 402) dieser Zentralen Dienstvorschrift,
- **CISO Rüstung** in den Anwendungsbereichen P und S (siehe Abschnitte 4.4 und 4.7) in Abstimmung mit dem ZCSBw,
- **CISO Infrastruktur** im Anwendungsbereich V (siehe Abschnitt 4.5) in Abstimmung mit dem ZCSBw sowie
- **ISBEinsatz** im Anwendungsbereich E (siehe Abschnitt 4.9) für alle DEU EinsKtgt unter Beachtung der Nr. 312.

7.2.3 Dokumentation / Informationssicherheitsinspektionsbericht

714. Das Ergebnis durchgeführter InfoSichhIn ist in einem **Informationssicherheitsinspektionsbericht** (InfoSichhInB) durch den Inspizierenden bzw. die Inspizierende zu dokumentieren und nach dessen Fertigstellung gemäß Verteiler zu übergeben bzw. zu übersenden.

715. Ist akkreditierte IT (vgl. Nr. 520) betroffen, ist die DEUmilSAA an der Meldung zu beteiligen.

716. Werden Mängel im Zusammenhang mit dem Schutz von PersDat festgestellt, ist der bzw. die für den jeweiligen Anwendungsbereich (siehe Nr. 402) zuständige ADSB zu informieren, der bzw. die ggf. weitere in seinem bzw. ihrem Zuständigkeitsbereich liegende Maßnahmen ergreift.

Werden Mängel im Zusammenhang mit dem Schutz von VS festgestellt, ist der bzw. die für den jeweiligen Anwendungsbereich (siehe Nr. 402) zuständige SichhBeauftr zu informieren, der bzw. die ggf. weitere in seinem bzw. ihrem Zuständigkeitsbereich liegende Maßnahmen ergreift.

717. Der InfoSichhInB muss Aussagen zur Gesamtbewertung der InfoSichh im geprüften Anwendungsbereich enthalten und ist wie folgt zu gliedern:

1. Allgemeines (geprüfter Anwendungsbereich, der bzw. die für die InfoSichh im Anwendungsbereich Verantwortliche, Datum und Anlass der Inspektion, Datum und Durchführender bzw. Durchführende der letzten Inspektion, Kryptomittel (falls vorhanden), Anlagen),
2. Bewertung(en) der InfoSichh, Kryptosicherheit (falls zutreffend),
3. Abschlussbesprechung,
4. Berichte des bzw. der für die InfoSichh im Anwendungsbereich Verantwortlichen,

5. Wesentliche Feststellungen sowie
6. Folgerungen und Vorschläge.

Muster für InfoSichhInB (mit und ohne Kryptomittel) finden sich in Anlage 11.8.3.1 und 11.8.3.2. Wird im Rahmen der InfoSichhIn nur die Kryptosicherheit geprüft (siehe Nr. 722), ist Anlage 11.8.3.1 zu nutzen.

718. Der Bericht sowie die Dokumentation der ggf. erforderlichen Mängelbeseitigung sind zur InfoSichhDok des Anwendungsbereiches (siehe Abschnitte 6.1.1) zu nehmen. Daneben ist die Dokumentation der Mängelbeseitigung in Form eines Abschlussberichtes auf dem Dienstweg an die prüfende Instanz zu senden.

719. Erkennt der bzw. die Inspizierende mögliche InfoSichhVork (siehe Abschnitt 8.2), teilt er diese unverzüglich dem zuständigen bzw. der zuständigen ISB der inspizierten Stelle und CSOCBw (Hotline 90-11111) zur weiteren Bewertung mit.

720. Die Beteiligung des MAD gemäß Nr. 709 ist durch die inspizierte Stelle zu prüfen.

7.2.4 Zeitintervalle

721. Die Zeitintervalle der InfoSichhIn ergeben sich aus der Schutzbedarfskategorie (siehe Abschnitt 2.1.4, Abb. 3) bezogen auf die Vertraulichkeit der mit der IT zu verarbeitenden/übertragenden Informationen bzw. aus einsatzrelevanten Anforderungen. Folgende Richtwerte gelten für

- Schutzbedarf der Vertraulichkeit normal oder hoch: 3 Jahre,
- Schutzbedarf der Vertraulichkeit sehr hoch: 2 Jahre und
- EinsKtgt / EinsStO je Ktgt mindestens einmal.

722. Kryptoverwaltungen einer DSt / eines EinsKtgt sind im Rahmen von InfoSichhIn[111] einmal jährlich nach den Vorgaben der Zentralen Dienstvorschrift A-961/1 VS-NfD „Kryptosicherheit in der Bundeswehr“, Abschnitt 9.11.10 (siehe Bezug Anlage 11.15 (lfdNr. 20)) zu inspizieren (dies gilt auch für InfoSichhIn in der geheimschutzbetreuten Wirtschaft durch den bzw. die ISBGBW).

723. Für IT, mit der NATO SECRET bzw. SECRET UE / EU SECRET eingestufte Informationen verarbeitet / übertragen wird, kann die DEUmilSAA im Rahmen der Akkreditierung (siehe Abschnitt 5.5) in Übereinstimmung mit den Vorgaben der NATO bzw. der EU abweichende Richtwerte festlegen.

724. Eine im Einzelfall vorzunehmende notwendige Verschiebung von Inspektionen[112] außerhalb der vorgegebenen Zeitintervalle ist zu beantragen. Die Beantragung sowie Genehmigung wird durch CISOBw geregelt. Die Entscheidung auf Verschiebung ist immer als Einzelfall unter Anlegung eines strengen Maßstabes zu bewerten.

[111] in diesem Falle als Kryptosicherheitsinspektion
[112] z.B. kurzfristige Beorderung der DSt in den Einatz bzw. Übung, Auslagerung von Kryptomaterial im Rahmen von Instandsetzungen

7.3 Informationssicherheitskontrollen

7.3.1 Allgemeines

725. InfoSichhKtr sind Überwachungsmaßnahmen, die insbesondere bei den IT-Anwendern und Administratoren innerhalb einer DSt / eines EinsKtgt bzw. einer IT-Btrb(Fü)Einr unregelmäßig erfolgen müssen[113]. Dazu zählen auch Kontrollen zur Überwachung der ordnungsgemäßen Behandlung von Kryptomitteln im Rahmen der Kryptoverwaltung und des Kryptobetriebes in der Bw und in der geheimschutzbetreuten Wirtschaft.

726. Im Rahmen der InfoSichhKtr ist durch den bzw. die ISBDSt / ISB i.E. das Kryptotagebuch (wenn Kryptomittel vorhanden sind) mindestens einmal jährlich nach den Vorgaben der Zentralen Dienstvorschrift A-961/1 VS-NfD „Kryptosicherheit in der Bundeswehr“, Abschnitt 9.11.10 (siehe Bezug Anlage 11.15 (lfdNr. 20)) zu überprüfen, insbesondere „Löschungen“ sind durch ihn bzw. sie zu prüfen und gelten erst nach Prüfung als abgeschlossen.

7.3.2 Zuständigkeiten (D, E, O)

727. InfoSichhKtr sind durch den bzw. die ISBOrgBer / ISBDSt / ISB i.E., ISBGBW bzw. jeden ISBBtrb grundsätzlich eigenständig im Zuständigkeitsbereich sowie durch den bzw. die ISBProj für den Anwendungsfall „IT-Betrieb und Aufgabenübernahme durch Dritte“ (O) durchzuführen. In besonderen Fällen sind sie auf Anweisung CISO Ressort, CISOBw, des ZCSBw, der ISBOrgBer, der vorgesetzten DSt oder des bzw. der ISBBMVg bzw. ISBMAD durchzuführen.

7.3.3 Dokumentation (D, E, O)

728. Die Ergebnisse der InfoSichhKtr sind in einem formlosen Bericht festzuhalten und dem bzw. der DStLtr / KtgtFhr bzw. Ltr NDA Germany sowie für den Anwendungsfall „IT-Betrieb und Aufgabenübernahme durch Dritte“ (O) dem bzw. der ProjLtr vorzulegen. Sie sind zur InfoSichhDok (siehe Abschnitt 6.1.1 bzw. 6.1.2) zu nehmen. Der Bericht ist bis zur vollständigen Abstellung ggf. festgestellter Mängel, mindestens jedoch bis zur nächsten InfoSichhIn aufzubewahren.

729. Die Beteiligung des MAD gemäß Nr. 709 ist durch die kontrollierte Stelle zu prüfen.

7.4 Informationssicherheitsprüfungen

7.4.1 Allgemeines

730. InfoSichhPrfg dienen der Aufklärung von InfoSichh-Verstößen und -Lücken (zur Begriffsbestimmung siehe Nrn. 806 und 807). Näheres zu InfoSichhPrfg zur Aufklärung von InfoSichh-

[113] Zur Unterscheidung der Dienstaufsicht von der Durchsuchung und weiteren rechtlichen Aspekten siehe Nr. 705 und die dort aufgeführten Verweise auf die A-960/5 einschließlich Arbeitshilfen und Leitfäden.

Verstößen regeln Abschnitt 8 und die A-960/5 „Behandlung von Informationssicherheitsvorkommnissen und Unterstützung von disziplinaren und strafrechtlichen Ermittlungen“ (siehe Bezug Anlage 11.15 (lfdNr. 59)).

7.4.2 Zuständigkeiten

731. Die Entscheidung zur Durchführung einer InfoSichhPrfg trifft der zuständige Rollenträger bzw. die zuständige Rollenträgerin (z.B. DStLtr / KtgtFhr / Kdr EinsStO / Ltr IPT / ProjLtr) für seinen bzw. ihren nachgeordneten Bereich auf Empfehlung des bzw. der jeweils zuständigen ISB oder auf Veranlassung durch den bzw. die CISO Ressort, CISOBw oder das ZCSBw.

732. InfoSichhPrfg sind von der Prüforganisation des ZCSBw (die Incident Response Teams im CSOCBw, alle Regionalzentren (vgl. Nr. 340) und alle Schwachstellenanalyse-Teams) durchzuführen.

733. Werden im Rahmen einer InfoSichhPrfg anlassbezogene Ermittlungen (Verdacht auf missbräuchliche oder unerlaubte Nutzung von IT) erforderlich, ist die Beteiligung der Personalvertretung zu prüfen (gemäß Rahmendienstvereinbarung über die Protokollierung informationstechnischer Systeme, siehe Bezug Anlage 11.15 (lfdNr. 40), dort § 7).

7.4.3 Dokumentation

734. Der bzw. die Prüfende hat das Ergebnis der InfoSichhPrfg in einem formlosen Bericht zu dokumentieren und dem bzw. der betroffenen Verantwortlichen im Anwendungsberich (z. B. DStLtr / KtgtFhr / Kdr EinsStO, ProjLtr) sowie Anordnenden vorzulegen. Mängel in der InfoSichh sind zu erläutern. Der bzw. die Prüfende schlägt Maßnahmen zur Abstellung der Mängel vor. Das Ergebnis sowie die Dokumentation der Mängelbeseitigung sind zur InfoSichhDok (siehe Abschnitt 6.1.1 bzw. 6.1.2) zu nehmen. Der Bericht ist bis zur vollständigen Abstellung ggf. festgestellter Mängel aufzubewahren.

735. Die Beteiligung des MAD gemäß Nr. 709 ist durch die geprüfte Stelle zu prüfen.

8 Meldewesen für und Behandlung von Informations-sicherheitsvorkommnissen

8.1 Allgemeines

801. In diesem Abschnitt werden das „Aufgaben- und fachbezogene Meldewesen“ gemäß Zentraler Dienstvorschrift A-200/5 „Meldewesen der Bundeswehr“ (siehe Bezug Anlage 11.15 (lfdNr. 17)) für spezifische Sachverhalte der InfoSichh sowie Grundsätze zu Aufgaben und Zuständigkeiten bei der Behandlung von InfoSichhVork geregelt. Da bei Informationssicherheitsvorkommnissen (InfoSichhVork) häufig personenbezogene Daten betroffen sind, ist stets zu prüfen, ob ein meldepflichtiger Datenschutzverstoß vorliegt und der bzw. die zuständige ADSB umgehend zu informieren ist.

802. InfoSichhVork sind durch die jeweils zuständigen Rollenträgerinnen und Rollenträger der Anwendungsbereiche (siehe Abschnitt 4) nach den Grundsätzen dieses Abschnittes sowie nach den Vorgaben der Zentralen Dienstvorschrift A-960/5 „Behandlung von Informationssicherheits-vorkommnissen und Unterstützung von disziplinaren und strafrechtlichen Ermittlungen“ (siehe Bezug Anlage 11.15 (lfdNr. 59))[114] zu behandeln.

Die A-960/5 regelt die Behandlung von InfoSichhVork im Detail, gibt Hilfestellung hinsichtlich der richtigen Reaktion bei InfoSichhVork und regelt die Unterstützung von disziplinaren und strafrechtlichen Ermittlungen.

InfoSichhVork können durch zu späte oder falsche Reaktionen kritisch werden. Daher ist es wichtig, frühzeitig und umfassend zu melden und sich im Zweifelsfall vor weiteren Maßnahmen durch CSOCBw beraten zu lassen. Dies trägt entscheidend zu einem vollständigen InfoSichh-Lagebild und einer Schadensminimierung im GB BMVg bei. Sofern bei der Bewertung des InfoSichhVork ein hohes Sicherheitsrisiko identifiziert wird, ist die A-960/15 „IT-Krisenmanagement in der Bundeswehr“ (siehe Bezug Anlage 11.15 (lfdNr. 47)) anzuwenden.

803. Die Behandlung von InfoSichhVork ist regelmäßig mit der zuständigen IT-Btrb(Fü)Einr hinsichtlich Maßnahmen zur Wiederherstellung und zum Wiederanlauf zu üben. Der Umfang sollte so gewählt und mit der IT-Btrb(Fü)Einr abgestimmt werden, dass Auswirkungen auf den laufenden IT-Betrieb begrenzt bleiben.

804. Eine Kommunikation mit der Presse bzw. Öffentlichkeit zu InfoSichhVork erfolgt ausschließlich durch CISOBw in Abstimmung mit dem jeweils zuständigen PIZ.

[114] Verweis ist vorläufig, da sich die ZDv A-960/5 in der Überarbeitung befindet.

805. Die Dokumentation zu abgeschlossenen InfoSichhVork ist drei Jahre aufzubewahren. Die Frist beginnt am Ende des laufenden Kalenderjahres.

8.2 Begriffsbestimmungen

806. Eine **Informationssicherheitslücke** liegt vor bei drohendem Verlust mindestens eines Grundwertes der Informationssicherheit (siehe Nr. 111) oder eines Gewährleistungszieles (siehe Nr. 112) durch unzureichende Umsetzung bestehender Vorgaben und Maßnahmen der InfoSichh oder dem Bekanntwerden einer neuen Gefährdung (siehe Nr. 115), der nicht zeitnah mit angemessenen InfoSichh-Maßnahmen begegnet werden kann.

807. Ein **Informationssicherheitsverstoß** liegt vor bei eingetretenem und vermutetem Verlust mindestens eines Grundwertes der Informationssicherheit (siehe Nr. 111) oder eines Gewährleistungszieles (siehe Nr. 112).

808. Ein **Sicherheitsvorkommnis im Kryptowesen** liegt vor, wenn durch Nichtbeachtung von Vorgaben der Kryptosicherheit (A-961/1 VS-NfD „Kryptosicherheit in der Bundeswehr“, (siehe Bezug Anlage 11.15 (lfdNr. 20))) die Kryptosicherheit beeinträchtigt oder gefährdet ist.

809. Ein **InfoSichhVork** liegt vor, wenn die InfoSichh durch

- eine Informationssicherheitslücke,
- einen Informationssicherheitsverstoß oder
- ein Sicherheitsvorkommnis im Kryptowesen

beeinträchtigt bzw. gefährdet wird.

Details zur Einordnung von InfoSichhVork sind der Arbeitshilfe „Kategorien und Anwendungsfälle für InfoSichhVork“ in der A-960/5 „Behandlung von Informationssicherheitsvorkommnissen und Unterstützung von disziplinaren und strafrechtlichen Ermittlungen“, Abschnitt 4.1, Nr. 3. zu entnehmen (siehe Bezug Anlage 11.15 (lfdNr. 59)).

810. Sicherheitsvorkommnisse im Kryptowesen (gemäß Zentraler Dienstvorschrift A-961/1 VS-NfD „Kryptosicherheit in der Bundeswehr“, Abschnitt 7) sind mit den dann notwendigen Meldungen (einschließlich Benachrichtigung per E-Mail) abschließend in der A-961/1 VS-NfD „Kryptosicherheit in der Bundeswehr“ geregelt. Sofortmeldung oder Abschlussbericht gemäß Abschnitt 8.4 entfallen daher bei Sicherheitsvorkommnissen im Kryptowesen.

8.3 Aufgaben und Zuständigkeiten

811. Alle Betreiber und Nutzer von IT im GB BMVg sowie Vertragspartner der Bw sollen Verdachtsmomente auf ein InfoSichhVork bzw. entsprechende auffällige Ereignisse unverzüglich dem bzw. der Zuständigen für die Bearbeitung von InfoSichhVork im jeweiligen Anwendungsbereich (siehe

Nr. 402) melden. Dies ist in der Regel der bzw. die bestellte ISB (z. B. ISBDSt / ISB i.E. / ISBProj, ISBFW). Falls kein bzw. keine ISB bestellt wurde, ist an den Verantwortlichen bzw. die Verantwortliche für die InfoSichh im jeweiligen Anwendungsbereich zu melden, der dann die im Folgenden beschriebenen Tätigkeiten eines ISB bezüglich der weiteren Bearbeitung übernimmt. Sind die o.g. Rollenträgerinnen und Rollenträger nicht verfügbar bzw. nicht unmittelbar erreichbar, ist ausnahmsweise direkt an CSOCBw[115] zu melden. CSOCBw hat zur Umsetzung seiner Zuständigkeiten bei der Behandlung von InfoSichhVork eine fachliche Weisungsbefugnis gegenüber den beteiligten Stellen in der Bw[116].

812. Der bzw. die zuständige ISB[117]

- prüft unverzüglich, ob es sich bei dem gemeldeten Verdachtsmoment bzw. Ereignis tatsächlich um ein InfoSichhVork oder ein anderes gemäß Abschnitt 8.5 „Weitere Meldungen“ meldepflichtiges Ereignis / Vorkommnis handelt.
- nutzt dabei und für die weitere Behandlung von InfoSichhVork bei Bedarf die fachliche Beratung durch CSOCBw.
- beachtet beim weiteren Vorgehen die detaillierten Vorgaben der A-960/5 „Behandlung von Informationssicherheitsvorkommnissen und Unterstützung von disziplinaren und strafrechtlichen Ermittlungen“ (siehe Bezug Anlage 11.15 (lfdNr. 59)).
- meldet umgehend dem bzw. der Verantwortlichen für die InfoSichh im Anwendungsbereich (i.d.R. der bzw. die DStLtr / KtgtFhr / ProjLtr, siehe Nr. 402) und holt bei allen weiteren Aktivitäten zur Behandlung des InfoSichhVork im notwendigen Umfang die Entscheidung des bzw. der Verantwortlichen für die InfoSichh im jeweiligen Anwendungsbereich ein.
- veranlasst für ein erkanntes bzw. vermutetes InfoSichhVork das Absetzen einer Sofortmeldung (siehe Abschnitt 8.4) innerhalb der in der A-960/5 „Behandlung von Informationssicherheitsvorkommnissen und Unterstützung von disziplinaren und strafrechtlichen Ermittlungen“ (siehe Bezug Anlage 11.15 (lfdNr. 59)) genannten Fristen (in Abhängigkeit von der Stufe des InfoSichhVork spätestens am nächsten Tag).
- veranlasst für InfoSichhVork gemäß A-960/5 „Behandlung von Informationssicherheits-vorkommnissen und Unterstützung von disziplinaren und strafrechtlichen Ermittlungen“ (siehe Bezug Anlage 11.15 (lfdNr. 59)) Sofortmaßnahmen bzw. setzt angewiesene Maßnahmen des CSOCBw um (ist ein Projekt betroffen, so ist der bzw. die zuständige Ltr IPT / ProjLtr zu beteiligen).
- veranlasst die Umsetzung der weiteren Maßnahmen zur Behandlung des InfoSichhVork gemäß A-960/5, Abschnitt 2.3.1.

[115] Tel: 90-11111 bzw. 02251-953-3105; Mail: CSOCBw@bundeswehr.org
[116] Mit Ausnahme von CISO Ressort / BMVg CIT II 2 und CISOBw.
[117] Ist kein bzw. keine ISB bestellt, übernimmt der bzw. die Verantwortliche für die InfoSichh im jeweiligen Anwendungsbereich (siehe Nr. 402) diese Aufgaben.

- schlägt bei Bedarf zur weiteren Aufklärung eines InfoSichhVork dem bzw. der Verantwortlichen für die InfoSichh im jeweiligen Anwendungsbereich (siehe Nr. 402) die Durchführung einer InfoSichhPrfg (siehe Abschnitt 7.4) vor.
- beteiligt den zuständigen bzw. die zuständige ADSB, wenn PersDat betroffen sind.
- beteiligt den bzw. die SichhBeauftr, wenn der Schutz von VS betroffen ist bzw. ein Hinweis auf extremistische / terroristische Bestrebungen oder sicherheitsgefährdende oder geheimdienstliche Tätigkeiten vorliegt (siehe dazu Abschnitt 8.6). Wird der bzw. die SichhBeauftr eingeschaltet und ergibt dessen / deren Prüfung, dass das Ereignis als Sicherheitsvorkommnis gemäß Zentraler Dienstvorschrift A-1130/1 VS-NfD „Militärische Sicherheit in der Bundeswehr – Militärische Sicherheit“[118] (siehe Bezug Anlage 11.15 (lfdNr. 14)) zu qualifizieren ist, übernimmt der bzw. die SichhBeauftr die Federführung für das Vorkommnis und die weitere Bearbeitung.
- beteiligt den bzw. die SichhBeauftr der DSt, wenn sich aus dem InfoSichhVork Hinweise auf ein Sicherheitsrisiko[119] (siehe Bezug Anlage 11.15 (lfdNr. 16)) ergeben.
- veranlasst bei Verdacht einer Straftat oder eines Dienstvergehens unverzüglich eine Meldung an den zuständigen Disziplinarvorgesetzten bzw. die zuständige Disziplinarvorgesetzte[120] (für Soldaten bzw. Soldatinnen), an den zuständigen Dienstvorgesetzten bzw. die zuständige Dienstvorgesetzte (für Beamte bzw. Beamtinnen) oder an die zuständige Personalführung (für Tarifbschäftigte). Das Ergebnis der Prüfungen und ggf. die Meldung an den bzw. die Disziplinarvorgesetzte(n) ist zu dokumentieren und bei der DSt / im EinsKtgt zur InfoSichhDok (siehe Abschnitt 6.1.1) zu nehmen.
- führt eine Übersicht über alle gemeldeten InfoSichhVork in der InfoSichhDok der DSt bzw. des EinsKtgt (siehe Abschnitt 6.1.1).

813. Der bzw. die Verantwortliche für die InfoSichh im Anwendungsbereich (**i.d.R. DStLtr / KtgtFhr / ProjLtr**)

- übernimmt die Aufgaben des bzw. der ISB, wenn er bzw. sie keinen bzw. keine ISB bestellt hat.
- ist verantwortlich für die unverzügliche und umfassende Meldung und weitere Behandlung der InfoSichhVork in seinem bzw. ihrem Zuständigkeitsbereich.

[118] Die Meldung eines erkannten Sicherheitsvorkommnisses erfolgt nach den Vorgaben des Zentralerlasses B-1130/32 VS-NfD „Melde-, Berichts- und Informationswege zur Erstellung der Militärischen Sicherheitslage der Bundeswehr“ (vgl. Nr. 820).

[119] ZDv A-1130/3 „Militärische Sicherheit in der Bundeswehr – Personeller Geheim- und Sabotageschutz“, Nr. 2408: Ein Sicherheitsrisiko liegt vor, wenn tatsächliche Anhaltspunkte
(1) Zweifel an der Zuverlässigkeit des Betroffenen bei der Wahrnehmung einer sicherheitsempfindlichen Tätigkeit begründen) oder
(2) eine besondere Gefährdung durch Anbahnungs- und Werbungsversuche fremder Nachrichtendienste, insbesondere die Besorgnis der Erpressbarkeit, begründen) oder
(3) Zweifel am Bekenntnis des Betroffenen zur freiheitlichen demokratischen Grundordnung im Sinne des Grundgesetzes oder am jederzeitigen Eintreten für deren Erhaltung begründen).

[120] Die endgültige Bewertung, ob ein Verdacht nach § 32 Absatz 1 der Wehrdisziplinarordnung vorliegt, sowie die ggf. anschließende Aufnahme disziplinarer Ermittlungen obliegt dem bzw. der zuständigen Disziplinarvorgesetzten.

- trifft notwendige Entscheidungen, damit eigene oder angewiesene Maßnahmen zur Behandlung von InfoSichhVork in seinem bzw. ihrem Zuständigkeitsbereich angemessen umgesetzt werden können.
- veranlasst die Beseitigung der Mängel.
- regelt grundsätzlich oder im Einzelfall die Kompetenzen des bzw. der ISB in seinem bzw. ihrem Anwendungsbereich, damit oft zeitkritische InfoSichhVork angemessen behandelt werden können und Schäden vermieden bzw. gering gehalten werden.

814. Sind andere Anwendungsbereiche (z.B. Projekte, vgl. Nr. 402) im Rahmen von Maßnahmen zur Eindämmung oder Schadensbeseitigung eines InfoSichhVork betroffen, so sind die verantwortlichen Rollenträgerinnen und Rollenträger (z.B. Ltr IPT / ProjLtr) für die Beseitigung InfoSichh-Mängel, für die notwendige Fortschreibung des InfoSichhK (z.B. InfoSichhKProj gemäß Abschnitt 6.3.2.3) und ggf. Einschränkung oder Aufhebung der Freigabe (siehe Nr. 561) verantwortlich.

815. Die weiteren detaillierten Aufgaben und Zuständigkeiten sind der A-960/5 „Behandlung von Informationssicherheitsvorkommnissen und Unterstützung von disziplinaren und strafrechtlichen Ermittlungen“ (siehe Bezug Anlage 11.15 (lfdNr. 59)) zu entnehmen.

8.4 Sofortmeldung, Zwischenbericht und Abschlussbericht zu einem Informationssicherheitsvorkommnis

816. Durch eine Sofortmeldung soll sichergestellt werden, dass schnellstmöglich evtl. notwendige Maßnahmen zum Schutz, zur Beweissicherung und ggf. zur Notfall- / Krisenbewältigung veranlasst werden können.

817. Sofortmeldungen sowie Zwischen- und Abschlussberichte sind an CSOCBw abzusetzen[121][122]. CSOCBw informiert alle weiteren relevanten Stellen (z. B. CISOBw, MAD, zuständige ISBOrgBer / ISBEinsatz, betroffene ISBBtrb, ISB HERKULES (falls IT aus dem durch die BWI betriebene IT betroffen ist), DEUmilSAA (falls akkreditierte IT betroffen ist), BMVg SE I 1, BMVg R II 4 / BfDBw und BMVg R I 7 (sofern PersDat SB 2 oder 3 betroffen sind), BMVg R II 6 / ES (Ermittlung in Sonderfällen) bei Verdacht einer Korruptionsstraftat[123]).

[121] Mit Ausnahme BMVg und BAMAD.

[122] Gilt nicht für Sicherheitsvorkommnisse im Kryptowesen, siehe Nr. 810. „Sofortmeldungen Kontingent“ mit möglichem InfoSichh-Bezug sind nachrichtlich an CSOCBw zu melden.

[123] Bei den Korruptionsstraftatbeständen bzw. des am Anfang stehenden Verdachts einer solchen Straftat, die eine Beteiligung BMVg R II 1 einfordern, handelt es sich um die Straftatbestände der Vorteilsannahme (§ 331 Strafgesetzbuch) und der Bestechlichkeit (§ 332 Strafgesetzbuch).
Die Einbindung BMVg R II 1 erfolgt im Einklang mit der Meldeverpflichtung nach dem Meldewesen Innere und Soziale Lage der Bundeswehr (Zentrale Dienstvorschrift A-2640/34, dort Nr. 337), welche eine Benachrichtigung BMVg R II 1 bei den Straftaten im Amt (dazu gehören die Vorteilsannahme und die Bestechlichkeit) festlegt, sowie im Einklang mit der anlässlich des Eintritts in den GB BMVg vorgenommenen "Belehrung über mögliche Korruptionsgefahren und Folgen korrupten Verhaltens" (Vordruck Bw/2611 in der Formulardatenbank der Bundeswehr).
Aus diesem Belehrungsvordruck können weitere allgemeine Informationen entnommen werden

818. Die Sofortmeldung sowie die gesamte weitere Dokumentation zum InfoSichhVork (einschließlich Zwischenbericht und Abschlussbericht) erfolgen grundsätzlich in einem von CSOCBw bereitgestellten Meldeportal[124]. Falls das Meldeportal nicht verfügbar ist, kann alternativ per E-Mail an CSOCBw@bundeswehr.org oder per Telefon[125] gemeldet werden.

819. Die Inhalte von Sofortmeldung, Zwischenbericht und Abschlussbericht sind in der A-960/5, Abschnitt 2.4.5 und 2.4.6 (siehe Bezug Anlage 11.15 (lfdNr. 59)) beschrieben.

8.5 Weitere Meldungen

820. Der bzw. die Verantwortliche für die InfoSichh im Anwendungsbereich (i.d.R. DStLtr / KtgtFhr / ProjLtr) prüft, ob das InfoSichhVork auch

- als leitungsrelevantes Ereignis gemäß Zentraler Dienstvorschrift A-200/5 VS-NfD „Meldewesen der Bundeswehr“ im Rahmen „Meldewesen Besondere Vorkommnisse“ (MW BV), „Einsatzmeldewesen der Bundeswehr“ (EinsMWBw) oder „Territoriales Meldewesen der Bundeswehr“ (TerrMWBw) zu melden ist. Einen Kriterienkatalog „Leitungsrelevante Ereignisse“ mit Beispielen gibt die Zentrale Dienstvorschrift A-200/5 in der Anlage 7.1 vor (z.B. bei wesentlichen Ereignissen im Bereich „Cyber-Sicherheit“ oder Vorkommnissen, welche die Führungsfähigkeit der Bw erheblich einschränken).
- im Rahmen eines anderen Aufgaben- und fachbezogenen Meldewesens meldepflichtig ist (z.B. bei Verdacht auf Straftaten von Bundeswehrangehörigen oder Verdacht auf Spionage gemäß Zentraler Dienstvorschrift A-2640/34 VS-NfD „Meldewesen Innere und Soziale Lage der Bundeswehr“ (siehe Bezug Anlage 11.15 (lfdNr. 18) bzw. Meldung nach Art. 33/34 EU-DSGVO (siehe Bezug Anlage 11.15 (lfdNr. 65)).
- als Sicherheitsvorkommnis gemäß Zentralerlass B-1130/32 VS-NfD „Melde-, Berichts- und Informationswege zur Erstellung der Militärischen Sicherheitslage der Bundeswehr“ (siehe Bezug Anlage 11.15 (lfdNr. 63)) (z.B. bei Verlust von Daten der Einstufung VS-VERTRAULICH und höher sowie vergleichbarer NATO- / EU-Einstufungen bzw. Einstufungen anderer Nationen, sonstiger überstaatlicher Organisationen oder „MISSION“ [126]) zu melden ist. Als Hilfe zur Erstellung der Meldung kann die Zentralrichtlinie A2-1130/1-0-1 VS-NfD „Militärische Sicherheit in der Bundeswehr - Arbeitshilfe Sicherheitsvorkommnis“ (siehe Bezug Anlage 11.15 (lfdNr. 64)) genutzt werden. Hinweis für zivile Organisationsbereiche: Gemäß Bereichsdienstvorschrift C-1130/12 VS-NfD „Meldungen bei Sicherheitsvorkommnissen sowie bei Vorkommnissen und Erkenntnissen, die mit der regionalen Sicherheitslage erfasst werden“ (siehe Bezug Anlage 11.15 (lfdNr. 41)) sind

[124] https://marvin.bundeswehr.org
[125] 90-3405-1245 oder +49 (0)2226 88 1245
[126] „*MISSION*“ ist der Platzhalter für eine spätere konkrete Benennung und setzt eine sog. *Security Policy* für den beabsichtigten Einsatz voraus. Insofern ist z.B. MISSION SECRET keine gültige Einstufung, sondern z. B. NATO / ISAF SECRET oder NATO SECRET Releasable to ISAF.

InfoSichhVork durch den zuständigen SichhBeauftr zugleich als Sicherheitsvorkommnis zu behandeln.

- gemäß anderer Befehle, Regelungen oder Verpflichtungen zu melden ist.

8.6 Beteiligung des Militärischen Abschirmdienstes

821. Liegt bei einem Vorkommnis / InfoSichhVork ein Hinweis auf extremistische / terroristische Bestrebungen oder sicherheitsgefährdende oder geheimdienstliche Tätigkeiten vor, hat der bzw. die SichhBeauftr die Federführung (siehe auch Nr. 812). Die Übernahme der federführenden Bearbeitung durch den MAD ist unverzüglich zwischen dem bzw. der SichhBeauftr und dem BAMAD abzustimmen[127]. Übernimmt der MAD die Bearbeitung, meldet der bzw. die Verantwortliche für InfoSichh im Anwendungsbereich (i.d.R. DStLtr / KtgtFhr / ProjLtr) lediglich an den bzw. die CISOBw die Übernahme eines InfoSichhVork durch den MAD. BAMAD zeigt die Übernahme unverzüglich bei CISOBw an und CISOBw und BAMAD stimmen sich bzgl. weitergabefähiger Informationen des InfoSichhVork ab, damit notwendige InfoSichh-Maßnahmen im IT-SysBw festgelegt und umgesetzt werden können. Eine Sofortmeldung bzw. Meldung an andere DSt / Bereiche darf in diesen Fällen nur nach Abstimmung zwischen dem bzw. der SichhBeauftr und dem BAMAD erfolgen (sofern das Vorkommnis nicht bereits in der Öffentlichkeit bekannt geworden ist). Übernimmt der MAD erst nach erfolgter Meldung eines InfoSichhVork die Bearbeitung, trägt der Federführende für die Behandlung des InfoSichhVork dies im Meldeportal ein.

822. Mit Übernahme der Bearbeitung des InfoSichhVork durch den MAD ist dieser federführend und verantwortlich für die Koordination aller weiteren Maßnahmen. Wenn die Bearbeitung beim MAD mangels Hinweisen auf extremistische / terroristische Bestrebungen oder sicherheitsgefährdende oder geheimdienstliche Tätigkeiten eingestellt wird, gibt der MAD die Bearbeitung des InfoSichhVork an CSOCBw zurück.

[127] Für Meldungen an den MAD ist die LotusNotes Adresse „MAD-ITSiVoKo“ zu nutzen. Bei Einstufung höher als VS-NfD ist die Meldung über NuKomBw NK-A abzusetzen.

9 Aufgabenbeschreibungen

9.1 Chief Information Security Officer Ressort

901. Der bzw. die CISO Ressort nimmt die Aufgaben für den gesamten GB BMVg wahr und ist in Angelegenheiten der InfoSichh im gesamten GB BMVg weisungsbefugt. Er hat ein direktes Vortragsrecht bei der Leitung des BMVg. Dieses schließt die Befugnis zur Durchführung und Anordnung von InfoSichhIn, InfoSichhKtr und InfoSichhPrfg ein.

Der bzw. die CISO Ressort hat folgende Aufgaben:

- Gewährleisten der InfoSichh des Ressorts.
- Herausgeben zentraler Regelungen zur InfoSichh für den GB BMVg.
- Etablieren und Leiten eines „Steuerkreises Informationssicherheit“ zur Koordination der Bereiche Cyber- / InfoSichh sowie der IT-relevanten Anteile der Bereiche Datenschutz, Geheimschutz und Militärische Sicherheit auf ministerieller Ebene.
- Beraten der Leitung hinsichtlich der InfoSichh unter Hinzuziehung der aktuellen Cyber- / Informationssicherheitslage.
- Erlassen von Vorgaben im Rahmen seiner bzw. ihrer Governance-Funktion zur InfoSichh inkl. IT-RM unter Nutzung des etablierten Informationssicherheitsmanagementsystems[128] (ISMS) gem. Umsetzungsplan des Bundes. Dieses beinhaltet u.a.:
  + Fortschreiben des Prozesses des Informationssicherheitsmanagements.
  + Koordinieren und Steuern des Prozesses IT-Risikomanagements für das Ressort BMVg
  + Erlassen zentraler Vorgaben zur InfoSichh sowie Steuern und Überwachen der InfoSichh im GB BMVg einschließlich Weisungs- und Kontrollrechten.
  + Veranlassen, Koordinieren und Steuern aller erforderlichen ressortübergreifenden Maßnahmen zur InfoSichh gemäß Konzept IT-Steuerung Bund, Umsetzungsplan Bund (siehe Bezug Anlage 11.15 (lfdNr. 45)), Cyber-Sicherheitsstrategie für Deutschland (siehe Bezug Anlage 11.15 (lfdNr. 44)) und IT-Krisenmanagement des Bundes.
  + Zulassen von im GB BMVg verwendeten InfoSichh-Produkten für die VS-Verarbeitung und -Übertragung.

[128] Hierbei handelt es sich um das Zusammenspiel der Organisationselemente, Anwendungsbereiche, Rollenträgerinnen und Rollenträger, Regelungskompetenzen, Verfahren und Zuständigkeiten im Rahmen des Informationssicherheitsmanagementprozesses (Nr. 109) gemäß dieser Zentralen Dienstvorschrift.

Der bzw. die CISO Ressort ist in allen Angelegenheiten der InfoSichh (einschließlich der Kryptomittelsicherheit) im GB BMVg weisungsbefugt. Hierbei hat er die Fachaufsicht über

- die Informationssicherheitsorganisation des GB BMVg; dies schließt insbesondere das ZCSBw mit seinen Anteilen der Kryptoorganisation, des Abstrahlprüfwesens, des Trustcenters der Bw, der Public Key Infrastruktur der Bundeswehr (PKIBw) sowie des Prüfzentrums InfoSichh der Bundeswehr (PZITSichhBw) mit ein und
- das Krisenmanagement im GB BMVg bei definierten InfoSichh-Risiken für das IT-SysBw oder bei IT-Krisen unter Berücksichtigung des IT-Krisenmanagements des Bundes.

9.2 Chief Information Security Officer der Bundeswehr

902. Der bzw. die CISOBw hat folgende Aufgaben:

- Steuern und Überwachen aller operativen Aufgaben zur Gewährleistung der InfoSichh inkl. IT-Risikomanangement (einschließlich der IT-relevanten Anteile des Datenschutzes, des Geheimschutzes und der Militärischen Sicherheit) in der Bw im Auftrag des CISO Ressort unter direktem Rückgriff auf das ZCSBw.
- Verantworten der Rolle des IT-Risikomanagers bzw. der IT-Risikomanagerin der Bundeswehr.
- Herausgeben von zentralen Durchführungsbestimmungen zur InfoSichh inkl. IT-RM für den GB BMVg.
- Vertreten der deutschen Interessen in bi- und multinationalen Gremien zur InfoSichh (z. B. NATO, EU), soweit nicht durch BMVg wahrgenommen.
- Erstellen und Herausgeben des Jahresberichtes zur Lage der InfoSichh in der Bw.
- Überwachen der InfoSichh (einschließlich der Kryptosicherheit und der Abstrahlsicherheit) im gesamten GB BMVg durch Bewerten der bundeswehrgemeinsamen Informationssicherheitslage und Identifizieren und Bewerten übergreifender (systemischer) IT-Risiken.
- Führen der bundeswehrgemeinsamen Informationssicherheitslage inkl. der IT-Risikolandkarte für das IT-SysBw.
- Steuern aller zentralen Überwachungsaufgaben des ZCSBw.
- Setzen von Schwerpunkten für Inspektionen und Schwachstellenanalysen des ZCSBw.
- Setzen von Schwerpunkten für die InfoSichh-Awareness in der Bw.
- Einsetzen der Incident Response Teams des ZCSBw bei Verdacht oder in Reaktion auf eine schwerwiegende Beeinträchtigung der InfoSichh in allen DSt / EinsKtgt / EinsStO der Bw („Incident Response“).
- Einsetzen der Penetration Test Teams des ZCSBw zur Durchführung von erweiterten Überprüfungen der InfoSichh in Projekten / DSt / EinsKtgt / EinsStO.

- Einsetzen der Red Teams des Zentrums für Cyberoperationen zur Durchführung von erweiterten Überprüfungen der InfoSichh in allen DSt / EinsKtgt / EinsStO der Bw sowie nach Absprache auch bei zivilen Providern.
- Beauftragen der ISBOrgBer und des ISBEinsatz mit der Durchführung von InfoSichhKtr in deren Zuständigkeitsbereich.
- Veranlassen von InfoSichhPrfg zur Aufklärung von InfoSichh-Verstößen und -Lücken.
- Erteilen von Ausnahmegenehmigungen bei der Besetzung von ISB in der Bw.
- Auswerten und Bewerten von Erkenntnissen allgemeiner und übergreifender Bedeutung für die InfoSichh in der Bw unter Berücksichtigung der seitens des ZCSBw zugearbeiteten bundeswehrgemeinsamen Informationssicherheitslage, Handlungsempfehlungen und Erkenntnissen aus bearbeiteten InfoSichhVork sowie Einleiten von Folgemaßnahmen insb. bei erkannten Mängeln.
- Leiten des Krisenmanagement-Boards bei hohen InfoSichh-Risiken für das IT-SysBw oder bei IT-Krisen gemäß IT-Krisenmanagement des Bundes.
- Erstellen und Herausgeben von für die OrgBer und Einsatzkontingente verbindlichen Vorgaben, Weisungen zur InfoSichh und Warnhinweisen zur Gewährleistung der InfoSichh.
- Erteilen von verbindlichen Vorgaben an alle mit IT-Betriebsaufgaben befassten DSt / EinsKtgt der Bw bei Routineangelegenheiten zur InfoSichh unter Beteiligung des EinsFüKdoBw für EinsKtgt sowie der betroffenen ISBOrgBer.
- Anerkennen von im GB BMVg verwendeten InfoSichh-Produkten für die VS-Verarbeitung und -Übertragung.
- Absetzen von Meldungen gemäß der Allgemeinen Verwaltungsvorschrift für das Meldeverfahren gem. § 4 Abs. 6 BSI-Gesetz.
- Auswerten einschlägiger Informationen (z. B. IT-Rat, BMI, BSI, Fachgremien, Industrie) zur InfoSichh mit Bedeutung für das IT-SysBw.
- Auswerten der durch die ISBOrgBer und den bzw. die ISBEinsatz übermittelten Übersichten zur Ausbildung der jeweiligen ISB und Einleiten von Maßnahmen bei Mängeln.
- Regelmäßiges Abstimmen mit den ISBOrgBer und dem ISBEinsatz.

9.3 Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte Organisationsbereich, Bundesministerium der Verteidigung, Militärischer Abschirmdienst und Einsatz (F, W, D, E)

903. Die ISBOrgBer[129] (einschl. ISBBMVg und ISBMAD) sowie der bzw. die ISBEinsatz haben folgende Aufgaben:

- Beraten des bzw. der bestellenden Vorgesetzten in allen Fragen zur InfoSichh inkl. IT-RM und der IT-relevanten Anteile des Datenschutzes, des Geheimschutzes und der Militärischen Sicherheit in ihrem Zuständigkeitsbereich bzw. in den EinsKtgt.
- Verantworten der Rolle eines IT-Risikomanagers bzw. einer IT-Risikomanagerin für seinen bzw. ihren Zuständigkeitsbereich.
- Erstellen von Beiträgen zur IT-Risikolandkarte.
- Unterstützen aller Verantwortlichen im OrgBer bei der Erstellung / Fortschreibung von InfoSichhKDSt, InfoSichhKFW und InfoSichhBef.
- Durchführen von InfoSichhIn und InfoSichhPrfg in ihrem Zuständigkeitsbereich (nur ISBBMVg und ISBMAD).
- Veranlassen der Durchführung von bzw. eigenes Durchführen von InfoSichhKtr zur Überwachung der InfoSichh in den DSt des Zuständigkeitsbereiches bzw. in den EinsKtgt (gemäß Nr. 727) und Erteilen von Vorgaben, Hinweisen und Handlungsanweisungen in Bezug auf InfoSichhKtr.
- Zu- und Mitarbeiten bei der Bearbeitung von InfoSichhVork mit Bedeutung für ihren Zuständigkeitsbereich.
- Auswerten und Bewerten von InfoSichhVork und von Ergebnissen aus Kontrolltätigkeiten im Zuständigkeitsbereich.
- Anlassbezogenes Übermitteln von für das IT-SysBw relevanten Erkenntnissen zur InfoSichh an den bzw. die CISOBw.
- Überwachen der InfoSichh im Zuständigkeitsbereich durch Zugriff auf die durch ZCSBw bereitgestellten zentralen Lagedaten und Auswertung hinsichtlich Relevanz für den jeweiligen Zuständigkeitsbereich.
- Anweisen von DSt seines bzw. ihres Zuständigkeitsbereiches, Sofortmeldungen gemäß Abschnitt 8 bzw. Empfehlungen an DSt seines bzw. ihres Zuständigkeitsbereiches „Weitere Meldungen“ gemäß Abschnitt 8.5 abzusetzen (vgl. hierzu auch Nr. 701).
- Wahrnehmen der Aufgaben gemäß A-960/15 „IT-Krisenmanagement in der Bundeswehr“ (siehe Bezug Anlage 11.15 (lfdNr. 47)).

[129] Der bzw. die ISBSKB zusätzlich für alle dem Generalinspekteur bzw. der Generalinspekteurin unmittelbar unterstellten Dienststellen

- Zuarbeiten bei der Erarbeitung, Koordinierung und Herausgabe von organisationsbereichs- bzw. einsatzspezifischen Hinweisen und Vorgaben zur InfoSichh bzw. einsatzspezifischen Hinweisen zur InfoSichh des bzw. der CISOBw zur Einhaltung und Wiederherstellung der InfoSichh im Zuständigkeitsbereich bzw. im Einsatz bei aktuellen InfoSichhVork oder sonstigem Handlungsbedarf.
- Identifizieren von organisationsbereichsspezifischen Regelungslücken zur InfoSichh und Erstellen von Vorgaben, Hinweisen und Handlungsanweisungen im jeweiligen Zuständigkeitsbereich zu diesen Lücken. Melden identifizierter organisationsbereichsübergreifender Regelungslücken an den bzw. die CISOBw.
- Vorlegen eines Beitrages zum Jahresbericht zur Lage der InfoSichh in der Bw für seinen bzw. ihren Zuständigkeitsbereich an den bzw. die CISOBw[130] zum 15. Februar eines jeden Jahres bezogen auf das Vorjahr gem. Nr. 650 nach Vorgaben des CISOBw.
- Mitwirken bei der Priorisierung der Lehrgangsteilnahmen des InfoSichh-Personals ihres Zuständigkeitsbereiches für folgende Lehrgänge: Kryptoverwalter, Prüfung von Kryptoverwaltungen, Informationssicherheitsbeauftragte, Informationssicherheitsbeauftragte Projekt, Informationssicherheitsgehilfen.
- Erteilen von Ausnahmegenehmigungen für die Bestellung von InfoSichhGeh.
- Mitwirken bei der Registrierung und Freigabe von dezentralen Netzübergängen gem. A-960/11 „Registrierung und Freigabe von dezentralen Netzübergängen“ (siehe Bezug Anlage 11.15 (lfdNr. 48)).
- Mitzeichnen von InfoSichhBef organisationsbereichs- / einsatzspezifischer Übungen (siehe Nr. 646).
- Teilnehmen an nationalen und internationalen Fachtagungen im Bereich InfoSichh.
- Durchführen des Sicherheitsauditings in den DEU EinsKtgt (nur ISBEinsatz).

9.4 Chief Information Security Officer Rüstung (P, O, S)

904. Der bzw. die CISO Rüstung im Bundesamtes für Ausrüstung, Informationstechnik und Nutzung (BAAINBw) hat folgende Aufgaben:

- Beraten der Leitung des BAAINBw und aller ProjLtr im BAAINBw in allen projekt- / programmbezogenen[131] Fragen zur InfoSichh inkl. IT-RM.
- Verantworten der Rolle eines IT-Risikomanagers bzw. einer IT-Risikomanagerin für seinen bzw. ihren Zuständigkeitsbereich.
- Erstellen von Beiträgen zum IT-Risikokatalog.

[130] ISBBMVg legt den Beitrag BMVg CIT II 2, ISBMAD BMVg R II 5 vor
[131] hier und fortfolgend: einschl. komplexe Dienstleistungen

- Umsetzen von Grundsatzregelungen des bzw. der CISO Ressort und des bzw. der CISOBw zur InfoSichh in Weisungen für die Projekte im BAAINBw.
- Auswerten der InfoSichhKProj, sowie darüber hinaus vorliegende Erkenntnisse, wie zum Beispiel Meldungen und Inspektionsberichte.
- Führen einer Übersicht über alle InfoSichhKProj in Verantwortung des OrgBer AIN und ggf. Nachsteuern bzgl. Erstellung und Aktualität unmittelbar bei den Projekten.
- Auswerten der durch ZCSBw bereitgestellten zentralen Lagedaten hinsichtlich Relevanz für den jeweiligen Zuständigkeitsbereich.
- Erstellen eines Beitrages zur bundeswehrgemeinsamen Informationssicherheitslage des CISOBw (Teillage InfoSichh Rüstung / Nutzung).
- Analysieren und Bewerten der Informationssicherheitsarchitektur der Bw basierend auf den operationellen Vorgaben des KdoCIR.
- Weiterentwickeln der Lösungsarchitektur zur InfoSichh im Zusammenwirken mit dem Systemarchitekt IT-SysBw und dem IT-Service Designer.
- Überwachen der Einhaltung der Vorgaben durch die Projektleitung im Rahmen der InfoSichh u.a. durch Veranlassung bzw. Durchführung von InfoSichhIn.
- Anordnen und Überwachen der Umsetzung von InfoSichh-Advisories im Rahmen der Verantwortung des Präsidenten bzw. der Präsidentin BAAINBw für den Erhalt der Einsatzreife.
- Koordinieren projektübergreifender Maßnahmen zum Obsoleszenzmanagement, sofern sie die InfoSichh betreffen.
- Teilnehmen an nationalen und internationalen Fachtagungen im Bereich InfoSichh.
- Vorlegen eines Beitrages zum Jahresbericht zur Lage der InfoSichh in der Bw für seinen bzw. ihren Zuständigkeitsbereich an den bzw. die CISOBw zum 15. Februar eines jeden Jahres bezogen auf das Vorjahr gem. Nr. 650 nach Vorgaben des bzw. der CISOBw.

9.5 Chief Information Security Officer Infrastruktur (V)

905. Der bzw. die CISO Infrastruktur im Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen der Bw (BAIUDBw) hat folgende Aufgaben:

- Beraten der Leitung des BAIUDBw und aller Verantwortlichen für Infra-Maßnahmen im BAIUDBw in allen Fragen zur InfoSichh inkl. IT-RM.
- Verantworten der Rolle eines IT-Risikomanagers bzw. einer IT-Risikomanagerin für seinen bzw. ihren Zuständigkeitsbereich.
- Erstellen von Beiträgen zum IT-Risikokatalog.
- Umsetzen von Grundsatzregelungen des bzw. der CISO Ressort und des bzw. der CISOBw zur InfoSichh in Weisungen für die Infrastrukturprojekte der Bw.

- Auswerten der InfoSichhKProj des BAIUDBw, sowie darüber hinaus vorliegende Erkenntnisse, wie zum Beispiel Meldungen und Inspektionsberichte.
- Führen einer Übersicht über alle InfoSichhKProj in Verantwortung des OrgBer IUD und ggf. Nachsteuern bzgl. Erstellung und Aktualität unmittelbar bei den Verantwortlichen für Infra-Maßnahmen.
- Auswerten der durch ZCSBw bereitgestellten zentralen Lagedaten hinsichtlich Relevanz für den jeweiligen Zuständigkeitsbereich.
- Erstellen eines Beitrages zur bundeswehrgemeinsamen Informationssicherheitslage des CISOBw (Teillage InfoSichh Infrastruktur).
- Überwachen der Einhaltung der Vorgaben durch die Verantwortlichen für Infra-Maßnahmen im Rahmen der InfoSichh u.a. durch Veranlassung bzw. Durchführung von InfoSichhIn.
- Koordinieren projektübergreifender Maßnahmen zum Obsoleszenzmanagement, sofern sie die InfoSichh betreffen.
- Teilnehmen an nationalen und internationalen Fachtagungen im Bereich InfoSichh.
- Vorlegen eines Beitrages zum Jahresbericht zur Lage der InfoSichh in der Bw für seinen bzw. ihren Zuständigkeitsbereich an den bzw. die CISOBw zum 15. Februar eines jeden Jahres bezogen auf das Vorjahr gem. Nr. 650 nach Vorgaben des bzw. der CISOBw.

9.6 Informationssicherheitsbeauftragter bzw. Informationssicherheits-beauftragte Projekt / Forschung und Wissenschaft (F, W, P, V, O, S)

906. Die ISBProj bzw. ISBFW haben folgende Aufgaben:

- Beraten des bzw. der Ltr IPT / ProjLtr bzw. des bzw. der Leitenden des jeweiligen Vorhabens in allen Belangen der InfoSichh inkl. IT-RM des Projekts bzw. Vorhabens.
- Erstellen / Fortschreiben des InfoSichhKProj bzw. InfoSichhKFW.
- Prüfen der Rechtsgrundlage für die Verarbeitung personenbezogener Daten auf Vorhandensein der erfolgten Anmeldung im Verfahrensverzeichnis sowie der ggf. notwendigen Datenschutz-Folgenabschätzung (Erstellung gem. Anlage 11.15 (lfdNr. 10) durch den bzw. die zuständigen ADSB).
- Prüfen des InfoSichhKProj bzw. InfoSichhKFW, sofern extern erstellt.
- Beantragen einer Akkreditierung gemäß Abschnitt 5.5.4 im Auftrag des Ltr IPT / ProjLtr bzw. des bzw. der Leitenden für das Vorhaben.
- Prüfen der Verfügbarkeit notwendiger zugelassener InfoSichh-Produkte und ggf. Beantragen notwendiger Zulassungen.
- Führen der InfoSichhDok in dem für das Projekt erforderlichen Umfang.
- Abstimmen mit dem bzw. der jeweils zuständigen SichhBeauftr und ADSB und dem bzw. der Bevollmächtigten Vertreter bzw. Vertreterin (BV) des (potenziell / zukünftig) nutzenden OrgBer im

IPT in Bezug auf die Projektelemente „Informationssicherheit, IT-Architektur / -Standardisierung und Datenschutz“ sowie „Militärische Sicherheit“ (nur ISBProj).

- Prüfen und Abnehmen der technischen InfoSichh-Maßnahmen gemäß InfoSichhKProj / InfoSichhKFW.
- Empfehlen der Freigabe zur Nutzung von IT (verfahrensbezogene Freigabe) gemäß Nr. 563 nach Durchführung der erforderlichen Prüfungen.
- Koordinieren der projektbezogenen Aufgaben der InfoSichh mit dem bzw. der BV des (potenziell / zukünftig) nutzenden OrgBer im IPT in Abstimmung mit der DEUmilSAA (nur ISBProj).
- Überprüfen geänderter / neuer InfoSichh-Maßnahmen des Projektes bzw. Vorhabens.
- Empfehlen der Freigabe zur Nutzung von IT (Freigabe in der Nutzung) gemäß Abschnitt 5.6.4 nach Durchführung der erforderlichen Prüfungen (nur ISBProj).
- Bearbeiten von InfoSichhVork im Projekt bzw. Vorhaben gem. Nr. 812.
- Teilnehmen an nationalen und internationalen Fachtagungen im Bereich InfoSichh.

9.7 Informationssicherheitsbeauftragter bzw. Informationssicherheits-beauftragte Dienststelle und im Einsatzgebiet (D, E, Ü)

907. Die ISBDSt / ISB i.E.[132] haben folgende Aufgaben:

- Beraten des bzw. der DStLtr / KtgtFhr / Kdr EinsStO in allen Fragen zur InfoSichh inkl. IT-RM sowie der IT-relevanten Anteile des Datenschutzes, des Geheimschutzes und der Militärischen Sicherheit.
- Verantworten der Rolle eines IT-Risikomanagers bzw. einer IT-Risikomanagerin für seinen bzw. ihren Zuständigkeitsbereich.
- Erstellen von Beiträgen zum IT-Risikokatalog.
- Erarbeiten und Fortschreiben des InfoSichhK für die DSt / das EinsKtgt unter Berücksichtigung der Vorgaben aus den InfoSichhK der genutzten IT (z.B. InfoSichhKProj, InfoSichhKFW).
- Prüfen der Rechtsgrundlage für die Verarbeitung personenbezogener Daten, auf Vorhandensein der erfolgten Anmeldung im Verfahrensverzeichnis sowie der ggf. notwendigen Datenschutz-Folgenabschätzung (Erstellung gem. Anlage 11.15 (lfdNr. 10) durch den bzw. der zuständigen ADSB).
- Umsetzen von Vorgaben des bzw. der ISBBtrb zur Einhaltung und Wiederherstellung der InfoSichh in den Betriebsprozessen aller IT-Services im IT-SysBw. Vorgaben für die Einsatzgebiete sind mit dem bzw. der ISBEinsatz abzustimmen.
- Prüfen der personellen, infrastrukturellen und organisatorischen InfoSichh-Maßnahmen gemäß InfoSichhKDSt. Der bzw. die ISB i.E. prüft zusätzlich die technischen InfoSichh-Maßnahmen gemäß der InfoSichhKProj.

[132] diese Aufgaben gelten für den bzw. die ISBÜb analog

- Empfehlen der Freigabe zur Nutzung von IT (operationelle Freigabe) gemäß Nr. 571 sowie der Freigabe in der Nutzung gemäß Nr. 574 nach Durchführung der erforderlichen Prüfungen.
- Anwenden / Umsetzen von Vorschriften und Weisungen zur InfoSichh (einschl. der Vorschriften und Weisungen zum Datenschutz und zum Geheimschutz), ggf. Erstellen von konkreten Handlungsanweisungen, soweit Besonderheiten seiner bzw. ihrer DSt oder seines bzw. ihres EinsKtgt dies fordern.
- Durchführen von Informationssicherheitsbelehrungen für Personal der DSt / des EinsKtgt.
- Weiterbilden / Sensibilisieren des IT-Personals und der IT-Anwender.
- Durchführen von InfoSichhKtr zur Überwachung der InfoSichh in der eigenen DSt / im eigenen EinsKtgt; dies schließt Kontrollen der in den DSt / im EinsKtgt genutzten IT nach Vorgabe der InfoSichhK ein.
- Unterstützen bei der Durchführung von InfoSichhIn und InfoSichhPrfg im eigenen Zuständigkeitsbereich.
- Bearbeiten von InfoSichhVork und Kryptoverstößen gem. Nr. 812.
- Führen der InfoSichhDok in dem für seine bzw. ihre DSt oder sein bzw. ihr EinsKtgt erforderlichen Umfang.
- Prüfen der Kryptotagebücher der Dienststelle gemäß Zentraler Dienstvorschrift A-961/1 VS-NfD „Kryptosicherheit in der Bundeswehr“ (siehe Bezug Anlage 11.15 (lfdNr. 20)) jährlich bzw. bei Kontingentwechsel.
- Überwachen der ordnungsgemäßen Durchführung der Kryptoverwaltung der DSt / des EinsKtgt gemäß Zentraler Dienstvorschrift A-961/1 VS-NfD „Kryptosicherheit in der Bundeswehr“ (siehe Bezug Anlage 11.15 (lfdNr. 20)).
- Überwachen des ordnungsgemäßen Einsatzes und Betriebs von Kryptomitteln der DSt / des EinsKtgt.
- Wahrnehmen der Aufgaben des COMSEC-Officers für die DSt / das EinsKtgt gemäß SDIP 293/1 NATO RESTRICTED „Instructions for the control and safeguarding of NATO cryptomaterial“ (siehe Bezug Anlage 11.15 (lfdNr. 33)) beim Einsatz von NATO-Kryptomitteln.
- Wahrnehmen weiterer Aufgaben im Bereich des Kryptowesens gemäß Zentraler Dienstvorschrift A-961/1 VS-NfD (insbesondere aus der Checkliste gemäß A-961/1 VS-NfD, dort Anlage 9.12).
- Zusammenarbeiten mit dem bzw. der jeweils zuständigen SichhBeauftr und ADSB.
- Übermitteln wesentlicher Erkenntnisse zur InfoSichh aus der DSt / dem EinsKtgt an den bzw. die ISBOrgBer / ISBEinsatz.
- Auswerten und Bewerten von Erkenntnissen aus den eigenen Kontrolltätigkeiten und den gemeldeten InfoSichhVork.
- Melden identifizierter Regelungslücken für die DSt / das EinsKtgt an den bzw. die ISBOrgBer / ISBEinsatz.
- Auswerten einschlägiger Informationen zur InfoSichh mit Bedeutung für die DSt / das EinsKtgt.

- Teilnehmen an nationalen und internationalen Fachtagungen im Bereich InfoSichh.
- Durchführen des Sicherheitsauditings in der DSt (nur ISBDSt).

908. Ein Muster einer Dienstanweisung für den bzw. die ISBDSt / ISB i.E. ist in der Anlage 11.8.5 enthalten.

9.8 Informationssicherheitsbeauftragter bzw. Informationssicherheits-beauftragte Betrieb (P, D, E)

909. Der bzw. die ISBBtrb haben folgende Aufgaben:

- Steuern und Überwachen aller technischen InfoSichh-Maßnahmen für die im Betrieb der jeweiligen IT-Btrb(Fü)Einr befindlichen IT-Services und Produkte.
- Auswerten von Erkenntnissen zur InfoSichh inkl. IT-RM mit Bedeutung für den Betrieb der jeweiligen IT-Btrb(Fü)Einr.
- Verantworten der Rolle eines IT-Risikomanagers bzw. einer IT-Risikomamagerin für seinen bzw. ihren Zuständigkeitsbereich.
- Erstellen von Beiträgen zum IT-Risikokatalog.
- Einleiten von geeigneten Maßnahmen, bei Einsatzrelevanz in enger Abstimmung mit dem bzw. der ISBEinsatz, auf Grundlage von Erkenntnissen mit Relevanz für die InfoSichh. Maßnahmen mit operationellen Auswirkungen sind immer im Rahmen des Demand bzw. Supply Managements zu entscheiden.
- Erarbeiten von Vorgaben zur Einhaltung und Wiederherstellung der InfoSichh in den Betriebsprozessen der in der jeweiligen IT-Btrb(Fü)Einr bereitgestellten IT-Services unter Berücksichtigung der Vorgaben des bzw. der CISOBw.
- Beraten des bzw. der DStLtr hinsichtlich der Berücksichtigung von Aspekten der InfoSichh bei der Bereitstellung und dem Betrieb von IT-Services durch die IT-Btrb(Fü)Einr.
- Zusammenarbeiten mit dem bzw. der ISBDSt und den ISBProj.
- Zusammenarbeiten mit allen für IT-Btrb(Fü)Einr zuständigen ISB.
- Abstimmen der Umsetzung von technischen InfoSichh-Maßnahmen mit den betroffenen ISB, bei Einsatzrelevanz über den bzw. die ISBEinsatz.
- Zusammenarbeiten mit den ISBAN vertraglich verpflichteter Unternehmen.
- Unterstützen bei der Durchführung von InfoSichhIn, InfoSichhKtr und InfoSichhPrfg zur Gewährleistung und ggf. Wiederherstellung der InfoSichh im Betrieb im eigenen Zuständigkeitsbereich.
- Einbringen von Erkenntnissen zur InfoSichh aus dem Betrieb in Initiativen und Projekte, die IT-Services für das IT-SysBw bereitstellen oder IT-Services im IT-SysBw in Anspruch nehmen sollen.
- Mitwirken bei der Erstellung von Freigabeempfehlungen (operationelle Freigabe gemäß Abschnitt 5.6.3 sowie Freigabe in der Nutzung gemäß Abschnitt 5.6.4).

- Identifizieren von Regelungsdefiziten mit Bedeutung für die InfoSichh im Betrieb und Meldung der Defizite an den bzw. die CISOBw unter Beteiligung der betroffenen ISBOrgBer oder des bzw. der ISBEinsatz.
- Mitwirken bei der Bearbeitung von InfoSichhVork.
- Anwenden / Umsetzen von nationalen und multinationalen Vorschriften und Weisungen zur InfoSichh im Betrieb.
- Koordinieren und Behandeln aller technischen Fragen der InfoSichh während des Betriebes.
- Bewertung des Systemauditings in der jeweiligen IT-Btrb(Fü)Einr.

9.9 Informationssicherheitsbeauftragter bzw. Informationssicherheits-beauftragte geheimschutzbetreute Wirtschaft (P, V, O, S)

910. Der bzw. die ISBGBW hat folgende Aufgaben (siehe Bezug Anlage 11.15 (lfdNr. 20)):

- Ausüben der Fachaufsicht Krypto / COMSEC gegenüber der geheimschutzbetreuten Wirtschaft derjenigen Unternehmen in der Bundesrepublik Deutschland, die Kryptomittel der Bw einsetzen.
- Initiieren, Beauftragen, Koordinieren und Durchführen von InfoSichhIn, InfoSichhKtr und InfoSichhPrfg bei Firmen der geheimschutzbetreuten Wirtschaft in Absprache mit dem Bundesministerium für Wirtschaft und Energie bezogen auf Krypto / COMSEC.
- Durchführen von „Ad-hoc“-Inspektionen aus besonderem Anlass zur Aufrechterhaltung bzw. Wiederherstellung der Kryptosicherheit.
- Durchführen von (Krypto-)Belehrungen der ISB bzw. SichhBeauftr in den Firmen der geheimschutzbetreuten Wirtschaft.
- Aus- und Weiterbilden im Geheimschutz für das InfoSichh-Personal (d. h. Kryptoverwalter bzw. ISB / SichhBeauftr) der mit nationalen und internationalen Kryptomitteln versorgten geheimschutzbetreuten Wirtschaft in Lehrgangsform an der IT-Schule der Bw.
- Zusammenarbeiten mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) in seiner Funktion als „EU NDA Germany“ hinsichtlich Kryptomittelversorgung der geheimschutzbetreuten Wirtschaft.
- Beraten der geheimschutzbetreuten Wirtschaft vor und bei Einrichtung / Eröffnung von Kryptobetriebsstellen / -verwaltungen und Abnahme / Kontrolle der Infrastruktur und IT-Ausstattung nach erfolgter Einrichtung / Eröffnung.
- Beraten und Unterstützen der geheimschutzbetreuten Wirtschaft bei Beantragung von Kryptomitteln.
- Beraten bei Erstellung und Überprüfung der Notfallplanung zum Schutz der eingesetzten und vorgehaltenen nationalen und internationalen Kryptomittel.
- Bearbeiten von InfoSichhVork / Sicherheitsvorkommnissen / Kryptoverstößen aus dem Bereich der geheimschutzbetreuten Wirtschaft.

- Beraten des bzw. der CISOBw und der ISBProj in Angelegenheiten der Kryptosicherheit und Kryptomittelversorgung (national und international) der geheimschutzbetreuten Wirtschaft.
- Teilnehmen an der Arbeitsgruppe der ISB / SichhBeauftr der geheimschutzbetreuten Wirtschaft.
- Erstellen und Fortschreiben der „Richtlinien zur Behandlung, Einsatz und Nutzung von Kryptomitteln der Bw, NATO sowie verbündeter Staaten in der geheimschutzbetreuten Wirtschaft“.

9.10 Informationssicherheitsgehilfen (D)

911. Die InfoSichhGeh als Unterstützung der ISBDSt in DSt mit umfangreicher IT-Ausstattung oder komplexer fachspezifischer IT-Ausstattung oder DSt, die stark disloziert sind[133], arbeiten unter Anleitung des ISBDSt und haben folgende Aufgaben:

- Mitwirken bei der Planung, Erarbeitung und Überwachung technischer, personeller, infrastruktureller und organisatorischer Maßnahmen zur Herstellung, Erhaltung und Wiederherstellung der InfoSichh inkl. IT-RM.
- Zuarbeiten bei der Erarbeitung und Fortschreibung des InfoSichhKDSt unter Berücksichtigung der InfoSichhKProj bzw. InfoSichhKFW der genutzten bzw. betriebenen IT.
- Mitarbeiten und Mitprüfen von Dokumenten zu Belangen der InfoSichh inkl. IT-RM in ihrem Zuständigkeitsbereich.
- Unterstützen bei InfoSichhKtr zur Überwachung von Maßnahmen zur Herstellung und Gewährleistung der InfoSichh in der eigenen DSt sowie im truppendienstlich und fachlich nachgeordneten Bereich.
- Unterstützen bei der Führung der InfoSichhDok.
- Mitwirken bei der Auswertung und Bewertung von Erkenntnissen aus den Inspektions-, Kontroll- und Prüftätigkeiten und den gemeldeten InfoSichhVork.
- Mitwirken bei der Auswertung einschlägiger Informationen zur InfoSichh mit Bedeutung für die DSt.
- Mitwirken bei der Empfehlung der Freigabe zur Nutzung von IT (operationelle Freigabe) gemäß Abschnitt 5.6.3 dieser Zentralen Dienstvorschrift (siehe Nr. 571) nach Durchführung der erforderlichen Prüfungen.
- Mitwirken bei der Abstellung von gemeldeten InfoSichh-Mängeln und InfoSichhVork.
- Mitarbeiten bei der Erstellung von IT-Notfallplänen / -handbüchern.
- Unterstützen bei InfoSichh-Belehrungen.
- Zusammenarbeiten mit dem InfoSichh-Personal, IT-Personal, Sicherheitspersonal und dem bzw. der ADSB.

[133] Gilt sinngemäß auch für die Unterstützung von ISB i.E. in EinsKtg

10 Ausbildung und Sensibilisierung

10.1 Ausbildung

10.1.1 Allgemeines

1001. Laufbahnlehrgänge und Führungslehrgänge aller Bundeswehrangehörigen, insbesondere IT-Lehrgänge, **müssen** der jeweiligen Ebene angepasste Ausbildungsanteile zur InfoSichh einschließlich der Thematik „Sensibilisierung für InfoSichh in der Bw“ berücksichtigen (siehe auch Abschnitt 10.2). Die Vermittlung soll im Zusammenhang mit den Grundlagen des Geheimschutzes erfolgen oder Anteile dazu enthalten, da der Geheimschutz bzgl. des Grundwertes Vertraulichkeit eine Basis für die InfoSichh-Maßnahmen bildet. Darüber hinaus sind IT-relevante Anteile des Datenschutzes zu berücksichtigen.

1002. Dem **Führungspersonal** sind die Grundlagen und besonderen Kenntnisse der InfoSichh, die in der Führungsverantwortung benötigt werden, zu vermitteln. Einen besonderen Schwerpunkt muss „Sensibilisierung für InfoSichh“ bilden. Diese Forderungen sind durch KdoCIR als Bedarfsträgerforderungen des OrgBer CIR an die OrgBer mit eigener Laufbahnausbildung (derzeit Heer, Luftwaffe und Marine) zu richten und aktuell zu halten. Gleiches gilt für die zivilen Laufbahnausbildungen.

1003. Für **IT-Personal** (siehe Begriffsbestimmungen in der Anlage 11.11) und **IT-Anwender** sind lehrgangsbezogen auf die Ausbildungshöhe und das Lehrgangsziel abgestimmte Anteile zu InfoSichh und Sensibilisierung für die InfoSichh einzuplanen.

1004. Das **IT-Personal** und alle **Rollenträgerinnen und Rollenträger** der InfoSichh gemäß Nr. 407, Abb. 9 müssen fach- und ebenen gerecht aus- und fortgebildet werden. Grundlage der Aus- und Fortbildung für InfoSichh ist diese Zentrale Dienstvorschrift.

1005. Für die **ISBDSt, ISB i.E., ISBProj, ISBBtrb und die InfoSichhGeh** sind insbesondere die Vorgaben gemäß Nr. 587 (Voraussetzungen) und Nr. 590 (Ausnahmen) zu beachten.

1006. Für **alle Rollenträgerinnen und Rollenträger** sind zusätzlich die Zentrale Dienstvorschrift A-961/1 VS-NfD „Kryptosicherheit in der Bundeswehr“, (siehe Bezug Anlage 11.15 (lfdNr. 20)) und die Zentrale Dienstvorschrift A-962/1 VS-NfD „Abstrahlsicherheit“ (siehe Bezug Anlage 11.15 (lfdNr. 21)) zugrunde zu legen.

1007. Auf der ministeriellen Ebene erfolgt die notwendige Steuerung der IT-Ausbildung federführend durch BMVg CIT I 2 unbeschadet der Gesamtverantwortung des Abteilungsleiters CIT im BMVg in seiner Funktion als Chief Information Officer (CIO).

1008. Federführende Stelle (FF-Stelle) auf der dem BMVg ersten nachgeordneten Ebene ist die Referatsgruppe InfoSichh im KdoCIR Abteilung Planung. Diese erarbeitet auf Grundlage dieser

Zentralen Dienstvorschrift Regelungen und konzeptionelle Vorgaben zur InfoSichh-Ausbildung und überwacht das diesbezügliche Gesamtsystem.

1009. KdoITBw Abteilung Ausbildung nimmt die Aufgaben der fachlich zuständigen Stelle (FZ-Stelle) für alle Trainingstypen der InfoSichh-Ausbildung wahr. Die FZ-Stelle ist für die inhaltliche Ausgestaltung in enger Abstimmung mit dem jeweiligen Bedarfsträger verantwortlich und hat dabei insbesondere folgende Aufgaben:

- Ermittlung des trainingstypspezifischen Ausbildungsbedarfs in Abstimmung mit der FF-Stelle und Eingabe der entsprechenden Planzahlen in IAMS,
- Veranlassung der Einrichtung und bedarfsgerechten Durchführung der gemäß dieser Zentralen Dienstvorschrift notwendigen Lehrgänge in Abstimmung mit der FF-Stelle aufgrund von durch die Bedarfsträger gemeldetem Ausbildungsbedarf,
- Sicherstellung der vollumfänglichen Bearbeitung der Dokumentenprozesse in IAMS und Hinterlegung dementsprechender Lehrpläne, sowie deren Zielhierarchien bzw. Lernfelder und Handlungsfelder entsprechend der kompetenzorientierten Ausbildung,
- Veranlassung der Einrichtung neuer Lehrgänge oder Änderung bestehender Lehrgänge auf Weisung oder in Abstimmung mit der FF-Stelle (vgl. Nr. 1008) und
- Identifizierung - in Ergänzung zu den bundeswehreigenen Lehrgängen - geeigneter Lehrgänge zur InfoSichh bzw. IT-Lehrgänge mit Anteilen zur InfoSichh der gewerblichen Wirtschaft und Abstimmung des Aus-, Fort- und Weiterbildungsbedarfs an zivilen Ausbildungseinrichtungen und Ausbildungseinrichtungen der Bw mit den ISBOrgBer.

1010. Digitale Ausbildungshilfsmittel (DigAHM) (vgl. Anlage 11.2.8 lfdNr. 26) wie z. B. der Cyber Hygiene Check Up sind im Rahmen der Ausbildung zu nutzen.

10.1.2 Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte Projekt und Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte Forschung und Wissenschaft (F, W, P, V, O, S)

1011. ISBProj sowie ISBFW sind für ihre Tätigkeit fachlich aus- und fortzubilden. Hierzu ist ein Lehrgang „**Informationssicherheitsbeauftragte Projekt“** zur Ausbildung von ISBProj und ISBFW einzurichten. Als Bedarfsträger ist vorrangig die DEUmilSAA in die Prozesse der Bearbeitung und Weiterentwicklung des Lehrgangs mit einzubeziehen.

1012. ISBProj und ISBFW sind zu befähigen, die InfoSichh in der Analyse und Realisierung von IT aus technischer, organisatorischer, infrastruktureller und personeller Sicht zu planen und aus technischer Sicht umzusetzen[134] sowie Vorgaben für die Nutzung von IT festzulegen.

[134] Die Umsetzung organisatorischer, infrastruktureller und personeller Maßnahmen erfolgt i.d.R. durch die DSt / EinsKtg

1013. Die Ausbildung des bzw. der ISBProj und ISBFW soll mindestens die Grundzüge dieser Zentralen Dienstvorschrift über alle Abschnitte und insbesondere alle sich aus dieser Zentralen Dienstvorschrift ableitenden Aufgaben eines bzw. einer ISBProj bzw. ISBFW sowie die Grundlagen des IT-Grundschutzes des BSI, des Kryptowesens (Zentrale Dienstvorschrift A-961/1 VS-NfD „Kryptosicherheit in der Bundeswehr“, siehe Bezug Anlage 11.15 (lfdNr. 20)) und der Abstrahlsicherheit (Zentrale Dienstvorschrift A-962/1 VS-NfD „Abstrahlsicherheit“, siehe Bezug Anlage 11.15 (lfdNr. 21)) sowie IT-relevante Anteile des Datenschutzes, des Geheimschutzes und der Militärischen Sicherheit beinhalten.

1014. Folgende Schwerpunkte sind bei der Ausbildung des bzw. der ISBProj und ISBFW zu berücksichtigen:

- Erarbeitung und Fortschreibung des InfoSichhKProj bzw. InfoSichhKFW, dabei
  - + Durchführung der Strukturanalyse,
  - + Festlegung der Informationsstruktur,
  - + Durchführung der Schutzbedarfsfeststellung,
  - + Auswahl und Bewertung von InfoSichh-Maßnahmen im Hinblick auf Wirksamkeit und Umsetzbarkeit,
  - + Durchführung von Ergänzender Sicherheitsanalyse mit ggf. folgender Risikoanalyse sowie
  - + Ableitung zusätzlicher / alternativer InfoSichh-Maßnahmen.
- IT-Grundschutzvorgehensweise nach BSI-Standard einschließlich bundeswehrspezifischer Besonderheiten und Nutzung des zentral bereitgestellten Werkzeugs zur Erstellung von InfoSichhK nach IT-Grundschutz.
- Planung und Erarbeitung von personellen, infrastrukturellen, organisatorischen und technischen InfoSichh-Maßnahmen sowie Umsetzung und Überprüfung von technischen InfoSichh-Maßnahmen zur Herstellung, Gewährleistung und Wiederherstellung der InfoSichh in Projekten.
- Führen der InfoSichhDok.

10.1.3 Informationssicherheitsbeauftragte Organisationsbereich / Dienststelle / Betrieb / im Einsatz / Geheimschutzbetreute Wirtschaft und Informationssicherheitsgehilfe (D, E, Ü)

1015. ISBOrgBer, ISBDSt, ISBBtrb, ISB i.E., ISBGBW[135] und InfoSichhGeh sind für ihre Tätigkeit fachlich aus-, und fortzubilden. Hierzu ist ein Lehrgang „**Informationssicherheitsbeauftragte“** zur Ausbildung von ISBOrgBer, ISBDSt, ISBBtrb, ISB i.E. und ISBGBW sowie ein Lehrgang „**Informationssicherheitsgehilfen**“ zur Ausbildung von InfoSichhGeh einzurichten. Als Bedarfsträger

[135] Für ISBÜb ist analog zu verfahren

sind die OrgBer in geeigneter Weise in die Prozesse der Bearbeitung und Weiterentwicklung des Lehrgangs mit einzubeziehen.

Für ISB i.E. ist zusätzlich ein Lehrgang „**Informationssicherheitsbeauftragte in Einsatz / Übung**“ einzurichten. Als Bedarfsträger ist hierbei das EinsFüKdoBw vorrangig in die Prozesse der Bearbeitung und Weiterentwicklung des Lehrgangs mit einzubeziehen.

1016. ISBDSt, ISB i.E. und ISBBtrb sind als fachlich qualifizierte Spezialisten zu befähigen, die InfoSichh bei Einsatz und Betrieb von IT in ihrem Zuständigkeitsbereich zur Unterstützung des bzw. der DStLtr / KtgtFhr / Kdr EinsStO oder Ltr IT-Btrb(Fü)Einr zu planen, umzusetzen und zu überwachen sowie zentrale / querschnittliche Aufgaben der InfoSichh zu bearbeiten. Dies gilt auch für die InfoSichhGeh zur Unterstützung des ISBDSt.

1017. Die Ausbildung der ISBDSt, ISB i.E. und ISBBtrb soll mindestens die Grundzüge aus allen Abschnitten dieser Zentralen Dienstvorschrift und insbesondere alle sich aus dieser Zentralen Dienstvorschrift ableitenden Aufgaben eines bzw. einer ISBDSt, ISB i.E. und ISBBtrb einschließlich Sicherheitsauditing sowie die Grundlagen des IT-Grundschutzes des BSI, des Kryptowesens (Zentrale Dienstvorschrift A-961/1 VS-NfD „Kryptosicherheit in der Bundeswehr“, siehe Bezug Anlage 11.15 (lfdNr. 20)) und der Abstrahlsicherheit (Zentrale Dienstvorschrift A-962/1 VS-NfD „Abstrahlsicherheit“, siehe Bezug Anlage 11.15 (lfdNr. 21)) sowie IT-relevante Anteile des Datenschutzes, des Geheimschutzes und der Militärischen Sicherheit beinhalten.

1018. Folgende Schwerpunkte sind bei der Ausbildung der ISBDSt, ISB i.E. und ISBBtrb zu berücksichtigen:

- Erarbeitung und Fortschreibung der InfoSichhDok, insbesondere des InfoSichhKDSt, dabei
  - Durchführung der Strukturanalyse,
  - Festlegung der Informationsstruktur,
  - Durchführung der Schutzbedarfsfeststellung,
  - Auswahl und Bewertung von InfoSichh-Maßnahmen im Hinblick auf Wirksamkeit und Umsetzbarkeit,
  - Durchführung von Ergänzender Sicherheitsanalyse mit ggf. folgender Risikoanalyse,
  - Ableitung zusätzlicher / alternativer InfoSichh-Maßnahmen sowie
  - Übernahme und Berücksichtigung von Vorgaben aus Projekten.
- IT-Grundschutzvorgehensweise nach BSI-Standard einschließlich bundeswehrspezifischer Besonderheiten und Nutzung des zentral bereitgestellten Werkzeugs zur Erstellung von InfoSichhK nach IT-Grundschutz.
- Planung, Festlegung, Umsetzung und Überwachung von personellen, infrastrukturellen, organisatorischen und technischen InfoSichh-Maßnahmen zur Herstellung, Gewährleistung und Wiederherstellung der InfoSichh in DSt, EinsKtgt und IT-Btrb(Fü)Einr.

- Überwachen der ordnungsgemäßen Durchführung der Kryptoverwaltung der DSt / des EinsKtgt.
- Durchführung des Sicherheitsauditings.
- Überwachung der InfoSichh durch Planung, Durchführung und Auswertung von InfoSichhKtr sowie Auswertung von InfoSichhIn und InfoSichhPrfg.
- Bearbeitung von InfoSichhVork und Kryptoverstößen inkl. der präventiven und reaktiven Erarbeitung, Festlegung und Überwachung von Ereignisprotokollen, Zugangs- und Zugriffskontrollen sowie Rechteverwaltungen in IT-Netzwerken.

1019. InfoSichhGeh sind dazu zu befähigen, die Aufgaben gemäß Abschnitt 9.10 zur Unterstützung des bzw. der ISBDSt unter dessen bzw. deren Anleitung wahrzunehmen. Dazu sind insbesondere die notwendigen Grundkenntnisse für einen InfoSichhGeh aus der A-960/1, der A-962/1 und anderen Regelungen (mit Ausnahme der Kryptosicherheit) sowie die erforderlichen praktischen Fähigkeiten zur Unterstützung des bzw. der ISBDSt zu vermitteln.

10.1.4 Weiterbildung für Informationssicherheitsbeauftragte und Informationssicherheitsgehilfen

1020. Die Weiterbildung bereits ausgebildeter ISB ist in den OrgBer zu regeln und soll regelmäßig (mindestens einmal jährlich) im Rahmen von Tagungen durch die ISBOrgBer oder ISB der vorgesetzten DSt durchgeführt werden. Darüber hinaus können Tagungen durch die Regionalzentren des ZCSBw für ihren jeweiligen Zuständigkeitsbereich durchgeführt werden.

1021. In diesen Tagungen ist in verkürzter Form Basiswissen aufzufrischen. Es sind im Schwerpunkt neue Vorschriften, Weisungen und aktuelle Entwicklungen im Bereich InfoSichh und IT-Grundschutz des BSI zu vermitteln.

1022. CISOBw richtet ergänzend mindestens zweimal pro Jahr Seminare zu aktuellen Themen der InfoSichh in der Bw am Bildungszentrum der Bundeswehr (BiZBw) für herausgehobene ISB[136] aus.

1023. Die Weiterbildung von InfoSichhGeh ist durch die ISBDSt im Rahmen von regelmäßigen bzw. anlassbezogenen Besprechungen durchzuführen. Zusätzlich können die ISBOrgBer eine Teilnahme an den Tagungen der ISB ermöglichen.

10.2 Sensibilisierung (D, E)

1024. Die Sensibilisierung und Schaffung eines Risikobewusstseins zur InfoSichh (Awareness) der Mitarbeiter und Mitarbeiterinnen ist eine allgemeine Führungsaufgabe aller Vorgesetzten. Die Rollenträgerinnen und Rollenträger der InfoSichh sensibilisieren darüber hinaus die IT-Anwender und -Anwenderinnen in ihrem Zuständigkeitsbereich (z. B. durch Awarenessveranstaltungen, Weisungen

[136] ISBOrgBer, ISBBMVg, ISBMAD, ISBEinsatz, CISO Rüstung, CISO Infrastruktur, ISBGBW sowie ISB in höheren Kommandobehörden / Oberbehörden / im Ämterbereich

und Hinweise zur InfoSichh, Lageberichte oder aktuelle Informationen) und nutzen dazu zur Veröffentlichung und Verbreitung auch moderne Informationsangebote (z. B. Intranet, E-Mail, DigAHM).

1025. Die Verantwortlichen müssen demzufolge von Anfang an für InfoSichh in der Bw sensibilisiert werden, damit ein Bewusstsein für InfoSichh (Sensibilisierung und Awareness) geschaffen und InfoSichh nicht als „Hürde“ im Dienstbetrieb wahrgenommen wird. Dieses Vorgehen stärkt die InfoSichh in der Bw grundlegend und ist daher für alle Verantwortlichen verbindlich.

1026. Hierbei sind Maßnahmen zur Mitarbeitersensibilisierung (Awarenessmaßnahmen) die notwendige Basis für ein allgemeines Verständnis hinsichtlich InfoSichh, um alle Rollenträgerinnen und Rollenträger für den Fall eines etwaigen Verstoßes gegen die Sicherheitsrichtlinien und den damit verbundenen richtigen Umgang zu sensibilisieren. Diese Awarenessmaßnahmen können typischerweise abhängig von Größe und Auftrag der Organisation variieren und reichen von Präsenzveranstaltungen über webbasierte Seminare bis hin zu Sensibilisierungskampagnen.

1027. Die Awarenessmaßnahmen müssen u. a. auch die Bedeutung der menschlichen Schwachstelle im Bereich der InfoSichh deutlich machen, da Spionage oder gezielte, wirtschaftlich motivierte Sabotage gegen Unternehmen und Behörden nicht allein mit technischen Mitteln ausgeführt werden. Um ihren Opfern zu schaden oder Informationen zu stehlen, nutzen die Angreifer Methoden wie beispielsweise Social Engineering[137], die nur abzuwehren sind, wenn die Mitarbeiter und Mitarbeiterinnen über mögliche Tricks und Vorgehensweisen der Angreifer orientiert sind und gelernt haben, mit potenziellen Angriffen umzugehen.

1028. Grundlegende Awarenessmaßnahmen zur Sensibilisierung hinsichtlich der InfoSichh sind:

- Festlegen eines Awareness- und Risikomanagements bis auf Dienststellenebene, das allen Verantwortlichen bekannt ist und ständig überprüft wird.
- Kontinuierliche Information und Aufklärung über aktuelle Entwicklungen im Bereich InfoSichh und Sensibilisierung.
- Regelmäßige Durchführung eines „Awareness Tages InfoSichh der Bw“ in Verantwortung des bzw. der CISOBw.
- Regelmäßige Durchführung von „Awareness Tagen InfoSichh / Nutzersensibilisierungs-maßnahmen“ aller DSt / EinsKtgt in ihrem Zuständigkeitsbereich.
- Ständige Überprüfung der Meldesysteme und deren Wege bei einem InfoSichh-Vorfall.
- Auswertung der Ergebnisse von Überwachungsmaßnahmen, um eigene Awarenessmaßnahmen zielgerichtet zu aktualisieren bzw. zu ergänzen.

1029. Zur Erarbeitung von Vorgaben und Maßnahmen zur Sensibilisierung und Schaffung eines Risikobewusstseins zur InfoSichh (Awareness) und zur Unterstützung aller Rollenträgerinnen und

[137] Ausnutzen von menschlichen Schwachstellen, um an sensible Informationen zu gelangen

Rollenträger und Führungsebenen im GB BMVg bei der Sensibilisierung in ihrem Zuständigkeitsbereich richtet CISOBw eine ständige Arbeitsgruppe InfoSichh-Awareness (AG InfoSichhAw) ein.

1030. Für die AG InfoSichhAw gilt:

- Die AG InfoSichhAw ist dem bzw. der CISOBw fachlich direkt unterstellt.
- Die AG besteht aus Angehörigen der OrgBer im GB BMVg sowie externer Partner (z.B. der BWI).
- Der bzw. die CISOBw bestellt den Leiter bzw. die Leiterin und den stellvertretenden Leiter bzw. die Stellvertreterin der AG InfoSichhAw.
- Die AG InfoSichhAw führt eine Geschäftsordnung.

1031. Zu den Aufgaben der AG InfoSichhAw gehört:

- Erarbeiten von Maßnahmen und Hilfsmitteln zur Anwendersensibilisierung (Awarenessmaßnahmen).
- Unterstützung aller DSt / EinsKtgt bei der Planung zur Durchführung von Awarenessmaßnahmen.
- Unterstützung des Dezernats „Übung und Sensibilisierung“ in der Abteilung Schutz und Prävention im ZCSBw, inkl. der Unterstützung bei Planung und Durchführung des „Awareness Tages InfoSichh der Bw“.
- Kontinuierliche Information und Aufklärung aller Mitarbeiter und Mitarbeiterinnen im GB BMVg über aktuelle Entwicklungen im Bereich InfoSichhAw.
- Evaluierung der durchgeführten Awarenessmaßnahmen, mit dem Ziel künftig die eigene InfoSichhAw zielgerichtet zu aktualisieren und zu erweitern.
- Quartalsweise Vorlage von Ergebnissen der AG InfoSichhAw an den bzw. die CISOBw.

1032. Alle DSt:

- unterstützen die AG InfoSichhAw bei der Wahrnehmung ihrer Aufgaben,
- ermöglichen den Mitgliedern der AG InfoSichhAw aus ihrem Zuständigkeitsbereich die Teilnahme und Mitarbeit an AG-Sitzungen, Projekten der AG InfoSichhAw und Ausbildungsunterstützungen sowie
- fördern die Teilnahme von Interessenten aus ihrem Zuständigkeitsbereich an Sitzungen der AG InfoSichhAw.

11 Anlagen

11.1 IT-Grundschutz-Methodik in der Bundeswehr

11.1.1 Allgemeines

1. Die Erstellung eines InfoSichhK im GB BMVg orientiert sich an der IT-Grundschutz-Methodik nach BSI-Standard, bedarf jedoch aufgrund von Besonderheiten in der Bw methodischen und inhaltlichen Anpassungen.

Die Besonderheiten liegen u.a. in den folgenden Aspekten begründet:

- Betrachtung nicht nur von ortsfesten DSt, sondern auch von Projekten und anderen Anwendungsbereichen sowie „verlegbaren DSt“ wie z.B. seegehende Einheiten,
- Vorliegen eines i.d.R. hohen bzw. sehr hohen Schutzbedarfes insbesondere aufgrund der Verarbeitung von VS-Informationen,
- Anwendung für oftmals sehr komplexe Systeme, die von den im IT-Grundschutz betrachteten Einsatzszenarien (Bürokommunikation) abweichen,
- Service-orientierter Ansatz für Systeme und
- notwendige Ergänzung der Maßnahmen aufgrund von zusätzlichen Vorgaben (z.B. NATO Vorgaben).

2. Daher werden zur Erstellung von InfoSichhK nach IT-Grundschutz im GB BMVg

- durch KdoCIR ein IT-Grundschutzkatalog der Bw[138], der neben den Bausteinen und Maßnahmen des BSI ergänzende bundeswehrspezifische Bausteine und Maßnahmen enthält (siehe Anlage 11.1.2),
- durch KdoCIR eine Arbeitshilfe zur Erstellung von InfoSichhKDSt[139] für die Anwendungsbereiche DSt (D), EinsKtgt und EinsStO (E) und
- durch die DEUmilSAA eine Arbeitshilfe zur Erstellung von InfoSichhKProj gemäß IT-Grundschutz[140] für die anderen Anwendungsbereiche F, W, P ,V, O, S, gem. Nr. 402

bereitgestellt. Diese sind zwingend zu nutzen.

Die beiden Arbeitshilfen beschreiben das Verfahren für die Erstellung von InfoSichhK in der Bw und bestehen jeweils aus zwei Teilen. Die Arbeitshilfen setzen die Vorgaben dieser Vorschrift um, konkretisieren diese und sind einzuhalten.

Teil 1 beschreibt jeweils die Bearbeitung des Dokumentanteils und Teil 2 die Arbeitsschritte, die im Werkzeug erfolgen.

[138] http://infosichh.bundeswehr.org im Bereich „Fachinformationen / IT-Grundschutz / Bausteine und Metadaten“
[139] http://infosichh.bundeswehr.org im Bereich „IT-Grundschutz“ im Downloadbereich
[140] http://infosichh.bundeswehr.org im Bereich „InfoSichhOrg / DEUmilSAA / InfoSichhProj“

3. Im InfoSichhK sollen möglichst viele Anteile / Kapitel werkzeuggestützt bearbeitet und dokumentiert werden. Details zu Gliederung und Inhalt des InfoSichhK sowie zur Nutzung des Werkzeugs regeln die beiden Arbeitshilfen zur Erstellung von InfoSichhKDSt bzw. InfoSichhKProj. Das einheitliche Werkzeug und die zugehörigen MetadatenBw[141] werden im Intranetauftritt http://infosichh.bundeswehr.org unter der Rubrik „Fachinformationen / IT-Grundschutz“ bereit gestellt (siehe Nr. 124)[142]. Im einheitlichen Werkzeug sind ausschließlich die MetadatenBw zu nutzen. Diese Metadaten enthalten die durch das BSI veröffentlichten IT-Grundschutzkataloge sowie die aktuellen bundwehrspezifischen Ergänzungen.

11.1.2 IT-Grundschutzkatalog der Bundeswehr

4. Das KdoCIR veröffentlicht periodisch (angestrebt jährlich, maximal zweimal im Jahr) einen fortgeschriebenen IT-Grundschutzkatalog der Bw im IntranetBw[143], der neben den Bausteinen und Maßnahmen des BSI ergänzende bundeswehrspezifische Bausteine und Maßnahmen enthält. Dieser bzw. die zugehörigen MetadatenBw (siehe Nr. 3) sind zur Erstellung und Fortschreibung (siehe Nr. 6) von InfoSichhK nach IT-Grundschutz zwingend zu nutzen.

5. Zur Fortschreibung des IT-Grundschutzkataloges der Bw ist – neben der zentralen Erstellung querschnittlicher Bausteine – die Zuarbeit durch die zuständigen Rollenträgerinnen und Rollenträger für InfoSichhK (z.B. Projekte und DSt) eine wesentliche Grundlage. Die DEUmilSAA, die Regionalzentren des ZCSBw und die ISBOrgBer werten dazu vorliegende oder in Erstellung befindliche InfoSichhK bezüglich neuer Bausteine und InfoSichh-Maßnahmen aus und übermitteln geeignete neue Bausteine / InfoSichh-Maßnahmen mit einer Empfehlung zur Berücksichtigung im Rahmen der Fortschreibung des IT-Grundschutzkataloges der Bw an die Referatsgruppe InfoSichh im KdoCIR Abteilung Planung.

6. Nach Veröffentlichung eines neuen IT-Grundschutzkatalogs der Bw sind die neuen Bausteine und Maßnahmen im Rahmen der Fortschreibung der InfoSichhK (siehe Abschnitte 6.3.2.3 und 6.3.3.3), innerhalb eines Jahres in die InfoSichhK einzuarbeiten.

7. Ein Überblick über die im IT-Grundschutzkatalog der Bw vorhandenen Bausteine ist auf der Intranetseite http://infosichh.bundeswehr.org im Bereich „Fachinformationen / IT-Grundschutz / Bausteine und Metadaten“ zu finden.

8. Der IT-Grundschutzkatalog teilt sich in Baustein-, Gefährdungs- und Maßnahmenkataloge auf. Alle dort aufgeführten Bausteine, Gefährdungen und Maßnahmen tragen Referenznummern, damit diese vereinfacht referenziert werden können (siehe Nrn. 12 – 13).

---

[141] Bausteine und Maßnahmen aus dem IT-Grundschutzkatalog der Bundeswehr

[142] Informationen und Metadatenupdates für das einheitliche Werkzeug sind im IntranetBw unter http://infosichh.bundeswehr.org im Bereich „Fachinformationen / IT-Grundschutz / SAVe“ veröffentlicht.

[143] http://infosichh.bundeswehr.org im Bereich „Fachinformationen / IT-Grundschutz / Bausteine und Metadaten“

9. Der **Bausteinkatalog** ist in sogenannte Schichten eingeteilt. Diese sind:

- B 1: Übergreifende Aspekte
- B 2: Infrastruktur
- B 3: IT-Systeme[144]
- B 4: Netze
- B 5: Anwendungen

10. Der **Gefährdungskatalog** ist in die folgenden Kategorien gegliedert, wobei die Referenzierung analog zu der des Bausteinkatalogs erfolgt:

- G 1: Höhere Gewalt
- G 2: Organisatorische Mängel
- G 3: Menschliche Fehlhandlungen
- G 4: Technisches Versagen
- G 5: Vorsätzliche Handlungen

11. Der **Maßnahmenkatalog** ist in die folgenden Kategorien gegliedert, wobei die Referenzierung analog zu der des Bausteinkatalogs erfolgt:

- M 1: Infrastruktur
- M 2: Organisation
- M 3: Personal
- M 4: Hard- und Software
- M 5: Kommunikation
- M 6: Notfallvorsorge

Für die Bw sind die InfoSichh-Maßnahmen der Kategorien 4 und 5 den technischen InfoSichh-Maßnahmen zuzuordnen.

12. Ein Baustein trägt Referenzen nach dem folgenden Muster „B X.YY(Y)“, wobei das B für „Baustein“, das X für die zugeteilte Bausteinschicht und YY(Y) eine eindeutige zwei- oder dreistellige Nummer in der Schicht ist. Ergänzende Bausteine der Bw erhalten eine dreistellige Endnummer (Schema: B X.YYY)

13. Analog dazu sind die Gefährdungen und Maßnahmen durchnummeriert mit dem Unterschied, dass alle bundeswehrspezifischen Gefährdungen und Maßnahmen eine vierstellige Endnummer erhalten (Schema: G oder M X.YYYY).

[144] Der Begriff "IT-System" wird hier im Sinne des IT-Grundschutzes des BSI als Bezeichnung der Schicht 3 der Bausteine verwendet. Anders als sonst in dieser Vorschrift bezeichnet der Begriff des BSI hier keine vollständigen Systeme, sondern einzelne IT-Komponenten, wie beispielsweise Clients, Server oder Router.

14. Es ist zu beachten, dass die Begrifflichkeiten des IT-Grundschutzes des BSI nicht immer denen in der Bw entsprechen. Entsprechende Begriffe sind daher sinngemäß anzuwenden, siehe folgende Tabelle:

Begriff IT-Grundschutz des BSI	Begriff Bundeswehr
Sicherheitskonzept	Informationssicherheitskonzept
Datenschutzbeauftragter / Datenschutzbeauftragte	Administrativer Datenschutzbeauftragter / Datenschutzbeauftragte (ADSB)
Geheimschutzbeauftragter / Geheimschutzbeauftragte	Sicherheitsbeauftragter / Sicherheitsbeauftragte (SichhBeauftr)
Leiter / Leiterin Haustechnik	Bundeswehr-Dienstleistungszentrum

Abb. 12 Gegenüberstellung von Begriffen IT-Grundschutz BSI – Bw

Bei Unklarheiten berät die DEUmilSAA.

15. Ebenfalls ist zu beachten, dass die InfoSichh-Maßnahmen aus dem IT-Grundschutz des BSI in der Regel als Empfehlung formuliert sind. Für die Bw sind diese Empfehlungen einer Sollvorgabe gleichzusetzen. Abweichungen können in begründeten Fällen im Einvernehmen mit dem bzw. der zuständigen ADSB und SichBeauftr beschlossen werden.

16. Die in den Bausteinen des IT-Grundschutzes des BSI aufgeführten sogenannten „Lebenszyklusphasen“, denen die InfoSichh-Maßnahmen zugeordnet sind, sind mit den CPM-Phasen vergleichbar, entsprechen diesen jedoch inhaltlich nicht vollständig. Die Lebenszyklusphasen des BSI verhalten sich zu den CPM-Phasen der Bw gemäß den in den folgenden zwei Tabellen definierten Zuordnungen:

Lebenszyklusphase in den IT-Grundschutz-Bausteinen	CPM-Phase	Erläuterung
Planung und Konzeption	Analysephase	–
Beschaffung	Realisierungsphase	Im CPM ist die Festlegung der Anforderungen an das System / Produkt (Lastenheft) und die eigentliche Beschaffung Teil der Realisierungsphase. Gemäß Phaseneinteilung des BSI gehören sowohl die Festlegung der Anforderungen an das System / Produkt als auch die eigentliche Beschaffung in die Lebenszyklusphase Beschaffung.
Umsetzung	Realisierungsphase	–
Betrieb	Nutzungsphase	–
Aussonderung	Nutzungsphase	–
Notfallvorsorge	Realisierungsphase (Notfallplanung) Nutzungsphase (Notfallbewältigung)	Nach dem BSI-Standard zum Notfallmanagement besteht dieses aus den zwei großen Teilen Notfallvorsorge und Notfall-bewältigung. Die Lebenszyklusphase „Notfall-vorsorge“ beinhaltet auch Maßnahmen zur Notfall-bewältigung und müsste daher „Notfall-management“ heißen; die jetzige Bezeichnung ist historisch gewachsen.

Abb. 13 Abbildung der CPM-Phasen auf die Lebenszyklusphasen

CPM-Phase	Lebenszyklusphase in den IT-Grundschutz-Bausteinen	Erläuterung
Analysephase	Planung und Konzeption	–
Realisierungsphase	Beschaffung Umsetzung Notfallvorsorge (Notfallplanung)	siehe oben
Nutzungsphase	Betrieb Aussonderung Notfallvorsorge (Notfallbewältigung)	siehe oben

Abb. 14 Abbildung der Lebenszyklusphasen auf die CPM-Phasen

11.1.3 Ablauf der Erstellung eines Informationssicherheitskonzepts

17. Die Erstellung eines InfoSichhK gliedert sich in folgende Aktivitätsfelder, die meist nacheinander, aber je nach Rahmenbedingungen und vorhandenem Personal auch (weitgehend) unabhängig und zeitgleich durchgeführt werden können:

- Definition des Geltungsbereiches (auch als Informationsverbund bezeichnet) (siehe Anlage 11.1.4) sowie der Rechtsgrundlage der Verarbeitung
  Hier wird definiert, welche Anteile Gegenstand des InfoSichhK sind.
- Strukturanalyse (siehe Anlage 11.1.5)
  Die Strukturanalyse erfasst eine Organisation bzw. ein System mit ihren / seinen technischen, infrastrukturellen und personellen Bestandteilen (Informationen, Anwendungen, IT, Netzen, Räumen, Gebäuden, Rollenträgerinnen und Rollenträger) bzw. zerlegt das System in seine verschiedenen Anteile sowohl im Hinblick auf organisatorische, personelle und infrastrukturelle als insbesondere auch technische Aspekte.
- Schutzbedarfsanalyse mit Informationsstruktur und Schutzbedarfsfeststellung (siehe Anlage 11.1.6)
  Die Informationsstruktur[145] und der jeweilige Schutzbedarf sind gemäß Abschnitt 2 anhand der verarbeiteten Informationen zu ermitteln. Ausgehend von der Informationsstruktur wird den Anteilen aus der Strukturanalyse der Schutzbedarf hinsichtlich der Grundwerte und die Relevanz der Gewährleistungsziele zugeordnet.
- Modellierung (siehe Abschnitt 11.1.7)
  Die Modellierung baut auf den Erkenntnissen der Strukturanalyse auf. Den Zielobjekten werden die relevanten Bausteine zugeordnet, die ggf. anzupassen und im Hinblick auf spezifische Aspekte im Anwendungsbereich zu ergänzen sind (siehe Anlage 11.1.4).

[145] Die Informationsstruktur ist eine bundeswehrspezifische Ergänzung zum IT-Grundschutz und ist gemäß Abschnitt 2.1 anzufertigen.

- Basis-Sicherheitscheck (siehe Anlage 11.1.9)
  Der Basis-Sicherheitscheck ist ein SOLL-IST-Abgleich auf Basis der Modellierung. Er gleicht die von den Bausteinen vorgegebenen Maßnahmen (SOLL) mit den tatsächlich umgesetzten Maßnahmen (IST) ab.
- Ergänzende Sicherheitsanalyse (siehe Anlage 11.1.10)
  Die ergänzende Sicherheitsanalyse dient dazu festzustellen, ob die festgelegten Maßnahmen ausreichend alle Risiken abdecken. Falls nicht, ist eine nachgelagerte, tiefer gehende Risikoanalyse erforderlich.
- Risikoanalyse (siehe Anlage 11.1.10)
  Ziel einer Risikoanalyse ist es, vor dem Hintergrund bestehender Schwachstellen bzw. Gefährdungen relevante Risiken abzuschätzen und festzustellen, ob das Risiko tolerierbar ist oder ergänzende Maßnahmen festzulegen sind.
- Basis-Sicherheitscheck Teil 2 (siehe Anlage 11.1.11)
  Wiederholung des Basis-Sicherheitschecks, wenn im Rahmen der Risikoanalyse Maßnahmen geändert wurden oder neu hinzugekommen sind.
- Realisierung (siehe Anlage 11.1.12)
  Für nicht oder nur teilweise umgesetzte Maßnahmen ist die Umsetzung zu planen und durchzuführen.

18. Die allgemeine Vorgehensweise zur Erstellung eines InfoSichhK in der Bw wird in der folgenden Abbildung dargestellt.

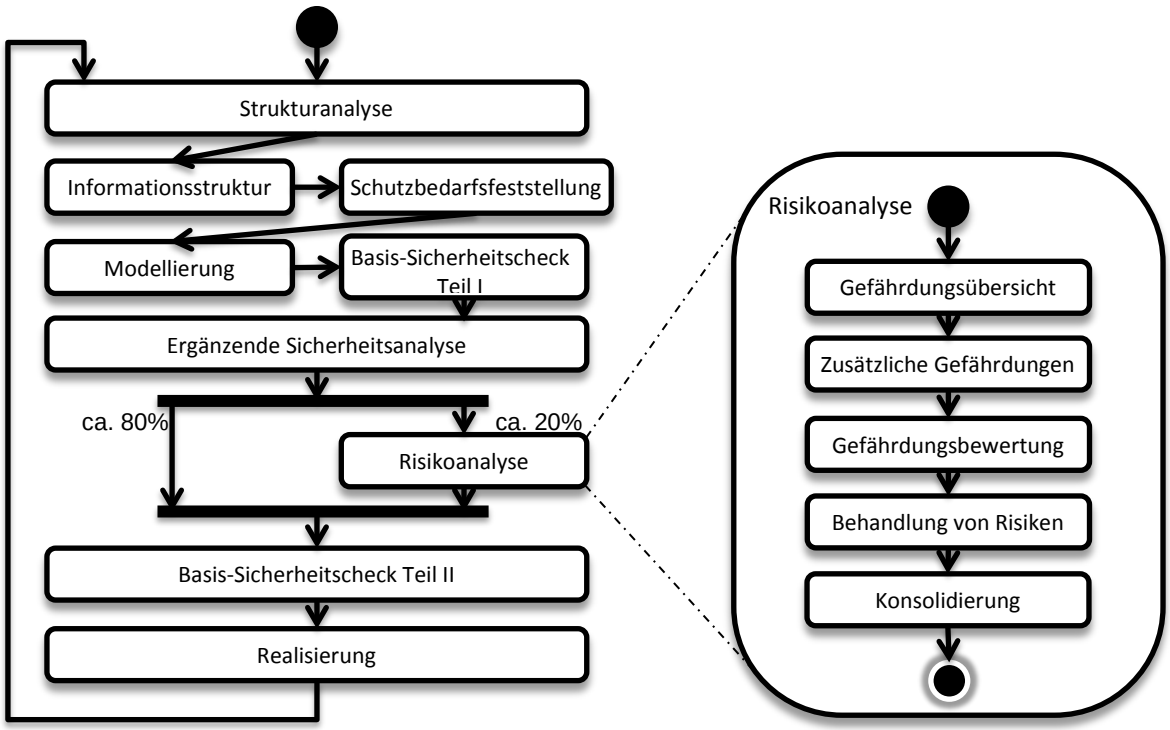

Abb. 15 Vorgehensweise zur Erstellung InfoSichhK in der Bundeswehr

19. In den folgenden Abschnitten werden die einzelnen Aktivitätsfelder dargestellt.

11.1.4 Definition des Geltungsbereiches

20. Bevor mit der Strukturanalyse begonnen werden kann, ist abzugrenzen, für welchen Gültigkeitsbereich das InfoSichhK erstellt werden soll und für welche Bereiche es nicht gültig ist. Dieser abgegrenzte Bereich wird als Informationsverbund bezeichnet.

Dazu zählen bei einem Projekt die IT und die damit verbundenen Geschäftsprozesse, aber auch Schnittstellen zu anderer beteiligter IT und deren Geschäftsprozessen.

Bei einer DSt ist der Informationsverbund die DSt mit ihrer Infrastruktur und der darin genutzten bzw. betriebenen IT, die der DSt auch durch andere Anwendungsbereiche (z.B. Projekte, Infrastruktur-vorhaben etc.) zur Nutzung bzw. zum Betrieb übergeben werden.

Der Informationsverbund ist kurz in Textform abzugrenzen und zu dokumentieren. Dazu gehören allgemeine Informationen zum Anwendungsbereich (z.B. Projekt bzw. DSt), wie z. B. die Projekt- oder Dienststellennummer. Im Idealfall dokumentiert die Strukturanalyse den Informationsverbund, der nur noch kurz beschrieben werden muss. Eine kurze Beschreibung des Informationsverbunds dient dem Verständnis der Prüfer und nachfolgender ISB.

Details regeln die Arbeitshilfen zur Erstellung von InfoSichhK (siehe Nr. 2).

11.1.5 Strukturanalyse

21. Die Strukturanalyse dient der Vorerhebung von Informationen, die für die weitere Erstellung eines InfoSichhK nach IT-Grundschutz benötigt werden. Dabei geht es um die Erfassung der Bestandteile (Informationen, Anwendungen, IT, Räume, Kommunikationsnetze), die im Geltungs-bereich zur Aufgabenerfüllung benötigt werden.

22. Dazu müssen die relevanten Informationen und Anwendungen ermittelt und die betroffenen IT-Komponenten, Räume und Netze erfasst werden. Eine Vorgehensweise ist, zuerst die Anwendungen und ausgehend davon die weiteren betroffenen Objekte zu ermitteln. Dabei ist es aber häufig schwierig, abstrakte Anwendungen losgelöst von konkreten IT-Komponenten zu erfassen. Daher kann es manchmal zweckmäßig sein, zuerst die IT-Komponenten zu erheben, da sich die Anwendungen häufig anhand der betrachteten IT leichter ermitteln lassen.

23. Es sollte geprüft werden, ob bereits Datenbanken oder Übersichten gepflegt werden, die im Rahmen der Strukturanalyse als Datenquellen genutzt werden können.

24. Die Strukturanalyse gliedert sich in folgende Teilaufgaben:

- Erfassung der zum Geltungsbereich zugehörigen Geschäftsprozesse, Anwendungen und Informationen
- Netzplanerhebung
- Erhebung von IT und ähnlicher Objekte
- Erfassung der Räume

25. Bei DSt liegt der Schwerpunkt in der Strukturanalyse auf der Infrastruktur (Schicht 2 im Bausteinkatalog) – sofern nicht separat aus Projekten bereitgestellt – sowie auf organisatorischen und personellen Aspekte (Schicht 1, Übergreifende Aspekte), während er bei Projekten grundsätzlich – sofern nicht durch die DSt selbst beschafft und betrieben – auf den technischen Komponenten (Schicht 3 bis 5) liegt.

26. Details regeln die Arbeitshilfen zur Erstellung von InfoSichhK (siehe Nr. 2).

11.1.6 Schutzbedarfsanalyse mit Informationsstruktur und Schutzbedarfsfeststellung

27. Die Erstellung der Informationsstruktur und die Schutzbedarfsfeststellung richten sich nach Abschnitt 2.1 dieser Zentralen Dienstvorschrift.

28. Ausgehend von den Informationen wird der Schutzbedarf auf die Anwendungen, auf die IT sowie den damit verbundenen Netzen vererbt. Darüber hinaus vererbt sich der Schutzbedarf auf Räume und Gebäude.

29. Bei der Vererbung des Schutzbedarfes sind das Maximumprinzip[146], der Kumulationseffekt[147] und der Verteilungseffekt[148] zu beachten.

30. Details regeln die Arbeitshilfen zur Erstellung von InfoSichhK (siehe Nr. 2)

11.1.7 Modellierung

11.1.7.1 Vorgehensweise

31. Die Modellierung baut auf den Erkenntnissen der Strukturanalyse auf und wird im Werkzeug durchgeführt. Den Zielobjekten werden ein oder mehrere Bausteine aus dem IT-Grundschutzkatalog der Bw (mit den Bausteinen des BSI und ergänzenden bundeswehrspezifischen Bausteinen) zugeordnet. Aus den zugeordneten Bausteinen ergeben sich die geforderten Maßnahmen.

32. Zur Auswahl, Anpassung und Konkretisierung von InfoSichh-Maßnahmen siehe Abschnitt 2.2.

33. In bestimmten, in Abschnitt 2.2.2 dargestellten Fällen reichen die vorhandenen InfoSichh-Maßnahmen nicht aus bzw. sind ggf. nicht anwendbar oder umsetzbar. In diesen Fällen sind zusätzliche bzw. alternative InfoSichh-Maßnahmen, wie in Abschnitt 2.2.2 dieser Zentralen Dienstvorschrift dargestellt, zu ermitteln.

---

[146] Vgl. Nr. 208 Schritt 5

[147] Beim *Kumulationseffekt* kann es vorkommen, dass sich bei einem Zielobjekt so viele Zielobjekte bzw. Instanzen eines Schutzbedarfes anhäufen, sodass für das Zielobjekt insgesamt ein höherer Schutzbedarf für einen oder mehrere Grundwerte ergibt.

[148] Beim Verteilungseffekt verhält es sich gegenläufig zum Kumulationseffekt. Hierbei wird ein Grundwert herabgestuft, da durch die Verteilung auf mehrere Instanzen bzw. Zielobjekte sich der hohe Schutzbedarf nicht weitervererbt oder nur unwesentliche Teilbereiche einer Anwendung mit hohem Schutzbedarf auf dem Zielobjekt laufen.

11.1.8 Grundsätze bei der Festlegung von Informationssicherheitsmaßnahmen

34. InfoSichh-Maßnahmen werden resultierend aus der Festlegung der Schutzbedarfskategorien (Schutzbedarfsfeststellung und Dokumentation, siehe Abschnitte 2.1.3 und 2.1.4) sowie gemäß dem Ergebnis der Modellierung der IT festgelegt.

35. Für die Bw gelten folgende Grundsätze:

- Werden Informationen unterschiedlichen Schutzbedarfes in IT verarbeitet oder übertragen, so ist zu untersuchen, ob Teilsysteme mit entsprechend einheitlichem Schutzbedarf realisiert und für diese entsprechend abgestufte InfoSichh-Maßnahmen realisiert werden können. Ist dies nicht möglich, sind die InfoSichh-Maßnahmen des jeweils höchsten Schutzbedarfes der zu verarbeitenden und / oder zu übertragenden Information für die gesamte IT umzusetzen.
- InfoSichh-Maßnahmen sind so aufeinander abzustimmen und so auf die Komponenten / Elemente der IT (z. B. IT-Netze, Server, Clients) zu verteilen, dass ihr Zusammenwirken einen mehrschichtigen Schutz gewährleistet, der nicht durch Ausfall / Ausschalten einer Einzelmaßnahme überwunden werden kann.
- Enthält die Informationsstruktur (siehe Abschnitt 2.1) PersDat, ist der Baustein „Datenschutz“ aus dem IT-Grundschutzkatalog der Bw heranzuziehen und die darin dokumentierten Maßnahmen sind zu beachten.
- Beschreiben InfoSichh-Maßnahmen aus dem IT-Grundschutzkatalog der Bw mehrere Handlungsalternativen, so ist die gewählte Alternative im jeweiligen InfoSichhK (siehe Abschnitt 6.3) zu dokumentieren.
- Sind in den InfoSichh-Maßnahmen Freiheiten im Rahmen der Parametrisierung möglich bzw. ist eine konkrete Parametrisierung gefordert, so ist diese ebenfalls im jeweiligen InfoSichhK zu der InfoSichh-Maßnahme zu dokumentieren.
- Zur Benennung von InfoSichh-Maßnahmen aus dem IT-Grundschutzkatalog der Bw in den InfoSichhK ist es ausreichend, die entsprechenden Maßnahmennummern zu referenzieren.
- Erforderliche InfoSichh-Maßnahmen sind auch dann umzusetzen, wenn sie den Einsatz oder die Entwicklung von IT erschweren.
- Alle aus dem Ergebnis der Modellierung der IT resultierenden InfoSichh-Maßnahmen sind zu betrachten und grundsätzlich umzusetzen, sofern für die geplante / einzusetzende IT anwendbar bzw. technisch zutreffend.
- Ist dies im Einzelfall – obwohl technisch zutreffend – nicht möglich, ist dies zu begründen und bezogen auf diese InfoSichh-Maßnahme(n), eine Ergänzende Sicherheitsanalyse mit ggf. folgender Risikoanalyse (siehe Abschnitt 6.2) durchzuführen. Bei Bedarf sind alternative InfoSichh-Maßnahmen festzulegen, die Risiken sind hinsichtlich ihrer Tolerierbarkeit zu bewerten und darzustellen.

- Können die in den InfoSichhKProj festgelegten InfoSichh-Maßnahmen kurzfristig nicht umgesetzt werden, ist die Festlegung und Umsetzung alternativer InfoSichh-Maßnahmen zu prüfen (siehe Anlage 11.1.10).
- Ist der Schutzbedarf in mindestens einem Grundwert höher als „normal“, sind zusätzlich die Vorgaben der Anlage 11.3 zu beachten und umzusetzen.
- Die zu beschaffende / entwickelnde IT ist grundsätzlich so auszulegen, dass die InfoSichh-Maßnahmen des IT-Grundschutzes umgesetzt werden können.

36. Falls für bestimmte projekt-, dienststellen- oder einsatzbezogene Anforderungen an die InfoSichh

- im IT-Grundschutzkatalog der Bw keine InfoSichh-Maßnahmen festgelegt sind (siehe Abschnitt 2.2.2) oder
- projekt- / dienststellen- / einsatzbezogene Ergänzungen erforderlich werden oder
- als Ergebnis einer Risikoanalyse (siehe Anlage 11.1.10) alternative / zusätzliche InfoSichh-Maßnahmen festzulegen sind (siehe auch Abschnitt 2.2.2),

so sind bei der Festlegung der alternativen / zusätzlichen InfoSichh-Maßnahmen, die über die gemäß Anlage 11.3 umzusetzenden InfoSichh-Maßnahmen hinausgehen, folgende Grundsätze zu beachten:

- Lassen Vorschriften bzw. Vorgaben Ermessensspielräume zu, z. B. durch die Möglichkeit, unterschiedliche InfoSichh-Maßnahmen einzusetzen, dann sind diese unter Berücksichtigung der Wirtschaftlichkeit angemessen zu nutzen.
- Es ist die wirtschaftlichste InfoSichh-Maßnahme auszuwählen, die den geforderten Schutz gewährleistet.
- Stehen mehrere funktional gleichwertige Produkte zur Verfügung, so ist der Einsatz eines zertifizierten (siehe Abschnitt 5.2) InfoSichh-Produktes grundsätzlich dem eines nicht zertifizierten InfoSichh-Produktes vorzuziehen. Entscheidend ist jedoch der erbrachte Sicherheitsnachweis durch eine Evaluierung (siehe Abschnitt 5.1).
- Decken bundeswehreigene Vorschriften bzw. Vorgaben die Anforderungen eines Projektes, einer DSt, eines EinsKtgt oder einer IT-Btrb(Fü)Einr nicht ab, sind InfoSichh-Maßnahmen in Anlehnung an anderweitige Regelungen wie z. B. der NATO zu bestimmen und zu begründen. Bei DSt / EinsKtgt / IT-Btrb(Fü)Einr, die mit Kryptomitteln der NATO ausgestattet oder die in Projekte der NATO involviert sind, gelten diesbezüglich die einschlägigen Vorschriften der NATO.
- Bei der Realisierung technischer InfoSichh-Maßnahmen sind grundsätzlich die Standardisierungs- und Ausstattungsvorhaben der Bw in der „Technischen Architektur IT-System der Bundeswehr“ (B1-1500/6-7001 VS-NfD „Technische Architektur des IT-Systems Bundeswehr“, siehe Bezug Anlage 11.15 (lfdNr. 49)) sowie die Vorgaben der NATO (insbesondere siehe Bezüge Anlage 11.15 (lfdNrn. 29, 30, 32 und 33)) bzw. EU (insbesondere siehe Bezüge Anlage 11.15 (lfdNrn. 35 und 36)) zu beachten. Ausnahmen sind zu begründen.

37. In Anwendungsbereichen (z.B. Projekten), die DSt IT zur Nutzung oder Betrieb bereitstellen, sind neben der Beschreibung der im eigenen Bereich umzusetzenden bzw. umgesetzten Maßnahmen, auch erforderliche Vorgaben für die nutzenden bzw. betreibenden DSt zu machen (s. Nr. 622). Vorgaben können sowohl die bereit gestellte IT, als auch das Systemumfeld in den DSt betreffen.

Sofern querschnittliche IT beschafft oder realisiert wird, die in anderen Projekten zum Einsatz kommen soll, sind Vorgaben ggf. auch für diese Projekte zu machen.

Vorgaben sind nur insoweit erforderlich, als diese von den nutzenden bzw. betreibenden DSt oder den anderen Projekten umzusetzen sind.

Form und Inhalt der bereitzustellenden Vorgaben sind der Arbeitshilfe zur Erstellung von projektbezogenen InfoSichhK (siehe Anlage 11.1.1, Nr. 2) zu entnehmen.

11.1.9 Basis-Sicherheitscheck

38. Der Basis-Sicherheitscheck ist ein SOLL-IST-Abgleich, der zum Ziel hat zu überprüfen, ob und wie alle im Rahmen der Modellierung ermittelten Maßnahmen (SOLL) tatsächlich im Informationsverbund umgesetzt sind bzw. umgesetzt werden sollen (IST)[149]. Die Überprüfung kann auch anhand von Interviews geführt werden. Das Ergebnis ist im Werkzeug zu dokumentieren.

39. Details regeln die Arbeitshilfen zur Erstellung von InfoSichhK (siehe Nr. 2)

11.1.10 Ergänzende Sicherheitsanalyse und Risikoanalyse

11.1.10.1 Ergänzende Sicherheitsanalyse

40. Eine ergänzende Sicherheitsanalyse ist stets durchzuführen in den Fällen der Nr. 605. Dabei ist zu bewerten, ob weitere Risikobetrachtungen erforderlich sind. Einzelheiten regeln die Arbeitshilfen zur Erstellung von InfoSichhK (siehe Nr. 2).

11.1.10.2 Risikoanalyse

41. Sofern gemäß Ergänzender Sicherheitsanalyse eine weitergehende Betrachtung erforderlich ist, sind im Rahmen der Risikoanalyse die verbleibenden Risiken zu bewerten und dazu grundsätzlich folgende Aktivitäten durchzuführen:

- Feststellung der relevanten Gefährdungen für die Organisation bzw. das System auf Basis der Gefährdungskataloge des IT-Grundschutzes des BSI.
- Ermittlung neuer / zusätzlicher Gefährdungen.

[149] Für Projekte ist im Rahmen der Analysephase bzw. der Realisierungsphase im Hinblick auf die Umsetzung der Maßnahmen immer bereits der für den Beginn der Nutzung des Systems vorgesehene Stand zu beschreiben. Das InfoSichhKProj dient in diesen Phasen zur Konzeption.
Nach Beginn der Nutzung dient das InfoSichhKProj der Dokumentation insbesondere der umgesetzten Maßnahmen.

- Bewertung der Gefährdungen und Feststellen von Schadenshöhen und Eintrittswahrscheinlichkeiten.
- Festlegung des Risikos bzw. Risikobewertung.
- Festlegung der Risikobehandlung mit Dokumentation der Maßnahmen zur Risikoreduktion und der tolerierbaren Risiken.

Diese Aktivitäten werden in den folgenden Abschnitten im Einzelnen erläutert.

11.1.10.3 Gefährdungsübersicht und zusätzliche Gefährdungen

42. Es sind die für die Organisation bzw. das System relevanten Gefährdungen auf Basis der Gefährdungen aus den verwendeten Bausteinen des IT-Grundschutzkataloges der Bw zu ermitteln. Darüber hinaus sind auch zusätzliche Gefährdungen zu ermitteln, die sich z.B. aus besonderen Einsatzszenarien oder auch konkreten Schwachstellen in der Organisation bzw. im System ergeben können. Einzelheiten regeln die Arbeitshilfen zur Erstellung von InfoSichhK (siehe Nr. 2).

11.1.10.4 Gefährdungsbewertung

43. Ausgehend von der vollständigen Gefährdungsübersicht wird bewertet, welche Gefährdungen durch Maßnahmen nicht hinreichend abgedeckt sind. Im Hinblick auf diese Gefährdungen bestehen Risiken, die nachfolgend zu bewerten sind.

44. Für jede Gefährdung ist die **Schadenshöhe** zu bewerten und die **Eintrittswahrscheinlichkeit** abzuschätzen, so dass sich ein **Risiko** ableiten lässt. Dabei wird für jeden Grundwert das Risiko ermittelt.

45. Die mögliche Schadenshöhe kann wie folgt bewertet werden:

- 0: kein,
- 1: gering,
- 2: mittel und
- 3: hoch.

46. Die Schadenshöhen bei Gefährdung der einzelnen Grundwerte sind in Abhängigkeit von der jeweiligen Schutzbedarfskategorie wie folgt abzuschätzen:

Schutzbedarfskategorie	**Schadenshöhe bei Gefährdung**
normal	0 (bei Vertraulichkeit nur für „öffentliche“ Informationen), sonst 1
hoch	2
sehr hoch	3

Abb. 16 Tabelle Festlegung der Schadenshöhen

47. Die Eintrittswahrscheinlichkeiten möglicher Schäden sind wie folgt abzuschätzen:

- 0 Keine: (Eintritt unwahrscheinlich),
- 1 Gering: (Eintritt möglich bis zu einmal im Jahr),
- 2 Mittel: (Eintritt möglich mehr als 1x im Jahr bis weniger als 1x im Monat)
- 3 Hoch: (Eintritt möglich einmal im Monat und häufiger).

11.1.10.5 Risikofestlegung und Festlegung alternativer Informationssicherheitsmaßnahmen

48. Die Festlegung des Risikos ergibt sich wie folgt:

Die Schadenshöhe wird multipliziert mit der Eintrittswahrscheinlichkeit. Abhängig von dem daraus entstehenden Wert ergibt sich die Risikofestlegung aus der folgenden Tabelle Abb. 17:

Wert	**Risiko**
0	Kein
1, 2, 3	Gering
4, 6	Mittel
9	Hoch

Abb. 17 Risikofestlegung

49. Auf Grundlage der durchgeführten Risikobewertung ist für jedes festgestellte Risiko zu entscheiden, welche Risikobehandlung anzuwenden ist.

50. Folgende Risikobehandlungen sind möglich:

- Risikoübernahme das Risiko wird akzeptiert(das verbleibende Risiko wird toleriert).
- Risikoreduktion alternative oder zusätzliche InfoSichh-Maßnahmen werden festgelegt und umgesetzt.
- Risikovermeidung Geschäftsprozesse oder die Organisation werden umstrukturiert.
- Risikoverlagerung das Risiko wird auf andere Bereiche der Organisation oder auf die Wirtschaft übertragen (in der Bw unüblich).

51. Bei einer Risikobewertung mit dem Ergebnis „Kein Risiko“ ist die Festlegung von alternativen InfoSichh-Maßnahmen nicht erforderlich.

52. Bei einer Risikobewertung mit dem Ergebnis „Risiko gering“ und Schadenshöhe „1“ für alle Schutzbedarfskategorien sind ebenfalls keine alternativen InfoSichh-Maßnahmen notwendig, da im Allgemeinen das verbleibende Risiko tolerierbar ist (Risikoübernahme).

53. Wenn eine Schadenshöhe von „2“ oder „3“ vorliegt, sind auch bei „geringem Risiko“ geeignete alternative oder ergänzende InfoSichh-Maßnahmen durch die zuständigen Rollenträgerinnen und

Rollenträger unter Beachtung der Anlage 11.1.8 festzulegen und umzusetzen (siehe auch Abschnitt 2.2.2) (Risikoreduktion).

54. Für die anderen Risikobewertungen „mittel“ oder „hoch“ (Schadenhöhe „4“, „6“ oder „9“) sind immer geeignete alternative oder ergänzende technische InfoSichh-Maßnahmen (ggf. in Kombination mit organisatorischen, personellen oder infrastrukturellen InfoSichh-Maßnahmen) durch die zuständigen Rollenträgerinnen und Rollenträger unter Beachtung der Anlage 11.1.2 festzulegen und umzusetzen (siehe auch Auswahl, Anpassung und Konkretisierung von InfoSichh-Maßnahmen gemäß Abschnitt 2.2) (Risikoreduktion).

55. Zusätzlich zur Risikoreduktion in den Nrn. 53 und 54 kann eine Vermeidung des Risikos durch Umstrukturierung der IT bzw. Änderung von Prozessen ergänzend wirken (Risikovermeidung).

11.1.10.6 Konsolidierung

56. Die ermittelten alternativen oder zusätzlichen Maßnahmen sind vor dem Fortsetzen der weiteren Aktivitätsfelder auf ihre Eignung, das Zusammenwirken mit schon bestehenden Maßnahmen, ihrer Benutzerfreundlichkeit und ihrer Angemessenheit unter Beachtung der Grundsätze in Anlage 11.1.8 zu prüfen.

11.1.11 Basis-Sicherheitscheck Teil 2

57. Falls eine Risikoanalyse durchgeführt wurde und ergänzende Maßnahmen festgelegt wurden, ist ein weiterer Basis-Sicherheitscheck durchzuführen, der mit den konsolidierten Maßnahmen aus der Risikoanalyse analog zum vorherigen Basis-Sicherheitscheck aus Anlage 11.1.9 verläuft.

11.1.12 Realisierung / Umsetzung

58. Nach dem Durchlaufen aller Aktivitätsfelder sind die ermittelten Maßnahmen zur Risikoreduzierung umzusetzen. Für Maßnahmen, die nur teilweise oder noch nicht umgesetzt sind, ist auf Basis der Bewertung der zugeordneten Risiken und der vorhandenen Ressourcen eine Umsetzungsreihenfolge mit Priorisierung festzulegen und eine Aufteilung der Maßnahmen auf Jahresscheiben vorzunehmen.

Die weitere Umsetzung der Maßnahmen aus der priorisierten Liste ist fortlaufend im InfoSichhK zu dokumentieren und fortzusetzen, bis alle Maßnahmen aus der priorisierten Liste vollständig umgesetzt sind.

11.2 Besondere Festlegungen für normalen Schutzbedarf

11.2.1 Regelungen zur Nutzung privater IT und IT Dritter

1. Die technische (kabelgebundene oder drahtlose) Verbindung privater IT mit dem IT-SysBw bzw. die Installation privater IT und die Nutzung privater Datenträger im IT-SysBw sind bis auf die in diesem Abschnitt explizit genannten Fälle verboten.

2. Die Verbindung dienstlicher IT mit privaten Datenübertragungseinrichtungen (z. B. DSL-Anschlüsse) ist ausschließlich für Zwecke der Telearbeit und des Remote-Zugangs zulässig und nur dann, wenn die dienstlichen Informationen gemäß den Vorgaben dieser Zentralen Dienstvorschrift bei der Übertragung geschützt sind.

3. Die Nutzung von privater IT zu dienstlichen Zwecken ist grundsätzlich nicht zulässig. Ausnahmen regeln die zuständigen DStLtr / KtgtFhr. Ausnahmegenehmigungen sind zur InfoSichhDok (siehe Abschnitt 6.1.1) zu nehmen. Bei der Verarbeitung / Übertragung von VS gemäß Nr. 202 bzw. PersDat der Schutzbereiche 2 und 3 gemäß Nr. 203 sind keine Ausnahmen zulässig.

4. In Unterkünften der Bw und in Diensträumen, in denen Informationen bis zur Einstufung von höchstens VS-NfD verarbeitet werden, ist die Verwendung privater IT zu privaten Zwecken grundsätzlich zulässig. Sprachgesteuerte Dienste der privaten IT sind zu deaktivieren. Entsprechende Regelungen hierzu sind durch die jeweils zuständigen DStLtr / KtgtFhr zu treffen.

5. Die Nutzung von IT Dritter[150] und deren (kabelgebundene oder drahtlose) Verbindung mit dem IT-SysBw (z. B. im Rahmen von Wartungsarbeiten) ist ausschließlich unter Einhaltung der vertraglich vereinbarten und im jeweiligen InfoSichhK festgelegten Regelungen unter Berücksichtigung der Vorgaben dieser Zentralen Dienstvorschrift zulässig.

6. Anlage 11.2.1 ist im IT-Grundschutzkatalog der Bw in den Maßnahmen M 2.1001, M 2.1002 und M 2.1003 umgesetzt.

11.2.2 Nutzung von dienstlicher IT

7. Die Nutzung dienstlicher IT ist grundsätzlich nur zu dienstlichen Zwecken zulässig. Die Nutzung dienstlicher IT zu privaten Zwecken ist ausschließlich im Rahmen zentral durch BMVg zu treffender Dienstvereinbarungen zulässig.

8. Anlage 11.2.2 ist im IT-Grundschutzkatalog der Bw in der Maßnahme M 2.1002 umgesetzt.

[150] „Dritter“ ist jemand der IT-Dienstleistungen für die Bundeswehr erbringt (z.B. Auftragnehmer). Andere Bundesressorts gelten dabei nicht als Dritte.

11.2.3 Fernwartung (P, V, O, S)

9. Bei Fernwartung über Fremdnetze mit vom Auftragnehmer betriebener, auftragnehmereigener IT sind die Vorgaben des Abschnitts 4.6.2 (Nutzung eines Sicherheitsgateways, siehe Begriffsbestimmungen in der Anlage 11.11) zu beachten.

10. Anlage 11.2.3 ist im IT-Grundschutzkatalog der Bw in der Maßnahmen M 4.1007 umgesetzt.

11.2.4 Nutzung von Werkzeugen zur Umgehung von Zugangskontrollen

11. Die Nutzung und Weitergabe von Werkzeugen / Programmen zum Umgehen bzw. Überwinden von Zugangskontrollen / -sicherungen gemäß StGB (Dokument (5), §§ 202a, 202b und 202c) im GB BMVg ist grundsätzlich verboten. Ausnahmen für Zwecke der InfoSichh (z. B. für Teile des ZCSBw) genehmigt der bzw. die CISOBw.

11.2.5 Protokollierung (P, V, O, S)

12. Die zu protokollierenden und nachzuweisenden Ereignisse bei der Verwendung der IT sind mindestens im Rahmen der Erstellung der InfoSichhKProj zu spezifizieren und unter Berücksichtigung des Datenschutzes (siehe Bezüge Anlage 11.15 (lfdNrn. 2,10 und 65)) und des Geheimschutzes (siehe Bezüge Anlage 11.15 (lfdNrn. 11 und 15)) umzusetzen.

13. Die Anforderungen an die Vertraulichkeit, Integrität und die Verfügbarkeit von Protokolldaten sind im InfoSichhKProj festzulegen (siehe auch Nr. 201 und Anlage 11.4.4, Abb. 24). Die Anlage 11.6 ist zu beachten.

14. Anlage 11.2.5 ist im IT-Grundschutzkatalog der Bw in der Maßnahmen M 2.1008 umgesetzt.

11.2.6 Informationsaustausch zwischen unterschiedlichen Informationsräumen (P, V, O, S)

15. Sollen zwischen unterschiedlichen Informationsräumen (siehe Begriffsbestimmungen in der Anlage 11.11) Informationen ausgetauscht werden, so ist der Informationsfluss durch Sicherheitsgateways (siehe Begriffsbestimmungen in der Anlage 11.11) technisch zu steuern. Sicherheitsgateways können sowohl Hardware- als auch Softwarekomponenten sein.

16. Sicherheitsgateways sind immer dann einzusetzen, wenn

- bzgl. der Vertraulichkeit ein Sicherheitsgefälle besteht oder
- verschiedene Informationsräume (z.B. DEU, NATO EU) genutzt werden sollen oder
- ein Dritter[151] (z. B. ein Auftragnehmer) – mit von ihm selbst betriebener IT – Aufgabenbereiche gemäß Abschnitt 4.6.2 für die Bw übernimmt.

[151] Andere Bundesressorts, die IT-Dienstleistungen für die Bundeswehr erbringen, gelten nicht als Dritte.

Bei einem Sicherheitsgefälle bzgl. der Grundwerte Integrität und Verfügbarkeit bzw. zwischen unterschiedlichen Systemen ist der Einsatz eines Sicherheitsgateways in Betracht zu ziehen.

17. Sind Informationen der Einstufung VS-VERTRAULICH oder höher betroffen, müssen die Sicherheitsgateways zugelassen sein (siehe auch Abschnitt 5.3). Bei den Grundwerten Integrität und Verfügbarkeit genügt eine Eignungsfeststellung durch CISOBw.

18. Anlage 11.2.6 ist im IT-Grundschutzkatalog der Bw in den Maßnahmen M 4.1005, M 4.1006, M 4.1007 und M 4.1008 umgesetzt.

11.2.7 Bauliche Absicherungsmaßnahmen (D, E)

19. Die Forderungen gemäß der Bereichsvorschrift C1-1810/0-6000 VS-NfD „Grundsätzliche Militärische Infrastrukturforderung für bauliche Absicherungsmaßnahmen im Bereich der Bundeswehr“, (siehe Bezug Anlage 11.15 (lfdNr. 24)) und der Bereichsdienstvorschrift C-1800/121 „Infrastrukturbearbeitung“ (InfraHBKasKdt, siehe Bezug Anlage 11.15 (lfdNr. 25)) sind umzusetzen. Die Baufachlichen Richtlinien (BFR) (C-1800/114 Version 1 „Allgemeine baufachliche Vorgaben für die Durchführung von Baumaßnahmen der Bundeswehr“, siehe Bezug Anlage 11.15 (lfdNr. 23)) und das „Handbuch Bauliche Absicherung“ (AllgUmdr 175, siehe Bezug Anlage 11.15 (lfdNr. 26)) sind zu beachten.

20. Bei mobiler IT sind die Besonderheiten des Einsatzes und die daraus resultierenden Gefährdungen zu berücksichtigen.

21. Anlage 11.2.7 ist im IT-Grundschutzkatalog der Bw in den Maßnahmen M 1.1009 umgesetzt. Die Anlage 11.9.1 ist zu beachten. Weitere Informationen sind in der Maßnahme M 1.61 zu finden.

11.2.8 Belehrungen und deren Nachweis (D, E)

22. Die IT-Anwender sowie das IT-Personal haben aufgrund der Amtsverschwiegenheit die Pflicht, durch Verschwiegenheit zur Wahrung der InfoSichh beizutragen.

23. Das IT-Personal ist – in Abhängigkeit von der Tätigkeit – durch den jeweils zuständigen bzw. die jeweils zuständige ISBDSt / ISB i.E. zur InfoSichh zu belehren und zu verpflichten (Unterzeichnung der Verpflichtungs- / Belehrungserklärung gemäß Anlage 11.8.6).

24. Die IT-Anwender sowie das IT-Personal sind über die für die DSt / das EinsKtgt geltenden InfoSichh-Bestimmungen und ihre Pflichten zur Wahrung der InfoSichh durch den bzw. die ISBDSt / ISB i.E. zu belehren. Die Belehrung soll mindestens folgende Thematik abdecken (Anhalt):

- Vorschriften und Regelungen zur InfoSichh,
- Belehrung über den sicheren Umgang mit mobiler IT (siehe Anlage 11.9.1),
- Belehrung über die Regeln zur InfoSichh am Arbeitsplatz (siehe Anlage 11.9.2),
- Belehrung über Art und Folgen von InfoSichh-Verstößen sowie

- Dienststellen- und ggf. einsatz- organisationsbereichsspezifische Regelungen zur InfoSichh.

25. Die InfoSichh-Belehrung ist zu Beginn der Tätigkeit und im Anschluss daran grundsätzlich einmal jährlich durchzuführen. Ausnahmen regeln die ISBOrgBer.

26. Für Zwecke der Belehrung nutzen die ISBDSt / ISB i.E. querschnittlich bereit gestellte digitale Ausbildungshilfsmittel (DigAHM) auf Weisung des bzw. der CISOBw. Sofern die zur Verfügung stehenden digitalen Ausbildungshilfsmittel die Spezifika der OrgBer, DSt bzw. des Einsatzkontingentes nicht ausreichend abbilden sollten, ergänzen die ISBDSt / ISB i.E. die Belehrung um die zusätzlich benötigten Inhalte nach Vorgabe des zuständigen ISBOrgBer in geeigneter Form.

27. Die Nachweise über diese Belehrungen sind zusammen mit der Abschlussbelehrung (Einzelnachweis oder Sammelnachweis) zur InfoSichhDok der DSt / des EinsKtgt zu nehmen. Die Nachweise sind fünf Jahre aufzubewahren. Nach Auflösung des EinsKtgt sind die Nachweise bei EinsFüKdoBw aufzubewahren.

28. Anlage 11.2.8 ist (mit Ausnahme der Nr. 26) im IT-Grundschutzkatalog der Bw in Maßnahme M 3.1011 umgesetzt.

11.2.9 Zutrittsregelungen (D, E)

29. Zutritt zu Räumen, in denen IT betrieben wird, ist nicht zutrittsberechtigten Personen (z. B. Wartungspersonal, Reinigungspersonal und Besuchern) nur unter Aufsicht zu gewähren. Hierfür sind entsprechende Regelungen zu schaffen. Die Zutrittsregelungen zu Sperrzonen, die gemäß A-1130/1 VS-NfD „Militärische Sicherheit in der Bundeswehr – Militärische Sicherheit“ (siehe Bezug Anlage 11.15 (lfdNr. 14)) eingerichtet werden, bleiben davon unberührt.

30. Server / Zentraleinheiten sind in zutrittsbeschränkten Räumen zu installieren; die Zutrittsberechtigungen sind durch die DStLtr festzulegen. Bei Ausscheiden oder Wechsel des IT-Personals und der IT-Anwender sind Zutrittsrechte unverzüglich aufzuheben.

31. Anlage 11.2.9 ist im IT-Grundschutzkatalog der Bw in den Maßnahmen M 1.4101 und M 1.4102 umgesetzt. Darüber hinaus sind die Maßnahmen M 1.58 und M 2.17 zu beachten.

11.2.10 Maßnahmen für die Verwendung von Testdaten bei Übungen oder Tests

32. Im Rahmen von Übungen oder Tests (z. B. bei F&T-Prototypen) sind ausschließlich Testdaten zu verwenden. Soll an IT, die sich in Nutzung befindet, Tests durchgeführt werden, ist auf eine getrennte Verarbeitung von Test- und Echtdaten zu achten.

33. Zu Testzwecken dürfen nur anonymisierte Daten verwendet werden. Sind Tests bei IT mit Verarbeitung PersDat mit Testdaten nicht ausreichend, können mit folgenden Auflagen im Einzelfall Echtdaten verwendet werden:

- detaillierte Dokumentation der Notwendigkeit,
- Prüfung und schriftliche Zustimmung durch den bzw. die zuständige ADSB,
- Beschränkung auf das zeitlich notwendige Minimum und
- Zugriff nur durch Personen, die auch im Echtbetrieb mit den Daten arbeiten.

34. Anlage 11.2.10 ist im IT-Grundschutzkatalog der Bw in der Maßnahmen M 2.1013 umgesetzt.

11.2.11 Registrierung und Freigabe von dezentralen Netzübergängen

35. Für die Registrierung und Freigabe von Netzübergängen gilt:

1. Im **Verfahren zur Registrierung und Freigabe von dezentralen Netzübergängen (ReFNÜ)** sind alle dezentralen Netzübergänge[152] zu erfassen. Die A-960/11 (siehe Bezug Anlage 11.15 (lfdNr. 48)) regelt die Registrierung und Freigabe von Netzübergängen. Eine Einrichtung / Nutzung von dezentralen Netzübergängen (NÜ) außerhalb des ReFNÜ ist unzulässig und stellt ein InfoSichhVork (siehe Abschnitt 8) dar.
2. DSt, die bereits bei der Ersterfassung NÜ gemeldet haben, die jedoch über keine Ausnahmegenehmigung für einen später als kritisch bewerteten NÜ verfügen, müssen diesen NÜ über das ReFNÜ erneut beantragen.
   Hinweis: Bei einem Neuantrag ist die bereits in der Erstmeldung vergebene Identifikation (DStNr und lfdNr) des NÜ zwingend mit anzugeben. In der beizufügenden „Meldeliste NÜ“ ist im Feld „Bemerkung der DSt“ auf den Neuantrag hinzuweisen.
3. Ausnahmegenehmigungen werden nur durch den bzw. die CISOBw mit folgenden Auflagen erteilt:
   a. Die Ausnahmegenehmigung wird befristet als Zwischenlösung erteilt. Grundsätzlich sind alle NÜ in eine gesicherte DMZ-Struktur zu überführen.
   b. Die Ausnahmegenehmigung ist zur InfoSichhDok der DSt (siehe Abschnitt 6.1.1) zu nehmen.
4. Als kritisch bewertete NÜ, die aus Sicht der InfoSichh keine Ausnahmegenehmigung erhalten können, sind entweder zu sperren oder gemäß der Prozesse gemäß A-960/15 „IT-Krisenmanagement in der Bundeswehr“ (siehe Bezug Anlage 11.15 (lfdNr. 47)) zu behandeln.

36. Anlage 11.2.11 ist im IT-Grundschutzkatalog der Bw in der Maßnahmen M 2.1014 umgesetzt.

[152] Zur Begriffsbestimmung siehe Anlage 11.11

11.3 Grundsätze und ergänzende Informationssicherheits-Anforderungen und -Maßnahmen für hohen und sehr hohen Schutzbedarf sowie für Gewährleistungsziele

11.3.1 Allgemeines

1. Der IT-Grundschutz des BSI deckt grundsätzlich das Schutzbedarfsniveau „normal“ ab und wird daher im IT-Grundschutzkatalog der Bw um InfoSichh-Anforderungen und -Maßnahmen für hohen und sehr hohen Schutzbedarf ergänzt. Diese Anforderungen und Maßnahmen haben **immer Vorrang** gegenüber den InfoSichh-Anforderungen und -Maßnahmen aus den aktuellen IT-Grundschutzkatalogen des BSI, wenn Aussagen redundant sind oder sich widersprechen.

2. Für höheren Schutzbedarf als „normal“ in mindestens einem der drei Grundwerte sind über die InfoSichh-Maßnahmen des IT-Grundschutzes des BSI hinaus ergänzende InfoSichh-Maßnahmen umzusetzen.

3. Ergänzende InfoSichh-Maßnahmen sind im IT-Grundschutzkatalog der Bw mit Referenz-nummern wie in Anlage 11.1.2, Nrn. 8 - 13 dargestellt gekennzeichnet.

4. Es ist ausreichend, in den jeweiligen InfoSichhK die Maßnahmennummer zu referenzieren. Neue InfoSichh-Maßnahmen zur Erfüllung der Anforderungen sind vollständig aufzuführen.

11.3.2 Zuordnung von Informationssicherheits-Anforderungen zu den Schutzbedarfskategorien

11.3.2.1 Allgemeines

5. Für die jeweilig betrachtete IT sind für alle zutreffenden InfoSichh-Anforderungen, geeignete InfoSichh-Maßnahmen zu deren Erfüllung festzulegen.

6. Innerhalb der Grundwerte sind die Anforderungen kumulativ zu den Schutzbedarfskategorien gestaltet, d. h. für z. B. sehr hohen Schutzbedarf bei der Vertraulichkeit sind die gemäß Modellierung erforderlichen InfoSichh-Maßnahmen des IT-Grundschutzes des BSI umzusetzen sowie die bei einem hohen und einem sehr hohen Schutzbedarf dem Grundwert Vertraulichkeit zugeordneten Anforderungen mit geeigneten InfoSichh-Maßnahmen zu erfüllen.

7. Sollten sich InfoSichh-Maßnahmen widersprechen, sind die der jeweils höherwertigen Schutzbedarfskategorie zugeordneten InfoSichh-Maßnahmen umzusetzen.

8. Die gemäß dem Ergebnis der Modellierung erforderlichen InfoSichh-Maßnahmen des IT-Grundschutzes des BSI sind soweit anwendbar umzusetzen.

9. Für **Sonstige schutzbedürftige Informationen** (SSI) mit höherem Schutzbedarf als „normal“[153] in mindestens einem der drei Grundwerte und bei **Relevanz der Gewährleistungsziele** gilt, dass über die InfoSichh-Maßnahmen des IT-Grundschutzes des BSI und des IT-Grundschutzkataloges der Bw hinaus die in den folgenden Abschnitten 11.3.2.2 bis 11.3.4.5 aufgeführten Maßnahmen zusätzlich umzusetzen sind. Die Beschreibung der Maßnahmen ist Anlage 11.3.4 zu entnehmen.

11.3.2.2 Anforderungen für hohen Schutzbedarf der Vertraulichkeit

10. Die geforderten Maßnahmen sind im Grundschutz-Baustein B 1.451 Vertraulichkeit (hoch) zusammengefasst.

11. Ergänzende technische InfoSichh-Maßnahmen für SSI:

- M 4.2001 – Pseudonymisierung / Anonymisierung
- M 4.2002 – Verschlüsselung Sonstiger schutzbedürftiger Informationen
- M 4.2003 – Schutz gegen unerlaubten Datenabfluss im Rahmen Sonstiger schutzbedürftiger Informationen
- M 4.2004 – Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten

12. Ergänzende organisatorische InfoSichh-Maßnahmen für SSI

- M 2.2001 – Organisatorische Regelungen zur Rollentrennung, zum Berechtigungskonzept und zur Verwaltung von Nutzerkonten für Nicht Bundeswehrangehörige (NBwA)
- M 2.2002 – Kennzeichnungspflicht von Sonstigen schutzbedürftigen Informationen

13. Ergänzende personelle InfoSichh-Maßnahmen für SSI

- M 3.2002 – Maßnahmen zur Korruptionsprävention für Nicht Bundeswehrangehörige (NBwA) bei Zugang zu IT

11.3.2.3 Anforderungen für sehr hohen Schutzbedarf der Vertraulichkeit

14. Ergänzend zu den Anforderungen für hohen Schutzbedarf (siehe Nr. 10) werden im Grundschutz-Baustein B 1.454 Vertraulichkeit (sehr hoch) die erforderlichen zusätzlichen Maßnahmen für den sehr hohen Schutzbedarf der Vertraulichkeit zusammengefasst.

15. Ergänzende personelle InfoSichh-Maßnahmen für SSI:

- M 3.2001 – Maßnahmen zum Schutz von Privat- und Betriebs-/Geschäftsgeheimnissen für Nicht Bundeswehrangehörige (NBwA) bei Zugang zu IT

[153] Für den Schutzbedarf „normal“ reicht die Umsetzung der InfoSichh-Anforderungen und –Maßnahmen im IT-Grundschutzkatalog der Bw bezüglich der betroffenen Grundwerte aus.

11.3.2.4 Anforderungen für hohen Schutzbedarf der Verfügbarkeit

16. Die geforderten Maßnahmen sind im Grundschutz-Baustein B 1.452 Verfügbarkeit (hoch) zusammengefasst.

17. Ergänzende technische InfoSichh-Maßnahmen für SSI:

- M 4.2003 – Schutz gegen unerlaubten Datenabfluss im Rahmen Sonstiger schutzbedürftiger Informationen
- M 4.2007 – Deaktivierungsmöglichkeiten von Funktionalitäten

11.3.2.5 Anforderungen für sehr hohen Schutzbedarf der Verfügbarkeit

18. Ergänzend zu den Anforderungen für hohen Schutzbedarf (siehe Nr. 16) sind für den Anwendungsbereich (z.B. Projekt oder DSt) spezifische Festlegungen auf technischer, organisatorischer, personeller und infrastruktureller Ebene zu treffen.

19. Ergänzende personelle InfoSichh-Maßnahmen für SSI:

- M 3.2003 – Maßnahmen für Eigenentwicklungen in IT

11.3.2.6 Anforderungen für hohen Schutzbedarf der Integrität

20. Die geforderten Maßnahmen sind im Grundschutz-Baustein B 1.453 Integrität (hoch) zusammengefasst.

21. Ergänzende technische InfoSichh-Maßnahmen für SSI:

- M 4.2002 – Verschlüsselung Sonstiger schutzbedürftiger Informationen
- M 4.2003 – Schutz gegen unerlaubten Datenabfluss im Rahmen Sonstiger schutzbedürftiger Informationen
- M 4.2006 – Authentizität

11.3.2.7 Anforderungen für sehr hohen Schutzbedarf der Integrität

22. Ergänzend zu den Anforderungen für hohen Schutzbedarf (siehe Nr. 20) sind für den Anwendungsbereich (z.B. Projekt oder DSt) spezifische Festlegungen auf technischer, organisatorischer, personeller und infrastruktureller Ebene zu treffen. Ein Beispiel ist der Einsatz qualifizierter elektronischer Signaturen gemäß Vertrauensdienstegesetz (siehe Bezug Anlage 11.15 (lfdNr. 3)). Die benötigten Zertifikate sind in diesem Fall in Zusammenarbeit mit dem Projekt PKIBw bereitzustellen.

23. Ergänzende technische InfoSichh-Maßnahmen für SSI:

- M 4.2004 – Schutz gegen unerlaubte Veränderungen von Daten

11.3.3 InfoSichh Maßnahmen bei Relevanz der Gewährleistungsziele

11.3.3.1 Gewährleistungsziel Nichtverkettung

24. Technische InfoSichh-Maßnahmen

- M 4.2001 – Pseudonymisierung / Anonymisierung
- M 4.2005 – Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten
- M 4.2007 – Deaktivierungsmöglichkeiten von Funktionalitäten
- M 4.4402[154] – Technische Vorgaben zur Rollentrennung
- M 4.4403 – Technische Vorgaben zur Rechteverwaltung

25. Organisatorische InfoSichh-Maßnahmen

- M 2.2001 – Organisatorische Regelungen zur Rollentrennung, zum Berechtigungskonzept und zur Verwaltung von Nutzerkonten für Nicht Bundeswehrangehörige (NBwA)
- M 2.4206 – Organisatorische Regelung zur Rollentrennung, zum Berechtigungskonzept und zur Verwaltung von Nutzerkonten

11.3.3.2 Gewährleistungsziel Transparenz

26. Technische InfoSichh-Maßnahmen

- M 4.2004 – Schutz gegen unerlaubte Veränderungen von Daten
- M 4.2006 – Authentizität

11.3.3.3 Gewährleistungsziel Intervenierbarkeit

27. Technische InfoSichh-Maßnahmen

- M 4.2004 – Schutz gegen unerlaubte Veränderungen von Daten
- M 4.2006 – Authentizität
- M 4.2007 – Deaktivierungsmöglichkeiten von Funktionalitäten

11.3.4 Beschreibung der ergänzenden Informationssicherheitsmaßnahmen im Zusammenhang mit Sonstigen schutzbedürftigen Informationen und den Gewährleistungszielen

11.3.4.1 Allgemeines

28. Dieser Maßnahmenkatalog ist unterteilt in die vier Kategorien Infrastruktur, Organisation, Personal und Technik. Er wird in unregelmäßigen Abständen aktualisiert. Die jeweils aktuelle Version

[154] Maßnahmen mit der Kennung M x.xxx sind Maßnahmen aus dem IT-Grundschutzkatalog der Bundeswehr

ist im Intranetauftritt http://it-sicherheit.bundeswehr.org im Bereich „Fachinformationen / IT-Grundschutz / Bausteine und Metadaten“ zu finden[155].

11.3.4.2 Infrastruktur

29. tbd

11.3.4.3 Organisation

30. M 2.2001 – Organisatorische Regelungen zur Rollentrennung, zum Berechtigungskonzept und zur Verwaltung von Nutzerkonten Nicht Bundeswehrangehöriger (NBwA)
Für absehbar mittel- oder langfristig erforderliche Unterstützungsleistungen durch externe Kräfte (NBwA) sind analog zu bereits bestehenden Rollen die Zugriffsberechtigungen zu berücksichtigen, die explizit für die Vergabe an NBwA vorzusehen sind. Der Umfang der Berechtigungen ist hierbei auf das Notwendige zu beschränken (need to know).

31. M 2.2002 – Kennzeichnungspflicht von Sonstigen schutzbedürftigen Informationen
Die mit IT zu verarbeitenden oder zu übertragenden Sonstigen schutzbedürftigen Informationen (SSI) sind entsprechend ihrer Behandlung zu kennzeichnen, z.B. „Firmenvertraulich“.

11.3.4.4 Personal

32. M 3.2001 – Maßnahmen zum Schutz von Privat- und Betriebs-/Geschäftsgeheimnissen für Nicht Bundeswehrangehörige (NBwA) bei Zugang zu IT
Soll Personen der Zugang zu IT gewährt werden, ist zu prüfen, ob diesen der Zugang nach förmlicher Verpflichtung oder nach Belehren als "sonstige mitwirkende Person" gewährt werden kann. Siehe hierzu den entsprechenden Hinweis von BMVg R I 5. (Anlage 11.14)

33. M 3.2002 – Maßnahmen zur Korruptionsprävention für Nicht Bundeswehrangehörigen (NBwA) bei Zugang zu IT
Etwaigen Strafbarkeitslücken hinsichtlich Korruptionsstraftaten in Folge fehlender Amtsträger-eigenschaft handelnder Personen (NBwA) ist durch förmliche Verpflichtung nach dem Verpflichtungs-gesetz entgegen zu wirken.

34. M 3.2003 – Maßnahmen für Eigenentwicklungen in IT
Bei Eigenentwicklungen sind die Programmierrichtlinien gem. B- 1500/8 „Erstellung von Applikationen durch IT-Anwender und IT-Anwenderinnen“ einzuhalten und zu dokumentieren.

[155] Die Maßnahmen werden durch KdoCIR in entsprechende Bausteine im IT-Grundschutzkatalog der Bw aufgenommen.

11.3.4.5 Technik

35. M 4.2001 – Pseudonymisierung / Anonymisierung

Die IT muss über eine Funktion zur Pseudonymisierung / Anonymisierung verfügen, um bei

- Entwicklungs-/Testumgebungen,
- Verkettung von IT sowie
- Bereitstellung von Daten an externe Dritte

Daten teil- bzw. automatisiert pseudo- / anonymisiert bereitstellen zu können.

36. M 4.2002 – Verschlüsselung Sonstiger schutzbedürftiger Informationen

Sonstige schutzbedürftige Informationen sind grundsätzlich mit Produkten / Verfahren, die dem Stand der Technik entsprechen, zu verschlüsseln. Ausnahmen sind zulässig, wenn ein unberechtigter Zugriff auf die Informationen durch andere Sicherheitsmaßnahmen verhindert werden kann (die Risikobewertung obliegt dem bzw. der zuständigen ProjLtr / DStLtr / KtgtFhr / Verantwortlichen für Infra-Maßnahmen und ist zu dokumentieren).

37. M 4.2003 – Schutz gegen unerlaubten Datenabfluss im Rahmen Sonstiger schutzbedürftiger Informationen

Die IT muss über die Funktionen verfügen, um

- unberechtigte Downloads,
- unberechtigtes Kopieren sowie
- unberechtigtes Drucken

zu verhindern.

38. M 4.2004 – Schutz gegen unerlaubte Veränderungen von Daten

Die IT muss über die Funktion verfügen, dass relevante Daten nach Handelsgesetzbuch (HGB), Bundeshaushaltsordnung (BHO) und / oder Abgabenordnung (AO) nicht veränderbar sind.

39. M 4.2005 – Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten

Die IT muss über die Funktion verfügen, eine programmtechnische Unterlassung bzw. Schließung von Schnittstellen in Verfahren und Verfahrenskomponenten durchzuführen.

40. M 4.2006 – Authentizität

Die IT muss über Funktionen,

- einen Nachweis der Datenquelle zu erbringen bzw. nachzuhalten,
- einer Versionierung sowie
- einer technischen Dokumentation der Verarbeitungsprozesse

verfügen.

41. M 4.2007 – Deaktivierungsmöglichkeiten von Funktionalitäten

Die IT muss über eine Funktion verfügen, einzelne Funktionalitäten ohne Auswirkung auf das Gesamtsystem deaktivieren zu können.

11.4 Vorgaben und Hilfestellungen zur Festlegung des Schutzbedarfes

11.4.1 Allgemeines

1. Um bei der Festlegung der Schutzbedarfskategorien (siehe Nr. 125 f) bezogen auf die Grundwerte der InfoSichh (siehe Nr. 111) und die Gewährleistungsziele (siehe Nr. 112) Inkonsistenzen in den verschiedenen InfoSichhK in der Bw zu vermeiden, werden in dieser Anlage Vorgaben gemacht und Hilfestellungen gegeben, die einen Kompromiss zwischen einer genauen und zielführenden Definition als auch einer universellen Anwendbarkeit darstellen. Diese Aufgabe gestaltet sich unterschiedlich bei den einzelnen Grundwerten.

11.4.2 Vertraulichkeit

11.4.2.1 Allgemeines

2. Bei der Vertraulichkeit (Definition siehe Nr. 111) geht es um den Schutz der Informationen gegen unbefugte Kenntnisnahme. Bei der Bewertung des Schutzbedarfes für die Vertraulichkeit ist zu beachten, dass es durch Zusammenstellungen großer Mengen vertraulicher Informationen auf IT notwendig werden kann, den Schutzbedarf für diesen Grundwert – bzgl. der genutzten IT-Plattform, auf der diese Informationen verarbeitet werden – höher als den Schutzbedarf der einzelnen Information zu bewerten (Kumulationseffekt)[156].

11.4.2.2 Verschlusssachen (VS)

3. Eine stringente Zuordnung der Schutzbedarfskategorien ist für VS bei der Vertraulichkeit möglich, da die Schutzbedarfskategorien in Abhängigkeit vom jeweiligen Geheimhaltungsgrad der VS festgelegt werden können. Die Bewertung der VS hinsichtlich des Grundwertes Vertraulichkeit wird für die Bw gemäß der generischen Informationsstruktur in Abschnitt 2.1.4 festgelegt.

11.4.2.3 Personenbezogene Daten (PersDat)

4. PersDat sind gemäß der Zentralen Dienstvorschrift A-2122/4 „Datenschutz“ (siehe Bezug Anlage 11.15 (lfdNr. 10)) entsprechend ihrer Schutzbedürftigkeit einem Schutzbereich (SB) zuzuordnen. PersDat mit geringem Schutzbedarf sind dem SB 1 zugehörig, sogenannte Funktionsträgerdaten (Name, Vorname, Dienst- bzw. Amtsbezeichnung, Funktion und Tätigkeitsbereich, dienstliche Haus-, Post- und E-Mailadresse, dienstliche Telefon- und Faxnummer). Diese abschließend aufgeführten Identifikationsdaten dürfen nur verarbeitet werden, soweit sie für die Gestaltung des Dienstbetriebes notwendig sind und nur für diese Zwecke verwendet werden.

[156] siehe hierzu VSA, dort Anlage 1, Nr. 2 (siehe Bezug Anlage 11.15 (LfdNr. 11)) und BSI-Standard 200-2, dort Unterkapitel 8.2.2 und 8.2.4 (siehe Bezug Anlage 11.15 (LfdNr. 46))

5. PersDat mit hohem Schutzbedarf sind dem SB 3 zugeordnet. Das sind zunächst die besonderen Kategorien personenbezogener Daten (BPersDat), die wie folgt in Art. 9 Abs. 1 EU-DSGVO abschließend aufgezählt sind:

- rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder Weltanschauliche Überzeugungen,
- Gewerkschaftszugehörigkeit
- genetische Daten,
- biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten, die sich auf eine körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen,
- Impfdaten und Daten zu Aspekten durchgeführter oder vorgesehenen Impfungen,
- Daten zum Sexualleben oder sexueller Orientierung inkl. Familienstand „eingetragene Lebenspartnerschaft“.

Zum Schutzbereich 3 zählen aber auch PersDat aufgrund ihrer vergleichbaren Eingriffsintensität, wie z.B.

- PersDat über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln,
- PersDat in Sicherheitsakten,
- PersDat in Disziplinarakten,
- Auszüge aus dem Bundeszentralregister (z.B. Führungszeugnisse),
- PersDat in Gerichtsakten oder Urteilen und Gerichtsbeschlüsse mit sensiblen Inhalten, z.B. Pfändungs- und Überweisungsbeschlüssen,
- Beurteilungen, auch Beiträge zu Beurteilungen, wenn Angaben zur Gesundheit enthalten sind,
- Personalaktendaten nach sachgerechter Bewertung können auch PersDat SB 3 zugeordnet sein.

Eine abschließende Aufzählung PersDat SB 3 ist nicht möglich.

6. Die übrigen PersDat haben einen mittleren Schutzbedarf und sind dem SB 2 zugehörig.

7. Weitere Einzelheiten sind bei Widersprüchen und Lücken vorrangig der anzuwendenden Nr. 1400 ff der Zentralen Dienstvorschrift A-2122/4 „Datenschutz“[157] (siehe Bezug Anlage 11.15 (lfdNr. 10)) zu entnehmen. Für die Bewertung von PersDat hinsichtlich des Grundwertes Vertraulichkeit können gemäß BSI-Standard 200-2 (siehe Bezug Anlage 11.15 (lfdNr. 46)) darüber hinaus die nachfolgenden Hilfestellungen dienen.

[157] Bis zur Fortschreibung der A-2122/4 Datenschutz gilt die Weisung BMVg R I 1 zur A-2122/4 „Datenschutz - Ausführungsbestimmung zur Europäischen Datenschutzgrundverordnung und dem Bundesdatenschutzgesetz vom 25. Mai 2018

8. Schutzbedarf „normal“

Es handelt sich um PersDat, durch deren Kenntnisnahme die Betroffenen in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen beeinträchtigt werden können. In der Bw handelt es sich hier um PersDat SB 1.

9. Schutzbedarf „hoch“

Es handelt sich um PersDat, durch deren Kenntnisnahme die Betroffenen in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden können. In der Bw handelt es sich hier in der Regel um PersDat SB 2.

10. Schutzbedarf „sehr hoch“

Es handelt sich um PersDat, durch deren Kenntnisnahme eine Gefahr für Leib und Leben oder die persönliche Freiheit der Betroffenen gegeben ist. In der Bw handelt es sich hier um PersDat SB 3. Entscheidend für die Einstufung ist ebenfalls der Verwendungszusammenhang. Dieser kann aus PersDat SB 1 bereits sehr hohen Schutzbedarf begründen.

11. Entscheidung

Bei der Entscheidung, welche Schutzkategorie zutreffend ist, ist zwingend der bzw. die ADSB der DSt zu beteiligen.

11.4.2.4 Sonstige schutzbedürftige Informationen

12. Für die Sonstigen schutzbedürftigen Informationen kann eine stringente Zuordnung zu den Schutzbedarfskategorien wie bei der Vertraulichkeit von VS (siehe Anlage 11.4.2.2) nicht vorgenommen werden. Hier wird auf die Hilfestellungen zu den Grundwerten „Verfügbarkeit“ und „Integrität“ gemäß Anlage 11.4.3.1 verwiesen.

11.4.3 Verfügbarkeit und Integrität

11.4.3.1 Allgemeines

13. Für diese zwei Grundwerte (Definitionen siehe Nr. 111) kann eine vergleichbare Zuordnung wie bei der Vertraulichkeit nicht vorgenommen werden. Hilfestellungen für eine Zuordnung liefern die nachfolgenden Erläuterungen und Tabellen. Für VS ist Abschnitt 2.1.4, Nr. 210 zu beachten.

14. Im Folgenden werden die Schutzbedarfskategorien für die Grundwerte Verfügbarkeit und Integrität mithilfe der vom BSI im BSI-Standard 200-2, Anhang 12.1 (siehe Bezug Anlage 11.15 (lfdNr. 46)) vorgeschlagenen Schadensszenarien definiert. Diesen liegt die Idee zu Grunde, dass sich die Auswirkungen, die von einem Verlust der Grundwerte ausgehen können, auf verschiedene Schadensszenarien beziehen können. Folgende Einteilung hat sich etabliert.

15. Beeinträchtigungen des Rechts auf informationelle Selbstbestimmung

Bei der Implementierung und dem Betrieb von IT besteht die Gefahr – im Einzelfall sogar strafbewährt - einer Verletzung des Rechts auf informationelle Selbstbestimmung bis hin zu einem Missbrauch von PersDat. Beispiele für die Beeinträchtigung des Rechts auf informationelle Selbstbestimmung sind:

- Verfälschung von PersDat in IT oder bei der Übertragung.

Typische Einzelfragen als Basis zur Bewertung dieses Schadensszenarios sind:

- Können Unbefugte PersDat zu anderen als den zulässigen Zwecken weiterverarbeiten?
- Ist es im Zuge einer zulässigen Verarbeitung von PersDat möglich, aus diesen Daten, z. B. Rückschlüsse auf den Gesundheitszustand oder die wirtschaftliche Situation einer Person, zu ziehen?
- Ist kontrollierbar, ob zulässige Zugriffsrechte nur dazu benutzt werden, Zugriffe nur im Rahmen der Wahrnehmung von dienstlichen Aufgaben durchzuführen?
- Gibt es Sicherheitslücken in IT-Verfahren, die es Angreifern ermöglichen, PersDat zu manipulieren?
- Erleichtert eine fehlende Funktionstrennung zwischen Programmierung, Systemtechnik und Verfahrensanwendung eine unerkannte Veränderung gespeicherter PersDat?
- Können bei Ausfall von IT oder bei Störung einer Datenübertragung PersDat verloren gehen oder verfälscht werden, so dass der bzw. die Betroffene massive Nachteile erleidet?

16. Beeinträchtigungen der persönlichen Unversehrtheit

Fehlerhafte oder fehlende Daten und Fehlfunktionen von IT oder IT-Anwendungen können die Verletzung, die Invalidität oder den Tod von Personen nach sich ziehen. Beispiele für kritische Bereiche sind:

- Lagedaten,
- Gesundheitsunterlagen sowie
- Steuerungsdaten von Waffensystemen, etc.

Typische Einzelfragen als Basis zur Bewertung dieses Schadensszenarios sind:

- Kann ein Vertraulichkeitsverlust von Daten indirekt die Gesundheit oder das Leben von Personen bedrohen?
- Können durch manipulierte Programmabläufe oder Daten Menschen gesundheitlich gefährdet werden?
- Bedroht der Ausfall von IT die persönliche Unversehrtheit von Personen?

17. Verstöße gegen andere Gesetze, Vorschriften oder Verträge

Ein Schaden entsteht, wenn in anderer Form als oben schon genannt gegen Gesetze oder Vorschriften verstoßen wird. Das können zum Beispiel das Strafgesetzbuch, zum Beispiel das unbefugte Offenbaren von Privatgeheimnissen nach § 203 Strafgesetzbuch oder Verändern von Daten nach StGB § 303a, Personalvertretungsgesetz, Urheberrechtsgesetz, sowie eigene Verordnungen und Vorschriften im GB BMVg, z. B. zum Umgang mit VS sein. Auch ein Vertragsvertoß ist als Schaden zu qualifizieren.

Beispiele für Verträge sind: Dienstleistungsverträge im Bereich Datenverarbeitung oder Verträge zur Wahrung von Betriebsgeheimnissen.

Bei solchen Verstößen erfolgt keine Bewertung des Schadens, da ein solcher Schaden aufgrund der Bindung der Verwaltung an Recht und Gesetz gem. Art. 20 Abs. 3 GG immer zu vermeiden ist.

18. Beeinträchtigungen der Aufgabenerfüllung

Insbesondere der Verlust der Verfügbarkeit einer IT-Anwendung oder der Integrität der Informationen kann die Aufgabenerfüllung der Bw beeinträchtigen. Die Schwere des Schadens richtet sich hierbei nach der zeitlichen Dauer der Beeinträchtigung, nach dem Umfang der Einschränkungen und nach dem Vorhandensein möglicher Ausweichlösungen. Bezüglich des Verlusts der Integrität ist auch die Dauer bis zur Bewusstwerdung des Schadens ein erheblicher Einflussfaktor.

Typische Einzelfragen als Basis zur Bewertung dieses Schadensszenarios sind:

- Können Datenveränderungen die Aufgabenerfüllung dergestalt einschränken, dass ein System / eine Einheit / eine DSt handlungsunfähig wird?
- Entstehen erhebliche Schäden, wenn die Aufgaben trotz verfälschter Daten wahrgenommen werden?
- Wann werden unerlaubte Datenveränderungen frühestens erkannt?
- Können verfälschte Daten in der betrachteten IT-Anwendung zu Fehlern in anderen IT-Anwendungen führen?
- Kann beim Ausfall von IT ein Notbetrieb aufrechterhalten werden?
- Können die Aufgaben einer betroffenen DSt (eingeschränkt, temporär) von einer anderen DSt übernommen werden?
- Wie zeitkritisch ist eine IT-Anwendung?
- Sind von dem Ausfall dieser IT-Anwendung andere IT-Anwendungen betroffen?
- Ist es für die DSt bedeutsam, dass der Zugriff auf die IT-Anwendungen nebst Programmen und Daten ständig gewährleistet ist?

19. Negative Innen- / Außenwirkung

Durch den Verlust von einem der Grundwerte Integrität oder Verfügbarkeit in einer IT-Anwendung kann das Ansehen einer DSt / einer Organisationseinheit bis hin zur gesamten Bw oder noch darüber hinaus nach innen und außen beeinträchtigt werden. Die Höhe des Schadens orientiert sich an der Schwere des Sicherheitsverlustes und des Verbreitungsgrades der Außenwirkung.

Ursachen für derartige Schäden können vielfältiger Natur sein:

- Handlungsunfähigkeit einer Einheit oder DSt durch IT-Ausfall.
- Fehlerhafte Veröffentlichungen durch manipulierte Daten.

Typische Einzelfragen zur Bewertung dieses Schadensszenarios sind:

- Wird die Verfälschung von Daten öffentlich bekannt?
- Entstehen bei einer Veröffentlichung von verfälschten Informationen Ansehensverluste?
- Schränkt der Ausfall der IT-Anwendung die Informationsdienstleistungen für Dritte bzw. die Zusammenarbeit mit diesen ein?
- Wird der (vorübergehende) Ausfall der IT-Anwendung extern bemerkt?

20. Finanzielle Auswirkungen

Finanzielle Schäden können unmittelbar oder mittelbar durch den die Veränderung von Daten oder den Ausfall einer IT-Anwendung entstehen. Beispiele dafür sind:

- finanzielle Folgeschäden nach Ausfall eines Dienstes,
- fehlerhafte Abrechnungen / Rechnungen,
- Diebstahl oder Zerstörung von Hardware / Software sowie
- Schadensersatzansprüche.

Typische Einzelfragen als Basis zur Bewertung dieses Schadensszenarios sind:

- Kann die Veröffentlichung falscher Informationen Regressforderungen nach sich ziehen?
- Werden mit der IT-Anwendung Informationen gespeichert, die einen erheblichen Wert darstellen? Was passiert, wenn sie verfälscht werden?
- Können durch Datenmanipulationen finanzwirksame Daten so verändert werden, dass finanzielle Schäden entstehen?
- Wie hoch sind die Reparatur- oder Wiederherstellungskosten bei Ausfall, Defekt, Zerstörung oder Diebstahl von IT?

11.4.3.2 Integrität

21. Für die Schutzbedarfskategorien beim Grundwert Integrität gibt es keine gesetzlichen oder sonstigen Vorgaben.

Bei der Integrität geht es darum, Manipulationen an den Informationen oder an der IT zu erkennen bzw. zu verhindern sowie um die Beurteilung der Notwendigkeit, nachweisen zu müssen, ob die Information einem bestimmten Urheber bzw. einer bestimmten Urheberin und / oder einem bestimmten Absender zugeordnet werden muss (Nichtabstreitbarkeit) bzw. einen bestimmten Empfänger erreicht hat (Nachweisbarkeit).

22. Für einen normalen Schutzbedarf müssen Manipulationen zumindest im Nachhinein manuell erkannt werden können.

23. Eine **hohe Integrität** bedeutet, dass zur Erkennung von Manipulationen IT-gestützte Funktionen realisiert werden müssen bzw. dass die Identität von IT-Anwendern, die Authentizität von Rechnern, die Echtheit übertragener Informationen, die Einhaltung vorgegebener Übertragungswege

oder Sende- und Empfangsnachweise für Übertragungen für die IT-Anwender verbindlich feststellbar als auch Dritten gegenüber beweisbar sind.

24. Eine **sehr hohe Integrität** bedeutet, dass zur Erfüllung der Aufgabe Manipulationen im Vorhinein verhindert werden müssen bzw. dass

- eine Gerichtsverwertbarkeit der Informationen gewährleistet sein muss bzw.
- gesetzliche Vorgaben die Schriftform oder eine der Schriftform gleichwertige elektronische Form fordern.

25. In der Abb. 18, Abb. 19 und Abb. 20 sind Hilfestellungen aufgeführt.

26. Schutzbedarf **„normal“**

Schutzbedarfs-kategorie / Schadens szenarien	**Normal (Integrität)**
Beeinträchtigung des Rechts auf informationelle Selbstbestimmung	• Eine Beeinträchtigung des informationellen Rechts auf Selbstbestimmung ist im Zusammenhang mit den betroffenen Daten nicht möglich. • Eine mögliche Fälschung von PersDat würde erkannt werden und die Daten könnten wiederhergestellt werden. • Es entstehen keine oder nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des bzw. der Betroffenen.
Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung der persönlichen Unversehrtheit aufgrund der nicht garantierten Zuordenbarkeit von Urheberschaft oder Empfang von Daten oder Aktionen in IT-Anwendungen oder von falschen / gefälschten Daten oder manipulierten IT-Anwendungen erscheint kaum möglich bzw. wäre hinsichtlich Umfang und Schwere auf ein, bezogen auf die Einsatzart, erträgliches Maß begrenzt.
Beeinträchtigung der Aufgabenerfüllung	• Ein Integritätsverlust hat keine oder unbedeutende Auswirkungen auf die Aufgabenerfüllung. • Die Beeinträchtigung der Aufgabenerfüllung würde von den Betroffenen als tolerabel eingeschätzt werden. • Verfälschte Daten oder manipulierte Funktionen würden erkannt werden und könnten zeitnah rekonstruiert / wiederhergestellt werden. • Fehlende Zuordenbarkeit von Urheberschaft oder Empfang von Daten bzw. generell von Aktionen im IT-Bereich würden erkannt werden und es könnte zeitnah Abhilfe geschaffen werden. Auch wenn keine Abhilfe geschaffen werden kann, wäre die Aufgabenerfüllung dadurch nur gering beeinträchtigt. • Es existieren effiziente Ausweichmöglichkeiten.
Negative Innen- / Außenwirkung	• Ein möglicher Ansehensverlust ist nicht nennenswert oder lediglich in der betroffenen Dienststelle / in deren engerem Bereich zu erwarten.
Finanzielle Auswirkungen	• Der finanzielle Schaden ist tolerabel (<= 100.000.- €)[158].

Abb. 18 Schutzbedarfskategorie „normal“ für den Grundwert Integrität

[158] Gemäß BSI-Standard (Anlage 11.15 (Nr. 46)) und Studie IABG zur Einführung des Grundschutzes in die Bundeswehr von 2010

27. Schutzbedarf **„hoch“**

Schutzbedarfs-kategorie / Schadens szenarien	Hoch (Integrität)
Beeinträchtigung des Rechts auf informationelle Selbstbestimmung	• Ein Verlust der Integrität zieht eine erhebliche Beeinträchtigung des Rechts auf informationelle Selbstbestimmung nach sich. Ein möglicher Missbrauch von Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder wirtschaftlichen Verhältnisse einer großen Anzahl Betroffener. • Eine mögliche Fälschung von PersDat würde über einen längeren Zeitraum nicht erkannt werden. • Aktionen mit PersDat können über einen längeren Zeitraum nicht zugeordnet werden. • Es sind aggregierte oder hochsensitive Daten betroffen.
Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung der persönlichen Unversehrtheit aufgrund der nicht garantierten Zuordenbarkeit von Urheberschaft oder Empfang von Daten oder Aktionen in IT-Anwendungen oder von falschen / gefälschten Daten oder manipulierten IT-Anwendungen ist wahrscheinlich. Die Beeinträchtigung ist schwerwiegend.
Beeinträchtigung der Aufgabenerfüllung	• Ein Integritätsverlust hat erhebliche Auswirkungen auf die Aufgabenerfüllung. • Die Beeinträchtigung der Aufgabenerfüllung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt werden. • Verfälschte Daten oder manipulierte Funktionen würden längere Zeit nicht erkannt werden. • Eine komplette Rekonstruktion verfälschter Daten ist nicht oder nur stark verzögert möglich. • Die Zuordenbarkeit von Urheberschaft oder Empfang von Daten bzw. generell von Aktionen im IT-Bereich ist wesentlicher Bestandteil der Aufgabe. • Die Behebung von Softwarefehlern ist sehr aufwändig und nur stark verzögert möglich. • Es existieren Ausweichmöglichkeiten, welche aber nur einen deutlich eingeschränkten Funktionsumfang bieten und nur bei erheblichem Aufwand arbeitsfähig wären.
Negative Innen- / Außenwirkung	• Eine breite und deutliche Ansehens- und Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	• Der Schaden bewirkt beachtliche finanzielle Verluste (zwischen 100.000.- € und 1.000.000,- €)[159].

Abb. 19 Schutzbedarfskategorie „hoch“ für den Grundwert Integrität

[159] Gemäß BSI-Standard (Anlage 11.15 (Nr. 46)) und Studie IABG zur Einführung des Grundschutzes in die Bundeswehr von 2010

28. Schutzbedarf **„sehr hoch“**

Schutzbedarfs-kategorie / Schadens szenarien	Sehr hoch (Integrität)
Verstoß gegen Gesetze / Vorschriften / Verträge	• Verstöße gegen Vorschriften oder gegen Gesetze. • Vertragsverletzungen mit ruinösen Konventionalstrafen. • Negative zivil-, straf-, verwaltungs-, oder disziplinarrechtliche Folgen für die Verantwortlichen.
Beeinträchtigung des Rechts auf informationelle Selbstbestimmung	• Der Verlust der Integrität führt zu einer erheblichen Beeinträchtigung des Rechts auf informationelle Selbstbestimmung vieler Personen. Ein möglicher Missbrauch der Daten hat ruinöse Auswirkungen auf die gesellschaftliche Stellung und wirtschaftlichen Verhältnisse der Betroffenen. • Eine mögliche Fälschung von PersDat würde über einen sehr langen Zeitraum nicht erkannt werden. • Aktionen mit PersDat können in großem Umfang auf nicht absehbare Zeit nicht zugeordnet werden. • Es sind in großem Umfang aggregierte und hochsensitive Daten betroffen.
Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung der persönlichen Unversehrtheit aufgrund der nicht garantierten Zuordenbarkeit von Urheberschaft oder Empfang von Daten bzw. generell von Aktionen im IT-Bereich oder von falschen / gefälschten Daten oder manipulierten IT-Anwendungen ist unabwendbar. • Es kommt zu massiven Schäden an Leib und Leben.
Beeinträchtigung der Aufgabenerfüllung	• Ein Integritätsverlust hat katastrophale Auswirkungen auf die Aufgabenerfüllung. • Die Beeinträchtigung der Aufgabenerfüllung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. • Verfälschte Daten oder manipulierte Funktionen würden über einen sehr langen Zeitraum nicht erkannt werden. • Verfälschte Daten wären nicht rekonstruierbar. • Die Behebung von Softwarefehlern ist nicht möglich. • Die Zuordenbarkeit von Urheberschaft oder Empfang von Daten bzw. generell von Aktionen im IT-Bereich ist der wichtigste Bestandteil der Aufgabe. • Es existieren keine Ausweichlösungen.
Negative Innen- / Außenwirkung	• Eine mindestens landesweite Ansehens- und Vertrauensbeeinträchtigung ist die Folge. • Die gesamte Bw ist betroffen.
Finanzielle Auswirkungen	• Der finanzielle Schaden liegt über 1.000.000.- €[160].

Abb. 20 Schutzbedarfskategorie „sehr hoch“ für den Grundwert Integrität

[160] Gemäß BSI-Standard (Anlage 11.15 (Nr. 46)) und Studie IABG zur Einführung des Grundschutzes in die Bundeswehr von 2010

11.4.3.3 Verfügbarkeit

29. Für die Schutzbedarfskategorien beim Grundwert Verfügbarkeit gibt es keine gesetzlichen Vorgaben. Gesetzlich oder sonstige Anforderungen an die Verfügbarkeit von Funktionalitäten, Diensten oder Dienstleistungen können jedoch im Einzelfall bestehen. Sie können unmittelbare Auswirkungen auf die Verfügbarkeit der IT haben, die die Bereitstellung dieser Funktionalitäten, Diensten oder Dienstleistungen sicherstellt oder steuert.

Bei der Verfügbarkeit geht es um die IT-gestützte zeitgerechte Bereitstellung von notwendigen Informationen, Funktionalitäten oder Diensten für die Aufgabenerfüllung.

30. Eine **hohe Verfügbarkeit** bedeutet, dass die Erfüllung der Aufgabe nur mit erheblichem Mehraufwand für einen tolerierbaren Zeitraum ohne die Informationen / die IT gewährleistet werden kann.

31. Eine **sehr hohe Verfügbarkeit** bedeutet, dass ohne die Informationen / die IT die Aufgabenerfüllung unmöglich ist.

32. Bei der Bewertung des Schutzbedarfes für die Verfügbarkeit ist zu beachten, dass es durch Betrieb mehrerer Anwendungen auf einem System notwendig werden kann, den Schutzbedarf für diesen Grundwert – bzgl. der genutzten IT-Plattform, auf der diese Anwendungen betrieben werden – höher als den Schutzbedarf der Einzelanwendungen zu bewerten (Kumulationseffekt).

33. Zusätzlich sind bei diesem Grundwert gesetzliche Aufbewahrungs- und Löschfristen (z. B. Bundesdatenschutzgesetz, siehe Bezug Anlage 11.15 (lfdNr. 2)) zu beachten.

34. In der Abb. 21, Abb. 22 und Abb. 23 sind Hilfestellungen aufgeführt.

35. Schutzbedarf **„normal“**

Schutzbedarfs-kategorie / Schadens szenarien	Normal (Verfügbarkeit)
Beeinträchtigung des Rechts auf informationelle Selbstbestimmung	• Eine Beeinträchtigung des Rechts auf informationelle Selbstbestimmung ist im Zusammenhang mit den betroffenen Daten nicht möglich. • Der Verlust von PersDat würde erkannt werden und die Daten könnten wiederhergestellt werden oder der Verlust würde keine bedeutsame Beeinträchtigung des informationellen Rechts auf Selbstbestimmung nach sich ziehen. • Es entstehen keine oder nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.
Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung der persönlichen Unversehrtheit aufgrund der Nichtverfügbarkeit von Daten oder Funktionen erscheint kaum möglich, bzw. wäre hinsichtlich Umfang und Schwere auf ein, bezogen auf die Einsatzart erträgliches, Maß begrenzt.
Beeinträchtigung der Aufgabenerfüllung	• Die Nichtverfügbarkeit von Daten oder Funktionen hat keine oder unbedeutende Auswirkungen auf die Aufgabenerfüllung. • Die Beeinträchtigung der Aufgabenerfüllung würde von den Betroffenen als tolerabel eingeschätzt werden. • Datenverlust oder der Ausfall von Funktionen würden schnell erkannt werden. • Daten könnten zeitnah rekonstruiert, Funktionalitäten wiederhergestellt werden. • Ausfallzeiten von mehr als 1 Stunde können hingenommen werden. • Es existieren effiziente Ausweichmöglichkeiten.
Negative Innen- / Außenwirkung	• Ein möglicher Ansehensverlust ist nicht nennenswert oder lediglich in der betroffenen Dienststelle / in deren engerem Bereich zu erwarten.
Finanzielle Auswirkungen	• Der finanzielle Schaden ist tolerabel (<= 100.000.- €)[161].

Abb. 21 Schutzbedarfskategorie „normal“ für den Grundwert Verfügbarkeit

[161] Gemäß BSI-Standard (Anlage 11.15 (Nr. 46)) und Studie IABG zur Einführung des Grundschutzes in die Bundeswehr von 2010

36. Schutzbedarf **„hoch“**

Schutzbedarfs-kategorie / Schadens szenarien	Hoch (Verfügbarkeit)
Beeinträchtigung des Rechts auf informationelle Selbstbestimmung	• Ein Verlust der Verfügbarkeit zieht eine erhebliche Beeinträchtigung des Rechts auf informationelle Selbstbestimmung nach sich. Eine Vielzahl an Personen hat mit erheblichen Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse zu rechnen. • Der Verlust von PersDat würde über einen längeren Zeitraum nicht erkannt werden. Die Daten sind kaum rekonstruierbar. • Es sind aggregierte oder hochsensitive Daten betroffen.
Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung der persönlichen Unversehrtheit aufgrund der Nichtverfügbarkeit von Daten oder Funktionen ist wahrscheinlich. Die Beeinträchtigung ist schwerwiegend.
Beeinträchtigung der Aufgabenerfüllung	• Die Nichtverfügbarkeit von Daten oder Funktionen hat erhebliche Auswirkungen auf die Aufgabenerfüllung. • Die Beeinträchtigung der Aufgabenerfüllung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt werden. • Datenverlust oder der Ausfall von Funktionen würden nicht rechtzeitig erkannt werden. • Eine komplette Rekonstruktion verloren gegangener Daten ist nicht oder nur stark verzögert möglich. • Die Wiederherstellung nicht verfügbarer Funktionen ist sehr aufwändig und nur stark verzögert möglich. • Ausfallzeiten zwischen 5 Minuten und einer Stunde können hingenommen werden. • Es existieren Ausweichmöglichkeiten, welche aber nur einen deutlich eingeschränkten Funktionsumfang bieten und nur bei erheblichem Aufwand arbeitsfähig wären.
Negative Innen- / Außenwirkung	• Eine breite und deutliche Ansehens- und Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	• Der Schaden bewirkt beachtliche finanzielle Verluste (zwischen 100.000.- € und 1.000.000,- €)[162].

Abb. 22 Schutzbedarfskategorie „hoch“ für den Grundwert Verfügbarkeit

[162] Gemäß BSI-Standard (Anlage 11.15 (Nr. 46)) und Studie IABG zur Einführung des Grundschutzes in die Bundeswehr von 2010

37. Schutzbedarf **„sehr hoch“**

Schutzbedarfs-kategorie / Schadens szenarien	Sehr hoch (Verfügbarkeit)
Verstoß gegen Gesetze / Vorschriften / Verträge	• Verstöße gegen Vorschriften oder gegen Gesetze. • Vertragsverletzungen mit ruinösen Konventionalstrafen. • Negative zivil-, straf-, verwaltungs-, oder disziplinarrechtliche Folgen für die Verantwortlichen.
Beeinträchtigung des Rechts auf informationelle Selbstbestimmung	• Ein Verlust der Verfügbarkeit führt zu einer erheblichen Beeinträchtigung des Rechts auf informationelle Selbstbestimmung vieler Personen. Er bzw. sie hat mit ruinösen Auswirkungen auf seine bzw. ihre gesellschaftliche Stellung oder seine bzw. ihre wirtschaftlichen Verhältnisse zu rechnen. • Der Verlust von PersDat würde über einen sehr langen Zeitraum nicht erkannt werden. Die Daten sind nicht rekonstruierbar. • Es sind aggregierte und hochsensitive Daten betroffen. Es sind in großem Umfang aggregierte und hochsensitive Daten betroffen.
Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung der persönlichen Unversehrtheit aufgrund der Nichtverfügbarkeit von Daten oder Funktionen ist unabwendbar. • Es kommt zu massiven Schäden an Leib und Leben.
Beeinträchtigung der Aufgabenerfüllung	• Die Nichtverfügbarkeit von Daten oder Funktionen hat katastrophale Auswirkungen auf die Aufgabenerfüllung. • Die Beeinträchtigung der Aufgabenerfüllung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. • Datenverlust oder der Ausfall von Funktionen werden lange Zeit nicht erkannt. • Eine Rekonstruktion verloren gegangener Daten ist nicht möglich. • Die Wiederherstellung nicht verfügbarer Funktionen ist nicht möglich. • Es können maximal Ausfallzeiten bis zu 5 Minuten hingenommen werden. • Es existieren keine Ausweichmöglichkeiten.
Negative Innen- / Außenwirkung	• Eine mindestens landesweite Ansehens- und Vertrauensbeeinträchtigung ist die Folge. • Die gesamte Bw ist betroffen.
Finanzielle Auswirkungen	• Der finanzielle Schaden liegt über 1.000.000.- €[163].

Abb. 23 Schutzbedarfskategorie „sehr hoch“ für den Grundwert Verfügbarkeit

[163] Gemäß BSI-Standard (Anlage 11.15 (Nr. 46)) und Studie IABG zur Einführung des Grundschutzes in die Bundeswehr von 2010

11.4.4 Beispiel für eine Informationsstruktur

38. Für ein geplantes Projekt wurden mit den Bedarfsträgern die notwendigen Anwendungen für die Fachaufgabe und die Informationen, die in den Anwendungen verarbeitet werden sollen, erfasst. Danach wurde festgestellt, welche Anforderungen zu den Informationen bezüglich der Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität bestehen. Daraufhin wurde für alle Informationen die Relevanz bezüglich der Gewährleistungsziele Nichtverkettung, Transparenz und Intervenierbarkeit zusammen mit dem bzw. der zuständigen ADSB festgelegt. Abschließend wurde der Schutzbedarf gemäß dem Maximumprinzip ermittelt.

39. Für das fiktive Projekt sieht die Informationsstruktur wie folgt aus (siehe Abb. 24):

Anwendung	**Informationen**	**Einstufung**	**Vertraulichkeit**	**Verfügbarkeit**	**Integrität**	**Relevanz Nichtverkettung**	**Relevanz Transparenz**	**Relevanz Intervenierbarkeit**
Wareneingang	Rohdaten der Lagerbestände	OFFEN	normal	normal	normal	nein	nein	nein
Materialnachweis	Bestände	OFFEN	normal	normal	hoch	nein	nein	nein
Materialnachweis	Kundendaten	OFFEN / PersDat SB 2	hoch	normal	normal	ja	ja	ja
Materialnachweis	Verträge	SSI / PersDat SB 2	hoch	normal	hoch	ja	ja	ja
IT-Betrieb	Nutzerdaten	OFFEN / PersDat SB 1	normal	normal	normal	nein	ja	ja
IT-Betrieb	Konfigurations-daten	OFFEN	normal	normal	normal	nein	nein	nein
IT-Betrieb	Protokoll-informationen (ohne PersDat)	OFFEN	normal	normal	normal	ja	ja	nein
Schutzbedarf / Ergebnis			**hoch**	**normal**	**hoch**	**ja**	**ja**	**ja**

Abb. 24 Beispiel für eine Informationsstruktur

11.5 Wegweiser für die Anwendungsbereiche

11.5.1 Anwendungsbereich Wehrtechnische Forschung & Technologie sowie sonstige Forschungsvorhaben, Erprobungen, Truppenversuche und Wehrtechnische Aufträge (F)

Phase	Tätigkeit	Bemerkungen
Studiendurch-führung	<u>Planen, Bearbeiten und Fertigstellen der InfoSichh</u> InfoSichhDok: Erstellung	
	InfoSichhKFW mit der	FF Leitende(r) des Vorhabens
	Informationsstruktur (abschließend) und	FF Leitende(r) des Vorhabens
	Ermittlung und Deckung des Schutzbedarfs sowie	FF Leitende(r) des Vorhabens
	Zuordnung von InfoSichh-Anforderungen zu den Schutzbedarfskategorien (bei Bedarf) und	FF Leitende(r) des Vorhabens
	Auswahl, Anpassung und Konkretisierung von InfoSichh-Maßnahmen (abschließend) sowie	FF Leitende(r) des Vorhabens
	Risikoanalyse – Dokumentation des verbliebenen Risikos (bei Bedarf) und ggf.	FF Leitende(r) des Vorhabens
	Ermittlung zusätzlicher bzw. alternativer InfoSichh-Maßnahmen (abschließend).	FF Leitende(r) des Vorhabens
	Mitzeichnung von DEUmilSAA einholen.	FF Leitende(r) des Vorhabens
	Mitteilung an DEUmilSAA bei Abweichung von den Empfehlungen der Mitzeichnung.	FF Leitende(r) des Vorhabens
	<u>Herstellung der InfoSichh</u> **Umsetzung** der InfoSichh-Maßnahmen.	FF Leitende(r) des Vorhabens
	InfoSichh-Verfahren: **Akkreditierung** (bei Bedarf),	FF DEUmilSAA
	Freigabe zur Nutzung (verfahrensbezogene oder vorläufige Freigabe).	FF Leitende(r) des Vorhabens

Abb. 25 Wegweiser F&T (F)

11.5.2 Anwendungsbereich Wissenschaftliche Unterstützung nicht-technisch (W)

Phase	Tätigkeit	Bemerkungen
Experiment-durchführung	<u>Planen, Bearbeiten und Fertigstellen der InfoSichh</u> InfoSichhDok: Erstellung **InfoSichhKFW** mit der	 FF Leitende(r) des Vorhabens
	Informationsstruktur (abschließend) und	FF Leitende(r) des Vorhabens
	Ermittlung und Deckung des Schutzbedarfs sowie	FF Leitende(r) des Vorhabens
	Zuordnung von InfoSichh-Anforderungen zu den Schutzbedarfskategorien (bei Bedarf) und	FF Leitende(r) des Vorhabens
	Auswahl, Anpassung und Konkretisierung von InfoSichh-Maßnahmen (abschließend) sowie	FF Leitende(r) des Vorhabens
	Risikoanalyse – Dokumentation des verbliebenen Risikos (bei Bedarf) und ggf.	FF Leitende(r) des Vorhabens
	Ermittlung zusätzlicher bzw. alternativer InfoSichh-Maßnahmen (abschließend).	FF Leitende(r) des Vorhabens
	Mitzeichnung von DEUmilSAA einholen.	FF Leitende(r) des Vorhabens
	Mitteilung an DEUmilSAA bei Abweichung von den Empfehlungen der Mitzeichnung.	FF Leitende(r) des Vorhabens
	<u>Herstellung der InfoSichh</u> **Umsetzung** der InfoSichh-Maßnahmen.	 FF Leitende(r) des Vorhabens
	InfoSichh-Verfahren: **Akkreditierung** (bei Bedarf),	 FF DEUmilSAA
	Freigabe zur Nutzung (verfahrensbezogene oder vorläufige Freigabe).	FF Leitende(r) des Vorhabens

Abb. 26 Wegweiser Wissenschaftliche Unterstützung nicht-technisch (W)

11.5.3 Anwendungsbereich Projekte nach Customer Product Management (P)

CPM-Phase	Tätigkeit	Bemerkungen
Analysephase Teil 1 (Ergebnis: FFF)	<u>Vorgaben für das Projektelement InfoSichh</u> Erstellung des Abschnittes „InfoSichh“ in der FFF mit Festlegung der **Informationsstruktur** (abschließend) und der	FF Ltr IPT im Panungsamt der Bundeswehr (PlgABw) bzw. bei Projekten in der Verantwortung der Abteilung BMVg CIT im KdoCIR
	Schutzbedarfsfeststellung (abschließend).	FF Ltr IPT im PlgABw bzw. bei Projekten in der Verantwortung der Abteilung BMVg CIT im KdoCIR
Analysephase Teil 2 (Ergebnis: Lösungsvor-schläge und Auswahlent-scheidung)	<u>Personal</u> **Bestellung eines ISBProj** (siehe Abschnitt 5.7)	FF Ltr IPT im BAAINBw
	<u>Planen des Projektelementes InfoSichh</u> InfoSichhDok: Erstellung **InfoSichhKProj** (gemäß Anlage 11.7.1) mit der	FF Ltr IPT / ISBProj
	Zuordnung von InfoSichh-Anforderungen zu den Schutzbedarfskategorien (bei Bedarf)	FF Ltr IPT / ISBProj
	Ermittlung und Deckung des Schutzbedarfs (abschließend) sowie	FF Ltr IPT / ISBProj
	Auswahl, Anpassung und Konkretisierung von InfoSichh-Maßnahmen sowie	FF Ltr IPT / ISBProj
	Risikoanalyse – Dokumentation des verbliebenen Risikos (bei Bedarf) und	FF Ltr IPT / ISBProj
	Ermittlung zusätzlicher bzw. alternativer InfoSichh-Maßnahmen.	FF Ltr IPT / ISBProj
	InfoSichh-Verfahren: **Zulassung von InfoSichh-Produkten** (bei Bedarf).	FF BSI
	Zertifizierung von InfoSichh-Produkten (bei Bedarf).	FF BSI

CPM-Phase	Tätigkeit	Bemerkungen
	Anerkennung von Zulassungen, die durch NATO- oder EU-Mitgliedstaaten ausgesprochen wurden (bei Bedarf)**.**	FF CISOBw
	Mitzeichnung von DEUmilSAA einholen.	FF Ltr IPT
	Mitteilung an DEUmilSAA bei Abweichung von den Empfehlungen der Mitzeichnung.	FF Ltr IPT
Realisierungs-phase (Ergebnis: GeNu)	<u>Bearbeiten und Fertigstellen des Projektelementes InfoSichh</u> InfoSichhDok: Fortschreibung **Projektbezogenes InfoSichh-Konzept (InfoSichhKProj** (gemäß Anlage 11.7.1) mit **Auswahl, Anpassung und Konkretisierung von InfoSichh-Maßnahmen** (abschließend) sowie **Risikoanalyse – Dokumentation des verbliebenen Risikos** (abschließend bei Bedarf) und **Ermittlung zusätzlicher bzw. alternativer InfoSichh-Maßnahmen** (abschließend).	 FF ProjLtr / ISBProj FF ProjLtr / ISBProj FF ProjLtr / ISBProj FF ProjLtr / ISBProj
	Mitzeichnung von DEUmilSAA einholen. **Mitteilung** an DEUmilSAA bei Abweichung von den Empfehlungen der Mitzeichnung.	FF ProjLtr FF ProjLtr
	<u>Herstellung der InfoSichh</u> **Umsetzung** der technischen InfoSichh-Maßnahmen. InfoSichh-Verfahren: **Akkreditierung** (bei Bedarf), **Freigabe zur Nutzung** (verfahrensbezogene oder vorläufige Freigabe).	 FF ProjLtr FF DEUmilSAA FF ProjLtr
Nutzungsphase	<u>Produktänderungen / -verbesserungen</u> InfoSichhDok: Fortschreibung **InfoSichhKProj** (gemäß Anlage 11.7.1)	 FF ProjLtr / ISBProj
	Mitzeichnung von DEUmilSAA einholen. **Mitteilung** an DEUmilSAA bei Abweichung von den Empfehlungen der Mitzeichnung.	FF ProjLtr FF ProjLtr

CPM-Phase	Tätigkeit	Bemerkungen
	InfoSichh-Verfahren: **Akkreditierung** (Re-Akkreditierung) (bei Bedarf),	FF DEUmilSAA
	Freigabe in der Nutzung bzw. Aufhebung oder zeitliche Befristung.	FF ProjLtr
	Gewährleistung der InfoSichh **Gewährleistung / Wiederherstellung** der technischen InfoSichh inkl. Obsolenzenzmanagements.	FF ProjLtr
	Dienststellen- und einsatzbezogene Aufgaben der InfoSichh in der Nutzungsphase sind in den Anwendungsbereichen „Dienststelle“ (siehe Anlage 11.5.6, Abb. 30) und „Einsatzkontingente und Einsatzstandorte“ (siehe Anlage 11.5.7, Abb. 31) beschrieben.	FF DStLtr / ISBDSt KtgtFhr / Kdr EinsStO / ISB i.E.
	Bei Übernahme von IT anderer Nationen, ist deren InfoSichh-Dokumentation zu prüfen (siehe Nr. 434) und durch DEUmilSAA bewerten zu lassen.	FF ProjLtr
Beendigung der Nutzung	Aussonderung Durchführung der Maßnahmen gemäß InfoSichhKProj (siehe Anlage 11.7.1).	FF ProjLtr

Abb. 27 Wegweiser Projekte nach CPM (P)

11.5.4 Anwendungsbereich Infrastruktur- / Baumaßnahmen bzw. sonstige Vorhaben mit IT-Anteil (V)

Phasen	Tätigkeit	Bemerkungen
	Für IT, die aus **Infrastruktur- / Baumaßnahmen** finanziert wird oder **sonstige Vorhaben, in denen IT-Anteile beschafft bzw. eingerüstet** werden (z. B. Gebäudeverkabelung, Gebäudeautomation), ist der Abschnitt 4.4 sinngemäß anzuwenden, ein **InfoSichhK Infra** zu erstellen und dieses an die nutzende DSt zu übergeben.	FF Verantwortliche(r) für die Infra-Maßnahme
	Erstellung und Begründung einer **Infrastruktur** (siehe Abschnitt 6.3.2)	FF Bedarfsträger
	Notwendige Abweichungen zu Struktur und Inhalt des InfoSichhK Infra mit DEUmilSAA abstimmen	FF Verantwortliche(r) für die Infra-Maßnahme
	Bei IT, welche aus Infrastrukturmitteln beschafft wird, sind Abweichungen und Regelungen mit CISO Infrastruktur abzustimmen. Abstimmung mit CISOBw und DEUmilSAA	FF Verantwortliche(r) für die Infra-Maßnahme FF CISO Infrastruktur

Abb. 28 Wegweiser Infrastruktur- / Baumaßnahmen bzw. sonstige Vorhaben mit IT-Anteil (V)

11.5.5 Anwendungsbereich IT-Betrieb und Aufgabenübernahme durch Dritte (O)

Phasen	Tätigkeit	Bemerkungen
Vor Beginn des Vertragsverhältnisses / vor der Nutzung	Grundlegende Beachtung von Abschnitt 4.6.1 „Übernahme von IT-Betriebsverantwortung“ und Abschnitt 4.6.2 „Übernahme von Aufgabenbereichen“ bei der Vertragsgestaltung.	FF ProjLtr / ISBProj
	Planen, Bearbeiten und Fertigstellen des Projektelementes InfoSichh	
	InfoSichhDok:	
	Erstellung **InfoSichhKProj** (in Anlehnung an Anlage 11.7.1) mit	FF ProjLtr / ISBProj
	Informationsstruktur (abschließend) und der	FF ProjLtr / ISBProj
	Schutzbedarfsfeststellung (abschließend) sowie	FF ProjLtr / ISBProj
	Zuordnung von InfoSichh-Anforderungen zu den Schutzbedarfskategorien (bei Bedarf) sowie	FF ProjLtr / ISBProj
	Ermittlung und Deckung des Schutzbedarfs (abschließend) und	FF ProjLtr / ISBProj
	Auswahl, Anpassung und Konkretisierung von InfoSichh-Maßnahmen (abschließend) sowie	FF ProjLtr / ISBProj
	Risikoanalyse – Dokumentation des verbliebenen Risikos (bei Bedarf) und	FF ProjLtr / ISBProj
	Ermittlung zusätzlicher bzw. alternativer InfoSichh-Maßnahmen.	FF ProjLtr / ISBProj
	Mitzeichnung von DEUmilSAA einholen.	FF ProjLtr
	Mitteilung an DEUmilSAA bei Abweichung von den Empfehlungen der Mitzeichnung.	FF ProjLtr
	InfoSichh-Verfahren:	
	Zulassung von InfoSichh-Produkten (bei Bedarf),	FF BSI / CISOBw
	Zertifizierung von InfoSichh-Produkten (bei Bedarf),	FF BSI
	Anerkennung von Zulassungen, die durch NATO- oder EU-Mitgliedstaaten ausgesprochen wurden (bei Bedarf).	FF CISOBw

Phasen	Tätigkeit	Bemerkungen
	<u>Herstellung der InfoSichh</u> **Umsetzung** der technischen InfoSichh-Maßnahmen sowie **Prüfung** deren Wirksamkeit. **Akkreditierung** (bei Bedarf), **Freigabe zur Nutzung** (verfahrensbezogene oder vorläufige Freigabe).	 FF ProjLtr / AN FF DEUmilSAA FF ProjLtr
Während des Vertragsverhältnisses / der Nutzung	siehe Anwendungsbereich „Dienststelle“ in Anlage 11.5.6, Abb. 30	FF ProjLtr / ISBProj / ISBAN

Abb. 29 Wegweiser IT-Betrieb und Aufgabenübernahme durch Dritte (O)

11.5.6 Anwendungsbereich Sofortinitiativen für den Einsatz (Phasendokument „Fähigkeitslücke und Funktionale Forderung“ (S)) (S)

Phasen	Tätigkeit	Bemerkungen
Vor Beginn der Nutzung	Bearbeiten der InfoSichh InfoSichhDok: Festlegung der **Informationsstruktur** (abschließend) und	FF Ltr IPT / bei PersDat unter Beteiligung des bzw. der zuständigen ADSB
	Ermittlung und Deckung des Schutzbedarfs sowie	FF Ltr IPT
	Zuordnung von InfoSichh-Anforderungen zu den Schutzbedarfskategorien (bei Bedarf) und	FF Ltr IPT
	Auswahl, Anpassung und Konkretisierung von InfoSichh-Maßnahmen.	FF Ltr IPT
	Mitzeichnung von DEUmilSAA einholen.	FF Ltr IPT
	Mitteilung an DEUmilSAA bei Abweichung von den Empfehlungen der Mitzeichnung.	FF Ltr IPT
Nutzungsphase	Fertigstellen der InfoSichh InfoSichhDok: Erstellung **Projektbezogenes InfoSichh-Konzept (IT-SichKProj)** (gemäß Anlage 11.7.1) mit	FF Ltr IPT
	Ermittlung und Deckung des Schutzbedarfs (abschließend) und	FF Ltr IPT
	Auswahl, Anpassung und Konkretisierung von InfoSichh-Maßnahmen (abschließend) sowie	FF Lt IPT
	Risikoanalyse – Dokumentation des verbliebenen Risikos (bei Bedarf) und	FF Ltr IPT
	Ermittlung zusätzlicher bzw. alternativer InfoSichh-Maßnahmen (abschließend).	FF Lt IPT
	Mitzeichnung von DEUmilSAA einholen.	FF Ltr IPT
	Mitteilung an DEUmilSAA bei Abweichung von den Empfehlungen der Mitzeichnung.	FF Ltr IPT

Phasen	Tätigkeit	Bemerkungen
	Herstellung der InfoSichh **Umsetzung** der technischen InfoSichh-Maßnahmen.	FF Ltr IPT
	InfoSichh-Verfahren: **Zulassung von InfoSichh-Produkten** (bei Bedarf),	FF BSI / CISOBw
	Zertifizierung von InfoSichh-Produkten (bei Bedarf),	FF BSI
	Anerkennung von Zulassungen, die durch NATO- oder EU-Mitgliedstaaten ausgesprochen wurden (bei Bedarf),	FF CISOBw
	Akkreditierung (bei Bedarf),	FF DEUmilSAA
	Freigabe zur Nutzung (verfahrensbezogene oder vorläufige Freigabe).	FF Ltr IPT
	Die anderen Tätigkeiten während der Nutzung ergeben sich aus dem Anwendungsbereich „Projekte nach CPM“ (siehe Anlage 11.5.3, Abb. 27).	

Abb. 30 Wegweiser Sofortinitiativen für den Einsatz (FFF(S)) (S)

11.5.7 Anwendungsbereich Dienststellen (D)

Phasen gemäß CPM	Tätigkeit	Bemerkungen
Nutzungsphase	Personal **Bestellung eines ISBDSt inkl. Vertreter** (siehe Abschnitt 5.7). **Belehrungen und deren Nachweis**	 FF DStLtr FF ISBDSt
	Nutzung InfoSichhDok: Erstellung / Fortschreibung **InfoSichhKDSt** (gemäß Anlage 11.7.3), dabei ggf. Festlegung der **Informationsstruktur** und	 In Abstimmung mit zuständigem Regionalzentrum und ggf. CISO Infrastruktur FF DStLtr / ISBDSt unter Beteiligung ADSB FF DStLtr / ISBDSt unter Beteiligung ADSB
	Auswahl, Anpassung und Konkretisierung von InfoSichh-Maßnahmen sowie **Risikoanalyse – Dokumentation des verbliebenen Risikos** (bei Bedarf) und **Ermittlung zusätzlicher bzw. alternativer InfoSichh-Maßnahmen** (bei Bedarf). Führen **Dienststellen- / einsatzbezogene InfoSichhDok**	FF DStLtr / ISBDSt unter Beteiligung ADSB FF DStLtr / ISBDSt unter Beteiligung ADSB FF DStLtr / ISBDSt unter Beteiligung ADSB FF ISBDSt unter Beteiligung ADSB

Phasen gemäß CPM	Tätigkeit	Bemerkungen
	Herstellung der InfoSichh **Umsetzung** der personellen, organisatorischen und infrastrukturellen InfoSichh-Maßnahmen aus den InfoSichhKProj. InfoSichh-Verfahren: **Akkreditierung** (Re-Akkreditierung) (bei Bedarf),	FF DStLtr / ISBDSt FF DEUmilSAA
	Freigabe zur Nutzung (operationelle oder vorläufige Freigabe). **Umsetzung** der dienststellenbezogenen Anteile der IT-Notfallvorsorge.	FF DStLtr FF DStLtr / ISBDSt
	Gewährleistung der InfoSichh **Wiederherstellen** der personellen, organisatorischen und infrastrukturellen InfoSichh-Maßnahmen in der Dienststelle nach Verlust / Beeinträchtigung der InfoSichh.	FF DStLtr
	Überwachung der InfoSichh **InfoSichhIn** mit Erstellung der **Dokumentation / Informationssicherheitsinspektionsbericht (InfoSichhInB)**	FF CISOBw, RegZ
	InfoSichhKtr **InfoSichhPrfg** **InfoSichhVork**	ISBOrgBer, DStLtr / ISBDSt
	Nutzersensibilisierung **Sensibilisierung**	FF DStLtr / ISBDSt
Bei IT-Betrieb durch die Dienststelle:		
	Herstellung der InfoSichh **Bestellung** ISBBtrb **Umsetzung** der für den IT-Betrieb relevanten technischen InfoSichh-Maßnahmen aus den InfoSichhKProj für in der DSt betriebene IT.	FF DStLtr FF DStLtr / ISBBtrb in Zusammenarbeit mit ISBDSt und ISBProj

Phasen gemäß CPM	Tätigkeit	Bemerkungen
	Gewährleistung der InfoSichh Gewährleistung der betrieblichen InfoSichh. Durchführung des Sicherheitsauditings. Durchführung von Notfallübungen.	 FF DStLtr / ISBDSt in Zusammenarbeit mit ISBBtrb

Abb. 31 Wegweiser Dienststellen (D)

11.5.8 Anwendungsbereich Einsatzkontingente und Einsatzstandorte (E)

Phasen gemäß CPM	**Tätigkeit**	**Bemerkungen**
Nutzungsphase	<u>Personal</u> **Bestellung eines ISB i.E.** (siehe Abschnitt 5.7). Ggf. Bestellung eines/einer Leiter(in) NOC i.E. (siehe Abschnitte 464, 465) **Belehrungen und deren Nachweis**	 FF KtgtFhr / Kdr EinsStO FF KtgtFhr / Kdr EinsStO FF ISB i.E.
	<u>Nutzung</u> InfoSichhDok: Erstellung / Fortschreibung **InfoSichhKDSt** (gemäß Anlage 11.7.3), dabei ggf. Festlegung der **Informationsstruktur** und **Auswahl, Anpassung und Konkretisierung von InfoSichh-Maßnahmen** sowie **Risikoanalyse – Dokumentation des verbliebenen Risikos** (bei Bedarf) und	 Mitzeichnung ISB vorgesetzte Dienststelle oder zuständiger ISB-OrgBer / ISBEinsatz FF KtgtFhr / Kdr EinsStO / ISB i.E. FF KtgtFhr / Kdr EinsStO / ISB i.E. FF KtgtFhr / Kdr EinsStO / ISB i.E. FF KtgtFhr / Kdr EinsStO / ISB i.E.
	Ermittlung zusätzlicher bzw. alternativer InfoSichh-Maßnahmen (bei Bedarf). Führen **Dienststellen- / einsatzbezogene InfoSichhDok**	FF KtgtFhr / Kdr EinsStO / ISB i.E. FF ISB i.E.
	<u>Herstellung der InfoSichh</u> **Umsetzung** der personellen, organisatorischen, infrastrukturellen und die für den IT-Betrieb relevanten technischen InfoSichh-Maßnahmen aus den InfoSichhKProj. InfoSichh-Verfahren: **Freigabe zur Nutzung** (operationelle oder vorläufige Freigabe).	 FF KtgtFhr / Kdr EinsStO / ISB i.E. FF KtgtFhr / Kdr EinsStO
	Umsetzung der dienststellenbezogenen Anteile der IT-Notfallvorsorge.	FF KtgtFhr / Kdr EinsStO / ISB i.E.

Phasen gemäß CPM	Tätigkeit	Bemerkungen
	Gewährleistung der InfoSichh **Wiederherstellen** der personellen, organisatorischen, infrastrukturellen und der für den IT-Betrieb relevanten technischen InfoSichh-Maßnahmen im EinsKtgt nach Verlust / Beeinträchtigung der InfoSichh. Durchführung von **Notfallübungen**.	FF KtgtFhr / Kdr EinsStO / ISB i.E.
	Überwachung der InfoSichh **InfoSichhIn** mit Erstellung der **Dokumentation / InfoSichhInB** **InfoSichhKtr** **InfoSichhPrfg** **InfoSichhVork**	FF CISOBw ISBOrgBer, ISBEinsatz, KtgtFhr / Kdr EinsStO / ISB i.E.
	Nutzersensibilisierung **Sensibilisierung**	FF KtgtFhr / Kdr EinsStO / ISB i.E.

Abb. 32 Wegweiser Einsatzkontingente und Einsatzstandorte (E)

11.5.9 Anwendungsbereich Übungen (Ü)

Phasen	Tätigkeit	Bemerkungen
Vor Beginn der Übung	<u>Personal</u> **Bestellung eines ISBÜb** (siehe Abschnitt 5.7)	FF nationales übungskoordinierendes Kommando
	<u>Bearbeiten der InfoSichh</u> InfoSichhDok: Erstellung **Informationssicherheitsbefehl** mit **Informationsstruktur** (abschließend) und **Ermittlung und Deckung des Schutzbedarfs**.	FF nationales übungskoordinierendes Kommando / ISBÜb FF nationales übungskoordinierendes Kommando / ISBÜb FF nationales übungskoordinierendes Kommando / ISBÜb
	Mitzeichnung von DEUmilSAA (ggf. ISBOrgBer) einholen.	FF nationales übungskoordinierendes Kommando
	<u>Herstellung der InfoSichh</u> **Umsetzung** der infrastrukturellen und organisatorischen Absicherungsmaßnahmen am Übungsort. InfoSichh-Verfahren: **Akkreditierung** (bei Bedarf).	FF nationales übungskoordinierendes Kommando / ISBÜb FF DEUmilSAA

Abb. 33 Wegweiser Übungen (Ü)

11.6 Grundsätze zu Protokollierung und Auditing

11.6.1 Allgemeines

1. Unter **Protokollierung** wird die während des IT-Betriebs stattfindende programmgestützte Aufzeichnung von Protokolldaten verstanden. Protokolldaten umfassen definierte Ereignisse und Aktionen sowie deren Zeitpunkte, Reihenfolge einschl. des bzw. der auslösenden / agierenden IT-Anwenders bzw. IT-Anwenderin (Nutzeridentifikation).

2. Unter **Auditing** wird die regelmäßige oder ereignisbezogene IT-gestützte Auswertung der aufgezeichneten Protokolldaten und damit das Erkennen von system-, sicherheits- und datenschutzrelevanten Ereignissen verstanden.

3. Die nachfolgend aufgeführten Grundsätze berücksichtigen die „Rahmendienstvereinbarung zur Protokollierung informationstechnischer Systeme“ (siehe Bezug Anlage 11.15 (lfdNr. 40)). Zur Sicherstellung der in § 4 der Rahmendienstvereinbarung aufgeführten Verhaltensgrundsätze können gemäß § 6 Absatz (1) dieser Vereinbarung folgende Daten protokolliert werden:

- bei Nutzung informationstechnischer Systeme:
  - Art des Vorgangs und der durchgeführten Veränderung des Datenbestandes,
  - Datum / Uhrzeit (ggf. Zeitpunkt der An- bzw. Abmeldung, der Änderung des Datenbestandes),
  - ggf. Rollen und Berechtigungen,
- des Weiteren bei Verbindungen:
  - Adressen von Absender und Empfänger,
  - Protokoll, Port,
  - Anmeldename und
  - übertragene Datenmenge bzw. Bezeichnung der durchgeführten Aktion.

4. Die Protokolle werden gemäß § 6 Absatz (2) der Rahmendienstvereinbarung (siehe Bezug Anlage 11.15 (lfdNr. 40)) ausschließlich zu Zwecken der

- Überwachung der Rechtmäßigkeit der Verarbeitung und Nutzung von PersDat,
- Prüfung und Sicherstellung der datenschutzrechtlichen Anforderungen,
- Analyse der Berechtigungsmodelle der Dienststellen,
- Analyse und Korrektur technischer Fehler,
- Gewährleistung der Systemsicherheit,
- Optimierung des Netzes,
- statistischen Feststellung des Gesamtnutzungsvolumens,
- Stichprobenkontrollen gemäß § 6 Absatz 3 der Rahmendienstvereinbarung,
- Verhinderung und Aufdeckung von Straftaten sowie sicherheitsgefährdendem Verhalten und
- Auswertung gemäß § 7 der Rahmendienstvereinbarung (Missbrauchskontrolle)

verwendet.

5. Protokolldaten dürfen nicht zur Leistungs- und Verhaltenskontrolle der IT-Anwender herangezogen werden.

6. Im Anwendungsbereich IT-Betrieb und Aufgabenübernahme durch Dritte (O) sind die Vorgaben zum Auditing auf Basis dieser Zentralen Dienstvorschrift vertraglich zu regeln.

7. Im IT-Grundschutz wird das Thema Protokollierung und Auditing sowohl im Baustein "Protokollierung" als auch in der Einzelmaßnahme "M 2.500 Protokollierung von IT-Systemen" behandelt. In Abhängigkeit der Größe und Komplexität des Informationsverbundes kann die Umsetzung der Einzelmaßnahme M 2.500 ausreichend sein. Für die Bw gelten zusätzlich die nachfolgend aufgeführten Grundsätze und Regelungen dieser Anlage.

11.6.2 Beschreibung der Auditingarten

11.6.2.1 Allgemein

8. Es ist zwischen den nachfolgend aufgeführten Auditingarten zu unterscheiden.

11.6.2.2 Systemauditing

9. Das Systemauditing dient der Überwachung und Kontrolle der Betriebs- und Funktionsfähigkeit von IT. Dabei werden Ereignisse auditiert, die Funktionalitäten, Leistungsmerkmale oder Performance von IT beeinträchtigen und die Nutzung einschränken oder verhindern.

10. Dieses Auditing wird in Verantwortung des IT-Betriebes durchgeführt und in dieser Zentralen Dienstvorschrift nicht weiter betrachtet.

11.6.2.3 Sicherheitsauditing

11. Das Sicherheitsauditing dient dem Nachvollzug von Ereignissen und Aktionen von an IT angemeldeten Anwendern und Administratoren bzw. unter deren Rechte ausgeführte Systemprozesse und Programme in Bezug auf die der Rechteverwaltung unterliegenden Objekte (z. B. Dateien, Verzeichnisse, andere Systemressourcen).

12. Im Rahmen des Sicherheitsauditings sind mindestens die nachfolgend aufgelisteten Ereignisse / Aktionen auszuwerten:

- Unberechtigter Zugang zur IT,
- Unberechtigter Zugriff auf Informationen,
- Durchführung von Änderungen in der Rechteverwaltung,
- Aktionen von an IT angemeldeten Anwendern mit Administrationsrechten und

- Aktionen von an IT angemeldeten Anwendern und Administratoren in Bezug auf die der Rechteverwaltung unterliegenden Objekte mit erhöhtem Schutzbedarf.

11.6.2.4 Datenschutzauditing

13. Im Datenschutzauditing werden datenschutzrelevante Ereignisse nach den jeweils geltenden Rechtsvorschriften und Bestimmungen zum Datenschutz sowie zur Amtsverschwiegenheit ausgewertet. Das Datenschutzauditing soll sicherstellen, dass Aktionen von an IT angemeldeten Anwendern und Administratoren bzw. unter deren Rechte aufgeführte Systemprozesse und Programme in Bezug auf die der Rechteverwaltung und dem Datenschutz unterliegenden Objekte (z. B. Dateien, Verzeichnisse, andere Systemressourcen mit PersDat) nachvollzogen werden können. Es sind datenschutzrelevante Protokolldaten nach den jeweils geltenden Rechtsvorschriften und Bestimmungen zum Datenschutz auszuwerten.

14. Dieses Auditing wird in Verantwortung des Datenschutzes durchgeführt und in dieser Zentralen Dienstvorschrift nicht weiter betrachtet.

11.6.3 Zuständigkeiten (P, V, O, S, D, E)

15. Der Leiter bzw. die Leiterin (Ltr) IPT / Projektleiter bzw. Projektleiterin (ProjLtr) bzw. der bzw. die Verantwortliche für Infra-Maßnahmen legt die zu protokollierenden Ereignisse und das projektbezogene Auditing (Vorgaben für ein Auditingkonzept) sowie die Anforderungen an die Integrität und die Verfügbarkeit der Protokolldaten (siehe auch Nr. 201 und Anlage 11.4.4, Abb. 24 Beispiel für eine Informationsstruktur) und die hierfür erforderlichen technischen InfoSichh-Maßnahmen im Rahmen der Erstellung bzw. Fortschreibung des InfoSichhKProj fest (vgl. Anlage 11.7.1).

16. Der bzw. die ISBBtrb ist zuständig für die Bewertung des Systemauditings in der jeweiligen IT-Btrb(Fü)Einr. In der nutzenden DSt bzw. dem nutzenden EinsKtgt ist der bzw. die bestellte ISBDSt oder der bzw. die ISBEinsatz für das Sicherheitsauditing und der bzw. die ADSB für das Datenschutzauditing zuständig.

11.6.4 Werkzeuge für das Auditing (P, V, O, S)

17. Soweit Protokolldaten entstehen und auszuwerten sind, muss sichergestellt sein, dass entsprechende Werkzeuge zu deren Auswertung und Verwaltung vorhanden sind. Die Werkzeuge unterliegen der Zugriffskontrolle und sind mit Ausführungsrechten ausschließlich für Auditoren bzw. ISB einzurichten.

18. Auditingwerkzeuge inklusive der zu deren Nutzung benötigten Ausbildung bzw. Ausbildungsdokumentation sind Bestandteil eines Projektes und sind wie jede andere Komponente durch das Projekt bereitzustellen. Für querschnittlich eingesetzte IT, welche nicht über ein Projekt beschafft wurde, ist gemäß der folgenden Nr. 19 vorzugehen.

19. Vor Werkzeugfestlegung ist zu prüfen, ob Werkzeuge für die Protokollierung und das Auditing in der „Technischen Architektur IT-System der Bundeswehr“ (B1-1500/6-7001 VS-NfD „Technische Architektur des IT-Systems Bundeswehr“, siehe Bezug Anlage 11.15 (lfdNr. 49)) aufgeführt sind. Sollten in der B1-1500/6-7001 VS-NfD „Technische Architektur des IT-Systems Bundeswehr“ keine oder keine geeigneten Werkzeuge aufgeführt sein, ist durch den jeweils zuständigen bzw. die jeweils zuständige ISB[164] die Verwendung des beabsichtigten Werkzeuges beim BAAINBw auf dem Dienstweg zu beantragen. BAAINBw prüft, auch unter Berücksichtigung der „Rahmendienstvereinbarung zur Protokollierung informationstechnischer Systeme“ (siehe Bezug Anlage 11.15 (lfdNr. 40)), ob das Werkzeug verwendet werden darf. Zudem prüft das BAAINBw, ob das geplante Werkzeug als Bw-Standard geeignet ist und ggf. in die B1-1500/6-7001 VS-NfD „Technische Architektur des IT-Systems Bundeswehr“ aufzunehmen ist.

11.6.5 Aufbewahrungs- und Löschfristen (P, V, O, S, D, E)

20. Bei der Festlegung der Aufbewahrungs- und Löschfristen von Protokolldaten und Auditinginformationen sind die Vorgaben des Datenschutzes und des Geheimschutzes sowie der Rahmendienstvereinbarung über die Protokollierung informationstechnischer Systeme (siehe Bezug Anlage 11.15 (lfdNr. 40)) zu berücksichtigen. Dabei ist folgendes zu beachten:

- Für die Aufbewahrungs- / Löschfrist von Protokolldaten und Auditinginformationen, die PersDat enthalten oder Rückschlüsse auf das Verhalten identifizierbarer IT-Anwender ermöglichen, gelten die Vorgaben der Rahmendienstvereinbarung (RDV) über die Protokollierung informationstechnischer Systeme §6 (5) (siehe Bezug Anlage 11.15 (lfdNr. 40)).
- Für die Aufbewahrungs- / Löschfrist von Protokolldaten und Auditinginformationen bei IT, die Informationen der Einstufung VS-VERTRAULICH oder höher sowie vergleichbare NATO- / EU-Einstufungen bzw. Einstufungen anderer Nationen, sonstiger überstaatlicher Organisationen oder „MISSION“[165] verarbeitet bzw. überträgt, gelten die Regelungen des Geheimschutzes[166].
- Die Aufbewahrungs- / Löschfrist von Protokolldaten und Auditinginformationen von Zugangskontrollanlagen in militärischen Sicherheitsbereichen beträgt grundsätzlich fünf Jahre. Ausnahmen können durch den zuständigen bzw. die zuständige DStLtr in Abstimmung mit BMVg SE I 1 festgelegt werden.
- Bei einem identifizierten Vorfall mit disziplinarischen Konsequenzen und / oder strafrechtlichen Ermittlungen oder einem Verdacht auf einen solchen Vorfall ist die Aufbewahrungs- / Löschfrist der

[164] ISB als Rollenträgerinnen und Rollenträger im jeweiligen Anwendungsbereich
[165] „MISSION“ ist der Platzhalter für eine spätere konkrete Benennung und setzt eine sog. *Security Policy* für den beabsichtigten Einsatz voraus. Insofern ist z.B. MISSION SECRET keine gültige Einstufung, sondern z. B. NATO / ISAF SECRET oder NATO SECRET Releasable to ISAF.
[166] Sicherheitsüberprüfungsgesetz (siehe Bezug Anlage 11.15 (LfdNr. 1)) i. V. m. der Verschlusssachenanweisung (VSA) (siehe Bezug Anlage 11.15 (LfdNr. 11)) und der A-1130/2 VS-NfD „Militärische Sicherheit in der Bundeswehr - Verschlusssachen“ (siehe Bezug Anlage 11.15 (LfdNr. 15)).

Protokolldaten und Auditinginformationen von dem bzw. der Disziplinarvorgesetzten ggf. in Abstimmung mit der Ermittlungsbehörde zu bestimmen.

- Bei Vorfällen mit Verdacht auf einen geheimdienstlichen Hintergrund ist der MAD über den bzw. die SichhBeauftr zu beteiligen (siehe auch Nr. 821, Nr. 822). Ausgewertete Protokolldaten ohne entsprechende Auffälligkeiten sind unverzüglich nach der Auswertung zu löschen (Wegfall der Zweckbindung).
- Protokolldaten, die nicht ausgewertet wurden und die keiner längeren Aufbewahrungsfrist unterliegen, sind spätestens nach drei Monaten zu löschen.
- Die Löschung von Protokolldaten darf nur durch Auditoren / InfoSichh-Personal erfolgen und bedarf bei der Verarbeitung von VS-VERTRAULICH oder höher eingestuften Informationen sowie vergleichbaren NATO- / EU-Einstufungen bzw. Einstufungen anderer Nationen, sonstiger überstaatlicher Organisationen oder „MISSION“[167] der Zustimmung des bzw. der SichhBeauftr.
- Sollen Protokolldaten und / oder die Auditinginformationen zu statistischen Zwecken genutzt werden, ist eine über die gemäß RDV über die Protokollierung informationstechnischer Systeme §6 (5) (siehe Bezug Anlage 11.15 (lfdNr. 40)) vorgeschriebene Löschfrist hinausgehende Aufbewahrung dieser Daten / Informationen nur in anonymisierter Form zulässig.

11.6.6 Separierung und Aufbewahrung von Protokolldaten (P, V, O, S)

21. Durch geeignete technische Maßnahmen und Mechanismen (z. B. durch Einrichten verschiedener Rollen mit unterschiedlichen Zugriffsberechtigungen auf die Daten), die durch den bzw. die Ltr IPT / ProjLtr zu planen und technisch zu realisieren sind, ist sicherzustellen, dass

- Protokolldaten der verschiedenen Auditingarten gemäß Anlage 11.6.2 zumindest logisch separiert abgelegt sind und
- Aufbewahrungs- und Löschfristen gemäß Anlage 11.6.5 regelkonform eingehalten werden können.

22. Es ist auch technisch sicherzustellen, dass das Sicherheitsauditing (insbesondere bei IT, die Informationen der Einstufung VS-VERTRAULICH oder höher sowie vergleichbare NATO- / EU-Einstufungen bzw. Einstufungen anderer Nationen, sonstiger überstaatlicher Organisationen oder „MISSION“[168] verarbeitet bzw. überträgt) unabhängig und unbeeinträchtigt vom Datenschutzauditing durchgeführt werden kann.

[167] „*MISSION*“ ist der Platzhalter für eine spätere konkrete Benennung und setzt eine sog. *Security Policy* für den beabsichtigten Einsatz voraus. Insofern ist z.B. MISSION SECRET keine gültige Einstufung, sondern z.B. NATO / ISAF SECRET oder NATO SECRET Releasable to ISAF.

[168] „MISSION“ ist der Platzhalter für eine spätere konkrete Benennung und setzt eine sog. Security Policy für den beabsichtigten Einsatz voraus. Insofern ist z.B. MISSION SECRET keine gültige Einstufung, sondern z. B. NATO / ISAF SECRET oder NATO SECRET Releasable to ISAF.

23. Protokolldaten und Auditinginformationen sind im Rahmen der festgelegten Aufbewahrungs- und Löschfristen gemäß der Anforderungen an ihre Verfügbarkeit und ihre Integrität (siehe Anlage 11.6.3, Nr. 15) aufzubewahren. Dazu muss technisch sichergestellt werden, dass

- alle im jeweiligen InfoSichhK bzw. Auditingkonzept vorgegebenen Ereignisse und Aktionen protokolliert werden und ausreichend Speicherplatz für die Protokolldaten vorhanden ist,
- die Protokolldaten während der IT-gestützten Generierung der Auditinginformationen nicht verändert werden können,
- die Protokolldaten und Auditinginformationen vor unbeabsichtigter und unbefugter Löschung, Vernichtung und Veränderung geschützt sind,
- die Protokolldaten und Auditinginformationen ohne Manipulationsmöglichkeiten zugriffsgeschützt gespeichert werden.

24. Maßnahmen zur manipulationssicheren Protokollierung (z. B. Schutz durch Hash-Verfahren oder Verschlüsselung) ggf. bis hin zur Revisionssicherheit sind durch das Projekt systembezogen zu prüfen und festzulegen.

11.6.7 Zugriff auf Protokollinformationen (D, E)

25. Es muss sichergestellt sein, dass **nur** InfoSichh-Personal (z. B. ISB, Auditoren) und Administratoren Zugriff auf die betriebs- und informationsssicherheitsrelevanten Protokollinformationen (zum Zweck der Betriebsführung und -überwachung der IT) bzw. **nur** Datenschutzauditoren (z. B. der bzw. die ADSB[169] / BfDBw[170]) und Administratoren Zugriff auf die datenschutzrelevanten Protokolldaten (zum Zweck des Datenschutzauditings) haben.

26. Der Zugriff des InfoSichh-Personals bzw. der Auditoren auf die Protokolldaten darf nur lesend möglich sein, zur notwendigen Löschung gemäß Anlage 11.6.5. ist diesem Personal das Löschrecht temporär durch den DStLtr einzuräumen.

27. Dem bzw. der ISB sind darüber hinaus lesende Rechte auf alle Systemdateien einzurichten. Weiterhin muss er bzw. sie zur Durchführung von InfoSichhKtr den Zugriff auf die Metadaten (d. h. Dateiname, -typ, -größe, -besitzer, Änderungsdatum und Rechteeinstellungen) von Nutzerdateien erhalten können.

[169] Der bzw. die ADSB hat die Berechtigung, Protokolldaten auszuwerten, soweit dies seine bzw. ihre durch den Dienststellenleiter bzw. die Dienststellenleiterin zugewiesenen Aufgaben umfasst.
[170] Der bzw. die BfDBw hat aufgrund seiner bzw. ihrer gesetzlichen Kontrollbefugnis die Berechtigung, Protokolldaten auszuwerten.

11.7 Aufbau und Struktur von Informationssicherheitskonzepten

11.7.1 Projekte und Vorhaben (P, V, O, S)

1. Neue und in der Erstellung bzw. Abstimmung befindliche InfoSichhK für Projekte und Vorhaben, die nach der Methodik dieser Zentralen Dienstvorschrift erstellt werden, sind gem. „Arbeitshilfe zur Erstellung von Projektbezogenen InfoSichhK gemäß IT-Grundschutz - Teil 1“. zu gliedern (siehe Nr. 2 in Anlage 11.1.1). Die aktuelle Version der Arbeitshilfe wird im Intranetauftritt http://infosichh.bundeswehr.org im Bereich „InfoSichhorg / DEUmilSAA / InfoSichhProj“ bereitgestellt.

Die Arbeitshilfe besteht aus zwei Teilen. Teil 1 beschreibt den Anteil der Dokumentation und Teil 2 die Arbeitsschritte, die im Werkzeug erfolgen.

11.7.2 Vorhaben Forschung und Wissenschaft (F, W)

2. Für Vorhaben der Wehrtechnischen Forschung & Technologie sowie sonstiger Forschungsvorhaben, Erprobungen, Truppenversuchen und Wehrtechnischen Aufträgen oder von Vorhaben der Wissenschaftlichen Unterstützung nicht-technisch sind InfoSichhKFW in Anlehnung an einen InfoSichhBef zu erstellen (siehe Abschnitt 6.3.5). Ein Muster für Aufbau und Struktur des InfoSichhBef mit Angaben zu den wesentlichen Inhalten ist Anlage 11.8.8 zu entnehmen.

11.7.3 Dienststellen / Einsatzkontingente (D, E)

3. Neue und in der Erstellung bzw. Abstimmung befindliche InfoSichhKDSt[171], die nach der Methodik dieser Zentralen Dienstvorschrift erstellt werden, sind gem. „Arbeitshilfe zur Erstellung von Dienststellenbezogenen InfoSichhK - Teil 1“ zu gliedern (siehe Nr. 2 in Anlage 11.1.1). Die aktuelle Version der Arbeitshilfe wird im Intranetauftritt http://infosichh.bundeswehr.org im Bereich „IT-Grundschutz“ im Downloadbereich bereitgestellt.

Die Arbeitshilfe besteht aus zwei Teilen. Teil 1 beschreibt den Anteil der Dokumentation und Teil 2 die Arbeitsschritte, die im Werkzeug erfolgen.

11.7.4 Übungen (Ü)

4. Für Übungen sind InfoSichhBef gemäß Abschnitt 6.3.5 zu erstellen. Ein Muster für Aufbau und Struktur des InfoSichhBef mit Angaben zu den wesentlichen Inhalten ist Anlage 11.8.8 zu entnehmen.

[171] gilt auch für Einsatzkontingente

11.8 Musterformulare[172]

11.8.1 (Vorläufige) Freigabe zur Nutzung[173]

(Vorläufige) Freigabe zur Nutzung im Projekt

.....
(Name, DGrad / ABez, Projektleiter/in)

.....
(Ort, Datum)

Az 62-

Betr.: Freigabe von IT

Bezug: 1. Zentrale Dienstvorschrift A-960/1 „Informationssicherheit“
2. InfoSichhKProj

Die IT aus dem Projekt

wurde unter Beachtung o. g. Bezüge in der / im

.....
(Ort, z. B. Liegenschaft, Gebäude, Raum, Kabine)
eingerichtet.

Es wird die Freigabe zur Nutzung im Projekt für Informationen, die für die Verarbeitung bzw. Übertragung von

☐ APersDat SB 1 ☐ Informationen der Einstufung

☐ erklärt

☐ erklärt mit folgenden Auflagen:

[172] siehe A-2122/4 (Nr. 285): In jedes Formular – unabhängig davon, ob es sich um ein Formular in Schriftform oder ein elektronisches Formular handelt – ist ein Feld aufzunehmen, aus dem eindeutig ersichtlich ist, ob das ausgefüllte Formular dem Schutzbereich 1, 2 oder 3 zugeordnet ist. Das Feld trägt die Bezeichnung „Schutzbereich“. Um ein einheitliches Vorgehen sicherzustellen, ist das Feld auf der ersten Seite des betreffenden Formulars oben rechts platziert. "

[173] siehe FormulardatenbankBw - Formularnummer Bw/2935, Schutzbereich 1

☐ **vorläufig** erklärt mit folgenden Auflagen:

[ ]

bis zum [ ]

☐ **nicht** erklärt

Begründung:

[ ]

....

(Unterschrift, Name Rollenträgerinnen und Rollenträger) (Unterschrift, Name zuständige(r) ISB)

Verteiler:

ISBOrgBer

ISBProj

Projektleiter/in

InfoSichhDok

IT-Arbeitsplatz

[ ]

[ ]

[ ]

[ ]

[ ]

[ ]

[ ]

[ ]

11.8.2 Muster für eine dienststellenbezogene Informationssicherheitsdokumentation

Informationssicherheitsdokumentation

1. Teil Allgemeine Grundlagen für die InfoSichh

Inhaltsverzeichnis

2. Teil Maßnahmen im personellen Bereich

Inhaltsverzeichnis

2.8 Stoffsammlung für Informationssicherheitsausbildung
(aktuelle Themen)

3. Teil Maßnahmen im infrastrukturellen Bereich

Inhaltsverzeichnis

3.1 Bauunterlagen / -pläne
(einschließlich Zonen gemäß Zonenmodell, Sperrzonen)[174]

4. Teil Maßnahmen im organisatorischen Bereich

Inhaltsverzeichnis

4.1 Dienststellenbezogenes InfoSichhK (InfoSichhKDSt)

4.2 Für die DSt relevante Auszüge der InfoSichhKProj bzw. InfoSichhKFW gemäß Nr. 1.1

4.3 Freigabeverfügungen, Akkreditierungsbescheinigungen

4.4 Terminkalender
(nur Termine InfoSichh, dabei auch Terminierung von Abstrahlprüfungen gemäß Zentraler Dienstvorschrift A-962/1 VS-NfD „Abstrahlsicherheit“ für abstrahlprüfpflichtiges Gerät, falls vorhanden)

4.5 InfoSichhVork
(Meldungen, Schriftverkehr, Aktenvermerke)

4.6 Vermerke über durchgeführte InfoSichhKtr
(bei eigener Dienststelle)

4.7 Prüfprotokolle, Abnahmebescheinigungen

4.8 Prüfberichte aus InfoSichhIn und InfoSichhPrfg

4.9 Dokumentation der Mängelbeseitigung (falls erforderlich)

5. Teil Maßnahmen im technischen Bereich

Inhaltsverzeichnis

5.1 Informationstechnische Regelungen / Maßnahmen

5.2 Übersicht über das abstrahlprüfpflichtige Gerät

5.3 Regelungen zur Softwarepflege und -änderung (SWPÄ)

5.4 Ausnahmegenehmigungen für Netzübergänge und Nutzung privater IT zu dienstlichen Zwecken

[174] Unterlagen können auch bei einer übergeordneten zuständigen Dienststelle geführt werden.

11.8.3 Berichte für Informationssicherheitsinspektionen

11.8.3.1 Bericht mit Kryptoanteil

Informationssicherheitsinspektionsbericht[175]

Zentrum für Cybersicherheit der Bundeswehr
Regionalzentrum NORD

Ort,
Postfach / Straße
Telefon: –
Bw: –
Bearbeiter:

Verteiler	Funktion	mit Anlagen
☐	CISOBw (anlassbezogen)	☐
☒	ISBOrgBer	☐
☐	DEUmilSAA (anlassbezogen)	☒
☒	DStLtr / DStLtr´in vorgesetzte DSt	☐
☒	ISBDSt vorgesetzte DSt	☒
☒	DStLtr / DStLtr´in geprüfte DSt	☐
☒	ISBDSt geprüfte DSt	☒
☐	Ltr / Ltr´in IT-Btrb(Fü)Einr (anlassbezogen)	☒
☐	ISBBtrb (anlassbezogen)[176]	☒
☒	ZCSBw CSOCBw	☒
☒	ZCSBw Gruppe Prüf- und Unterstützungsteams	☒
☐		☐
☐		☐
☐		☐
☐		☐

[175] siehe FormulardatenbankBw - Formularnummer Bw/2934K, Schutzbereich 1
[176] Nur bei Einsatz bezogenen Inspektionen

Informationssicherheitsinspektionsbericht Nr.: ☐

1. Allgemeines

1.1. Überprüfte Dienststelle: ☐

1.2. Dienststellenleiter / Dienststellenleiterin: ☐

1.3. Vorgesetzte Dienststelle: ☐

1.4. Inspektion vom: ☐ Anlass: ☐

1.5. Letzte Inspektion am: ☐ durch: ☐

1.6. Die im vorhergehenden Inspektionsbericht genannten Mängel sind abgestellt: ja ☐ nein ☐

1.7. Vorhandene Kryptomittel:

☐ NATO ☐ National ☐ Multinational / Coalition ☐ Sonstige

1.8. Anlagen:

☐ Prüfbemerkungen zu den Prüffragen der Bw-einheitlichen Prüfliste

☐ Log-Dateien ☐ Screenshots

☐ Liste der vom Prüfteam verwendeten Hard- und Software

2. Bewertung

2.1. Der ***Gesamtzustand*** der Informationssicherheit wird wie folgt bewertet:

„Die Informationssicherheit ist ☐ gewährleistet.“

2.2. Der ***Zustand*** der Informationssicherheit, den die ***Dienststelle zu verantworten*** hat, wird wie folgt bewertet:

„Die Informationssicherheit ist ☐ gewährleistet.“

2.3. Die Prüfung der Kryptoverwaltung gemäß gültigem Bestandsbericht ergab:

„Die Kryptosicherheit ist ☐ gewährleistet.“

3. Abschlussbesprechung

In einem Abschlussgespräch am ☐ wurde dem ☐ eine vorläufige Bewertung der Informationssicherheit mit kurzer Begründung eröffnet. Dabei wurden die festgestellten Probleme und Lösungsmöglichkeiten erörtert.

4. Berichte des Dienststellenleiters / der Dienststellenleiterin

4.1. Termine:

☐ Am ☐ wird ein Bericht für die als „Sofortmaßnahme“ gekennzeichneten Anteile erwartet.

☐ Am ☐ wird ein Abschlussbericht über die Bearbeitung der kompletten Mängelliste erwartet.

☐ Es sind keine Maßnahmen erforderlich.

4.2. Inhalt:

Die Berichte haben mindestens eine stichpunktartige Beschreibung der getroffenen Maßnahmen und ggf. deren Ergebnisse bzw. Sachstände zu den im Informationssicherheitsinspektionsbericht aufgeführten Mängeln zu enthalten.

5. Wesentliche Feststellungen

Zu 2.1.: ☐
Zu 2.2.: ☐
Zu 2.3.: ☐

6. Folgerungen und Vorschläge

☐

(Ort, Datum, Unterschrift)

Bewertung	**Kriterium**
Gewährleistet	Höchstens 2 % der umzusetzenden einfachen InfoSichh-Anforderungen / InfoSichh-Maßnahmen[177] für normalen Schutzbedarf nicht oder nicht vollständig umgesetzt.
Eingeschränkt gewährleistet	Mehr als 2 % und höchstens 15 % der umzusetzenden einfachen InfoSichh-Anforderungen / InfoSichh-Maßnahmen für normalen Schutzbedarf nicht *oder* nicht vollständig umgesetzt. *oder* Höchstens eine umzusetzende wesentliche InfoSichh-Anforderung / InfoSichh-Maßnahme[178] für hohen Schutzbedarf nicht oder nicht vollständig umgesetzt.
Nicht gewährleistet	Mehr als 15 % der umzusetzenden einfachen InfoSichh-Anforderungen / InfoSichh-Maßnahmen für normalen Schutzbedarf nicht oder nicht vollständig umgesetzt. *oder* Mindestens zwei umzusetzende und höchstens 10 % der umzusetzenden wesentlichen InfoSichh-Anforderungen / InfoSichh-Maßnahmen für hohen Schutzbedarf nicht oder nicht vollständig umgesetzt. *oder* Höchstens eine umzusetzende wesentliche InfoSichh-Anforderung / InfoSichh-Maßnahme für sehr hohen Schutzbedarf nicht oder nicht vollständig umgesetzt.
Aufgrund schwerwiegender Mängel nicht gewährleistet	Mehr als 10 % der umzusetzenden einfachen InfoSichh-Anforderungen / InfoSichh-Maßnahmen für hohen Schutzbedarf nicht oder nicht vollständig umgesetzt. *oder* Mindestens zwei umzusetzende wesentliche InfoSichh-Anforderungen / InfoSichh-Maßnahmen für sehr hohen Schutzbedarf nicht oder nicht vollständig umgesetzt.

[177] Prüffragen gem. der Bw-einheitlichen Prüfliste, die nicht mit einem wesentlichen Mangel (wM) angegeben sind.
[178] Prüffragen gem. der Bw-einheitlichen Prüfliste, die mit einem wesentlichen Mangel (wM) angegeben sind.

11.8.3.2 Bericht ohne Kryptoanteil

Informationssicherheitsinspektionsbericht[179]

Zentrum für Cybersicherheit der Bundeswehr
Regionalzentrum NORD

Ort,
Postfach / Straße
Telefon: –
Bw: –
Bearbeiter:

Verteiler	Funktion	mit Anlagen
☐	CISOBw (anlassbezogen)	☐
☒	ISBOrgBer	☐
☐	DEUmilSAA (anlassbezogen)	☒
☒	DStLtr / DStLtr´in vorgesetzte DSt	☐
☒	ISBDSt vorgesetzte DSt	☒
☒	DStLtr / DStLtr´in geprüfte DSt	☐
☒	ISBDSt geprüfte DSt	☒
☐	Ltr / Ltr´in IT-Btrb(Fü)Einr (anlassbezogen)	☒
☐	ISBBtrb (anlassbezogen)[180]	☒
☒	ZCSBw CSOCBw	☒
☒	ZCSBw Gruppe Prüf- und Unterstützungsteams	☒
☐		☐
☐		☐
☐		☐
☐		☐

[179] siehe FormulardatenbankBw - Formularnummer Bw/2934, Schutzbereich 1
[180] Nur bei Einsatz bezogenen Inspektionen

Informationssicherheitsinspektionsbericht Nr.: ☐

1. Allgemeines

1.1. Überprüfte Dienststelle: ☐

1.2. Dienststellenleiter / Dienststellenleiterin: ☐

1.3. Vorgesetzte Dienststelle: ☐

1.4. Inspektion vom: ☐ Anlass: ☐

1.5. Letzte Inspektion am: ☐ durch: ☐

1.6. Die im vorhergehenden Inspektionsbericht genannten Mängel sind abgestellt: ja ☐ nein ☐

1.7. Keine Kryptomittel vorhanden ☐

1.8. Anlagen:

☐ Prüfbemerkungen zu den Prüffragen der Bw-einheitlichen Prüfliste

☐ Log-Dateien ☐ Screenshots

☐ Liste der vom Prüfteam verwendeten Hard- und Software

2. Bewertung

2.1. Der ***Gesamtzustand*** der Informationssicherheit wird wie folgt bewertet:

„Die Informationssicherheit ist gewährleistet.“

2.2. Der ***Zustand*** der Informationssicherheit, den die ***Dienststelle zu verantworten*** hat, wird wie folgt bewertet:

„Die Informationssicherheit ist gewährleistet.“

3. Abschlussbesprechung

In einem Abschlussgespräch am ☐ wurde dem ☐ eine vorläufige Bewertung der Informationssicherheit mit kurzer Begründung eröffnet. Dabei wurden die festgestellten Probleme und Lösungsmöglichkeiten erörtert.

4. Berichte des Dienststellenleiters / der Dienststellenleiterin

4.1. Termine:

☐ Am ☐ wird ein Bericht für die als „Sofortmaßnahme“ gekennzeichneten Anteile erwartet.

☐ Am ☐ wird ein Abschlussbericht über die Bearbeitung der kompletten Mängelliste erwartet.

☐ Es sind keine Maßnahmen erforderlich.

4.2. Inhalt:

Die Berichte haben mindestens eine stichpunktartige Beschreibung der getroffenen Maßnahmen und ggf. deren Ergebnisse bzw. Sachstände zu den im Informationssicherheitsinspektionsbericht aufgeführten Mängeln zu enthalten.

5. Wesentliche Feststellungen

Zu 2.1.: ☐
Zu 2.2.: ☐

6. Folgerungen und Vorschläge

☐

(Ort, Datum, Unterschrift)

Bewertung	**Kriterium**
Gewährleistet	Höchstens 2 % der umzusetzenden einfachen InfoSichh-Anforderungen / InfoSichh-Maßnahmen[181] für normalen Schutzbedarf nicht oder nicht vollständig umgesetzt.
Eingeschränkt gewährleistet	Mehr als 2 % und höchstens 15 % der umzusetzenden einfachen InfoSichh-Anforderungen / InfoSichh-Maßnahmen für normalen Schutzbedarf nicht *oder* nicht vollständig umgesetzt. *oder* Höchstens eine umzusetzende wesentliche InfoSichh-Anforderung / InfoSichh-Maßnahme[182] für hohen Schutzbedarf nicht oder nicht vollständig umgesetzt.
Nicht gewährleistet	Mehr als 15 % der umzusetzenden einfachen InfoSichh-Anforderungen / InfoSichh-Maßnahmen für normalen Schutzbedarf nicht oder nicht vollständig umgesetzt. *oder* Mindestens zwei umzusetzende und höchstens 10 % der umzusetzenden wesentlichen InfoSichh-Anforderungen / InfoSichh-Maßnahmen für hohen Schutzbedarf nicht oder nicht vollständig umgesetzt. *oder* Höchstens eine umzusetzende wesentliche InfoSichh-Anforderung / InfoSichh-Maßnahme für sehr hohen Schutzbedarf nicht oder nicht vollständig umgesetzt.
Aufgrund schwerwiegender Mängel nicht gewährleistet	Mehr als 10 % der umzusetzenden einfachen InfoSichh-Anforderungen / InfoSichh-Maßnahmen für hohen Schutzbedarf nicht oder nicht vollständig umgesetzt. *oder* Mindestens zwei umzusetzende wesentliche InfoSichh-Anforderungen / InfoSichh-Maßnahmen für sehr hohen Schutzbedarf nicht oder nicht vollständig umgesetzt.

[181] Prüffragen gem. der Bw-einheitlichen Prüfliste, die nicht mit einem wesentlichen Mangel (wM) angegeben sind.
[182] Prüffragen gem. der Bw-einheitlichen Prüfliste, die mit einem wesentlichen Mangel (wM) angegeben sind.

11.8.4 Bestellung zum bzw. zur Informationssicherheitsbeauftragten, zum ständigen Vertreter bzw. zur ständigen Vertreterin sowie zum Informationssicherheitsgehilfen bzw. zur Informationssicherheitsgehilfin[183]

(Dienststelle und ggf. Bezeichnung konkreter Anwendungsbereich)

(Aktenzeichen)

Nr.	Dienststellung	Name	Vorname	DGrad / ABez / EntgeltGr	Funktion Hauptamtlich Nebenamtlich	letzter Lehrgang IT-SiBe / ISB Monat / Jahr von	bis	Krypto-ausbildung	SÜ	Ermächtigt zum Umgang mit National / NATO	Unterschrift
1	ISB DSt				Hauptamt			NEIN	Ü3	GEHEIM NATO SECRET	
2	Stv. ISB DSt				Nebenamt			NEIN	Ü2	GEHEIM NATO SECRET	
3	InfoSichhGeh				Nebenamt			NEIN	Ü2	GEHEIM NATO SECRET	
4	InfoSichhGeh				Nebenamt			NEIN	Ü2	GEHEIM NATO SECRET	
5	InfoSichhGeh				Nebenamt			NEIN	Ü2	GEHEIM NATO SECRET	

1. Die Bestellung kann vom bzw. von der Unterzeichnenden jederzeit zurückgezogen werden. Personelle Veränderungen sind dem Verteiler umgehend schriftlich mitzuteilen. Eine neue Bestellung ist umgehend zu erstellen. Ungültige Bestellungen sind gemäß A-1130/2 VS-NfD „Militärische Sicherheit in der Bundeswehr – Militärische Sicherheit“ aufzubewahren.
2. Die Richtigkeit der Unterschriften wird bescheinigt.
3. Die Bestellung verliert mit dem Tage der Versetzung ihre Gültigkeit.

Der Dienststellenleiter der Dienststelle bestellt die oben genannten Personen mit Wirkung zum heutigen Tag.

(Ort) (Datum) (Dienstsiegel)

(Unterschrift, Name, DGrad / ABez des DStLtr)

Verteiler (bitte auswählen):

bestellte Person
DStLtr
ISBOrgBer
zuständige Kryptoverteilerstelle
ISB vorgesetzte DSt

[183] Für ISBProj, ISBBtrb, ISBFW und ISBÜb ist analog zu verfahren, FormulardatenbankBw - Formularnummer Bw/2938, Schutzbereich 1

11.8.5 Dienstanweisung für den Informationssicherheitsbeauftragten bzw. die Informationssicherheitsbeauftragte Dienststelle / im Einsatz

Dienstanweisung

für den Informationssicherheitsbeauftragten bzw. die

Informationssicherheitsbeauftragte Dienststelle / im Einsatz[184]

Dienststelle:		Ort, Datum:	
Az:		Tel.:	
		Bw:	
		Fax:	

I. Bezeichnung der Dienststellung

1. Der bzw. die mit der Überwachung der Informationssicherheit (InfoSichh) der Dienststelle / des EinsKtgt Beauftragte führt die Bezeichnung: „Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte (Dienststelle / im Einsatz)“, Abkürzung: „ISBDSt / ISB i.E.“.
2. Die Aufgabe des bzw. der ISBDSt / ISB i.E. wird durch den Inhaber des Dienstpostens **DP-ID** wahrgenommen.

II. Vorgesetztenverhältnis und Unterstellung

1. Der bzw. die ISB ist zur Herstellung, Gewährleistung und Wiederherstellung der InfoSichh inkl. IT-RM anordnungs- / weisungsbefugt gegenüber allen Soldaten bzw. Soldatinnen, Beamten bzw. Beamtinnen und Arbeitnehmern bzw. Arbeitnehmerinnen in ihrem jeweiligen Zuständigkeitsbereich. Militärische ISB sind in ihrem jeweiligen Zuständigkeitsbereich Vorgesetzte aller Soldatinnen und Soldaten gemäß § 3 VorgV.
2. Der bzw. die ISBDSt / ISB i.E. untersteht im Aufgabenbereich der InfoSichh in der DSt / im EinsKtgt unmittelbar dem Dienststellenleiter bzw. der Dienststellenleiterin / Kontingentführer bzw. Kontingentführerin / Kommandeur bzw. Kommandeurin Einsatzstandort und hat in der Wahrnehmung seiner bzw. ihrer Aufgaben ein direktes Vortragsrecht bei dem bzw. der für die InfoSichh verantwortlichen Vorgesetzten.

III. Aufgaben

1. Der bzw. die ISBDSt / ISB i.E. überwacht und veranlasst Maßnahmen zum Herstellen, Gewährleisten und Wiederherstellen der InfoSichh inkl. des IT-Risikomanagements in der DSt / im EinsKtgt.
2. Der bzw. die ISBDSt / ISB i.E. ist zur Wahrnehmung seiner bzw. ihrer Aufgaben auf Zusammenarbeit mit dem bzw. der Sicherheitsbeauftragten, dem bzw. der IT-Verantwortlichen

[184] siehe FormulardatenbankBw - Formularnummer Bw/2937, Schutzbereich 1

der DSt / des EinsKtgt, dem bzw. der administrativen Datenschutzbeauftragten (ADSB) der Dienststelle sowie den ISBProj, den ISBFW undden ISBBtrb, die der DSt /dem EinsKtgt IT zur Nutzung übergeben haben bzw. IT für die DSt / das EinsKtgt betreiben angewiesen.

3. Aufgaben des bzw. der ISBDSt / ISB i.E. sind:
   - Beraten des bzw. der DStLtr / KtgtFhr / Kdr EinsStO in allen Fragen zur InfoSichh inkl. IT-RM sowie der IT-relevanten Anteile des Datenschutzes, des Geheimschutzes und der Militärischen Sicherheit.
   - Verantworten der Rolle eines IT-Risikomanagers bzw. einer IT-Risikomanagerin für seinen bzw. ihren Zuständigkeitsbereich.
   - Erstellen von Beiträgen zum IT-Risikokatalog.
   - Erarbeiten und Fortschreiben des InfoSichhK für die DSt / das EinsKtgt unter Berücksichtigung der Vorgaben aus den InfoSichhK der genutzten IT (z.B. InfoSichhKProj, InfoSichhKFW).
   - Umsetzen von Vorgaben des bzw. der ISBBtrb zur Einhaltung und Wiederherstellung der InfoSichh in den Betriebsprozessen aller IT-Services im IT-SysBw. Vorgaben für die Einsatzgebiete sind mit dem bzw. der ISBEinsatz abzustimmen.
   - Prüfen der personellen, infrastrukturellen und organisatorischen InfoSichh-Maßnahmen gemäß InfoSichhKDSt. Der bzw. die ISB i.E. prüft zusätzlich die technischen InfoSichh-Maßnahmen gemäß der InfoSichhKProj.
   - Empfehlen der Freigabe zur Nutzung von IT (operationelle Freigabe) gemäß A-960/1, Abschnitt 5.6.3 sowie der Freigabe in der Nutzung gemäß Abschnitt 5.6.4 nach Durchführung der erforderlichen Prüfungen.
   - Anwenden / Umsetzen von Vorschriften und Weisungen zur InfoSichh (einschl. der Vorschriften und Weisungen zum Datenschutz und zum Geheimschutz), ggf. Erstellen von konkreten Handlungsanweisungen, soweit Besonderheiten seiner bzw. ihrer DSt / seines bzw. ihres EinsKtgt dies fordern.
   - Durchführen von Informationssicherheitsbelehrungen für Personal der DSt / des EinsKtgt.
   - Weiterbilden / Sensibilisieren des IT-Personals und der IT-Anwender.
   - Durchführen von InfoSichhKtr zur Überwachung der InfoSichh in der eigenen DSt / im eigenen EinsKtgt; dies schließt Kontrollen der in den DSt / im EinsKtgt genutzten IT nach Vorgabe InfoSichhKProj ein.
   - Unterstützen bei der Durchführung von InfoSichhIn und InfoSichPrfg im eigenen Zuständigkeitsbereich.
   - Bearbeiten von Informationssicherheitsvorkommnissen und Kryptoverstößen.
   - Führen der InfoSichhDok in dem für seine bzw. ihre DSt / sein bzw. ihr EinsKtgt erforderlichen Umfang.
   - Prüfen der Kryptotagebücher der Dienststelle gemäß Zentraler Dienstvorschrift A-961/1 VS-NfD „Kryptosicherheit in der Bundeswehr“ jährlich bzw. bei Kontingentwechsel.

- Überwachen der ordnungsgemäßen Durchführung der Kryptoverwaltung der DSt / des EinsKtgt gemäß Zentraler Dienstvorschrift A-961/1 VS-NfD „Kryptosicherheit in der Bundeswehr“.
- Überwachen des ordnungsgemäßen Einsatzes und Betriebs von Kryptomitteln der DSt / des EinsKtgt.
- Wahrnehmen der Aufgaben des COMSEC-Officers für die DSt / das EinsKtgt gemäß SDIP 293/1 NATO RESTRICTED „Instructions for the control and safeguarding of NATO cryptomaterial“ beim Einsatz von NATO-Kryptomitteln.
- Wahrnehmen weiterer Aufgaben im Bereich des Kryptowesens gemäß Zentraler Dienstvorschrift A-961/1 VS-NfD „Kryptosicherheit in der Bundeswehr“ (insbesondere aus der Checkliste gemäß A-961/1, Anlage 9.12)
- Zusammenarbeiten mit dem bzw. der jeweils zuständigen Sicherheitsbeauftragten und dem bzw. der ADSB.
- Übermitteln wesentlicher Erkenntnisse zur Informationssicherheit aus der DSt / dem EinsKtgt an den bzw. die ISBOrgBer / ISBEinsatz.
- Auswerten und Bewerten von Erkenntnissen aus den eigenen Kontrolltätigkeiten und den gemeldeten InfoSichhVork.
- Melden identifizierter Regelungslücken für die DSt / das EinsKtgt an den bzw. die ISBOrgBer / ISBEinsatz.
- Auswerten einschlägiger Informationen zur Informationssicherheit mit Bedeutung für die DSt / das EinsKtgt.
- Teilnehmen an nationalen und internationalen Fachtagungen im Bereich InfoSichh.
- Durchführen des Sicherheitsauditings in der DSt (nur ISBDSt)

IV. Zeichnungsrecht, Stellvertretung

1. Der bzw. die ISBDSt / ISB i.E. zeichnet in Wahrnehmung seiner bzw. ihrer Aufgaben unter dem Briefkopf „ISBDSt“ / „ISB i.E.“ mit dem Zusatz „Im Auftrag“ durch Unterschrift unter Hinzufügen von Name und Dienstgrad / Amtsbezeichnung / Entgeltgruppe.
2. Der bzw. die ISBDSt / ISB i.E. wird vertreten durch den Inhaber bzw. die Inhaberin des Dienstpostens **DP-ID** .

V. Besonderheiten und Übergangsbestimmungen

1. Weisungen im Aufgabenbereich der InfoSichh erhält er bzw. sie vom bzw. von der CISOBw / ISBOrgBer / ISBEinsatz. Weisungen zur InfoSichh organisatorischer und administrativer Art kann er bzw. sie auch vom bzw. von der ISB der fachlich vorgesetzten Dienststelle erhalten.

Dienststellenleiter bzw. Dienststellenleiterin / Kontingentführer bzw. Kontingentführerin / Kommandeur bzw. Kommandeurin Einsatzstandort

_____

(Unterschrift, Name)

Verteiler:
(Wird durch OrgBer festgelegt)

11.8.6 Verpflichtungs- und Belehrungserklärung für Informationssicherheitspersonal

Verpflichtungs- und Belehrungserklärung

für Informationssicherheitspersonal[185]

Ich,

DGrad / ABez / EntgeltGr	Vorname	Nachname

bin heute im Rahmen meiner dienstlichen Tätigkeit als ☐

über die Bestimmungen[186] der / des ☐ **A-1130/2 VS-NfD**

☐ **A-960/1**

☐ **A-961/1 VS-NfD**

☐ **§ 53 BDSG**

☐ ☐

☐ ☐

belehrt worden.

Ich verpflichte mich,

- die o. a. Bestimmungen einzuhalten,
- keine privaten Notizen über mir anvertraute und zur Kenntnis gelangte Angelegenheiten zu machen und
- über alle schutzbedürftigen Informationen, die mir im Verlauf meiner Dienstzeit zur Kenntnis gelangen, gegenüber Unbefugten Stillschweigen zu bewahren.

[185] siehe FormulardatenbankBw - Formularnummer Bw/2936, Schutzbereich 1
[186] kann ggf. durch weitere Bestimmungen ergänzt werden (z. B. Regelungen der OrgBer)

Ich weiß, dass jeder fahrlässige, grob fahrlässige oder vorsätzliche Verstoß gegen die o. a. Bestimmungen strafrechtlich oder disziplinar bzw. arbeitsrechtlich geahndet werden kann.

Diese Verpflichtung gilt auch für die Zeit nach meinem Ausscheiden aus der Bundeswehr.

Der bzw. die Verpflichtete (Unterschrift, Name)	Der bzw. die Verpflichtende (Unterschrift, Name)
 (Ort / Datum)	

11.8.7 Akkreditierungsbescheinigung

Akkreditierungsbescheinigung

Betreff: **Bestätigung der Akkreditierung**

☐ Approval to Operate (ATO)
☐ Interim Approval to Operate (IATO)
☐ Approval for Testing (AfT)

IT: "Name des Systems"
Ort: "Liegenschaft"

Bezug:
1. A-960/1 „Informationssicherheit“
2. A-961/1 VS-NfD „Kryptosicherheit in der Bundeswehr“
3. A-962/1 VS-NfD „Abstrahlsicherheit“
4. InfoSichhKProj "Name des Systems"

	Stand:	
☐		
☐		
☐		

Anlage(n): – – –

Hiermit wird ein Approval to Operate für die IT "Name des Systems" in "Ort (Liegenschaft)" ausgesprochen.
Die genannte IT erfüllt die Voraussetzungen für die Verarbeitung von eingestuften Informationen bis zum Geheimhaltungsgrad (einschl.).

National: **VS-NfD**
International: **NATO RESTRICTED**

Auflagen: Die IT "Name des Systems" darf ohne vorherige Genehmigung der DEUmilSAA nicht mit weiterer IT verbunden werden.
Änderungen innerhalb der IT "Name des Systems", die die Informationssicherheit beeinträchtigen können, bedürfen ebenfalls der Zustimmung der DEUmilSAA.

Zusätzliche Auflagen: ☐ keine ☐ folgende ☐ siehe Anlage

Eine Nichtbeachtung dieser Auflagen führt zum Verlust dieser Akkreditierung! Diese ist gemäß A-960/1 Grundlage für die Freigabe zur Nutzung der IT.

Informationssicherheitsvorkommnisse bzgl. dieser IT sind der DEUmilSAA zu melden.

Dieser Approval to Operate ist gültig vom [ ] bis zum [ ] oder bis zu dem Zeitpunkt, an dem einer der in Bezug [ ] genannten Gründe für eine Re-Akkreditierung eintritt.

11.8.8 Muster für einen Informationssicherheitsbefehl Übung

(Einheit / Dienststelle) Schutzbereich:

Informationssicherheitsbefehl für die Übung X

Bezug:
1. (ggf.) Befehl vorgesetzte Dienststelle zur Übung
2. Übungsbefehl der eig. Dienststelle zur Übung
3. Regelung A-960/1 – Informationssicherheit in der Bundeswehr
4. Regelung A-961/1 – Kryptosicherheit in der Bundeswehr *[bei Bedarf, wenn Kryptosicherheit relevant]*
5. Regelung A-962/1 – Abstrahlsicherheit *[bei Bedarf, wenn Abstrahlsicherheit relevant]*
6. Informationssicherheitskonzept Dienststelle (InfoSichhKDSt)
7. Projektbezogenes Informationssicherheitskonzept (InfoSichhKProj) XXX Stand XX.XX.XXXX
8. *[weitere InfoSichhKProj bei Bedarf]*
9. *[weitere Bezüge bei Bedarf]*

Anlagen:
- A Bestellung Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte Übung (ISBÜb)
- B Informationssicherheitsbelehrung Nutzer
- C Verpflichtungserklärung Informationssicherheitspersona]
- D Freigaben
- *[E]* *[weitere Anlagen bei Bedarf]*

1. Lage

a) Die Übung X *[hier Bezeichnung / Name der Übung einfügen]* hat das Ziel, die Fähigkeit *[hier Übungszweck einfügen]* zu beüben. Die Übung X wird im Zeitraum vom XX.XX.XXXX bis zum XX.XX.XXXX als *[Art der Übung, z.B. Gefechtsstandübung]* durchgeführt.

b) Dieser Befehl regelt die übungsspezifischen Informationssicherheitsvorgaben für die Übung X und ergänzt somit die Vorgaben der zentralen Regelungen (Bezüge 3 bis 5) sowie der InfoSichhKDSt / InfoSichhKProj. Er dient gleichzeitig als Grundlage für die Einweisung, Belehrung und Verpflichtung des eingesetzten IT-Personals sowie der Nutzer und Bediener von IT.

2. Auftrag

Für die Übung X sind geeignete Maßnahmen gemäß der Bezüge 1. und 5. bis XX.XX.XXXX zur Sicherstellung der Informationssicherheit beim Umgang mit und der Lagerung der eingesetzten IT anzuwenden (siehe Nr. 3. c) (4) dieses Befehls).

3. Durchführung

a) Absicht

Absicht ist es, durch die Einhaltung der Vorgaben für die Informationssicherheit zur erfolgreichen Durchführung der Übung X beizutragen und die Handlungssicherheit des teilnehmenden Personals in

Bezug auf die Informationssicherheit zu gewährleisten.

b) Einzelaufträge

(1) **FF Kdo / Dienststellenleiter bzw. Dienststellenleiterin / Exercise Director /…**

- Ist / sind verantwortlich für die Informationssicherheit während der Übung X,
- bestimmen und bestellen ISBÜb sowie weiteres Informationssicherheitspersonal (z.B. Informationssicherheitsgehilfen für dislozierte Bereiche) für die Übung X (siehe Anlage A), der dem Verantwortlichen in allen Belangen der Informationssicherheit zuarbeitet,
- gibt mit der Freigabeverfügung (Anlage D), nach Empfehlung durch den verantwortlichen ISB, die entsprechende IT frei.

(2) **Abteilungen und selbstständige Dezernate**

- *[ggf. Benennung weiteren Informationssicherheitspersonals]*
- unterstützen ISBÜb in allen Belangen der Informationssicherheit.

(3) **Dienststellen, an der Übung beteiligte Einheiten, externe Teilnehmer etc.**

- *[ggf. Benennung weiteren Informationssicherheitspersonals]*
- unterstützen ISBÜb in allen Belangen der Informationssicherheit.

(4) **ISBÜb**

- erstellt Freigabeverfügungen und legt diese dem FF Kdo / Dienststellenleiter bzw. Dienststellenleiterin / Exercise Director zur Unterschrift vor,
- weist ein Kryptobeauftragten bzw. Kryptobeauftragte/ Vertreter bzw. Vertreterin und bereitet Dokumentation zur Bestellung durch FF Kdo / Dienststellenleiter bzw. Dienststellenleiterin / Exercise Director vor,
- führt durch Informationssicherheitsbelehrung im Rahmen der Einschleusung,
- dokumentiert und weist schriftlich oder per elektronischer Signatur die Informationssicherheitsbelehrung nach,
- ist im Übungszeitraum ständiger Berater der bzw. des Übungsleitenden,
- führt durch Kontrollen und meldet Informationssicherheitsvorkommnisse gemäß Bezug 3,
- *[bei Bedarf weitere übungsspezifische Aufträge für den ISBÜb].*

(5) **Kryptoverwalter**

- *[bei Bedarf übungsspezifische Aufträge zur Kryptosicherheit]*

(6) **Kryptobeauftragte *(bei Bedarf)***

- *[bei Bedarf übungsspezifische Aufträge zur Kryptosicherheit]*

(7) **IT-Beauftragte**

- *[bei Bedarf übungsspezifische Aufträge bzgl. IT-Material, Meldewesen etc.]*

(8) **Referat / Dezernat X, Informationsmanagement**

- *[bei Bedarf übungsspezifische Aufträge zur Bereitstellung von Netzplänen, Software- / Hardware-, Nutzer-, Rollen- / Rechteübersichten, IT-Meldewesen etc.]*

(9) **Sicherheitsbeauftragter**

- *[bei Bedarf übungsspezifische Aufträge zur Militärischen Sicherheit und zum Geheimschutz]*

(10) **Administrativer Datenschutzbeauftragter**

- *[bei Bedarf übungsspezifische Aufträge zum Datenschutz]*

(11) **IT-Btl / IT-Kräfte XY**

- *[bei Bedarf übungsspezifische Aufträge im Zusammenhang mit der Informationssicherheit]*

c) Organisation

(1) Informationsstruktur

Während der Übung X werden folgende Informationen verarbeitet und / oder übertragen:

[Informationsstruktur gemäß Nr. 210, Abbildung 3]

(2) Militärische Sicherheit

[bei Bedarf übungsspezifische Regelungen zur Militärischen Sicherheit, Absicherung dislozierter Bereiche, ggf. Verweis auf Absicherungsbefehl für die Übung]

(3) Eingesetzte IT

[bei Bedarf Einzelheiten zur eingesetzten IT und übungsspezifische Grundsätze zur eingesetzten IT hier festlegen]

(4) Übungsspezifische Informationssicherheitsmaßnahmen

a) Personelle Maßnahmen

[übungsspezifische Maßnahmen hier oder in Anlage aufführen]

b) Infrastrukturelle Maßnahmen

[übungsspezifische Maßnahmen hier oder in Anlage aufführen]

c) Organisatorische Maßnahmen

[übungsspezifische Maßnahmen hier oder in Anlage aufführen]

d) Technische Maßnahmen

[übungsspezifische Maßnahmen hier oder in Anlage aufführen]

4. Maßnahmen zur Koordinierung

[Maßnahmen hier aufführen]

5. Führungsunterstützung

a) Erreichbarkeiten Dienststelle X:

ISBÜb
Tel.: 90 XXXX XXXX
Mail: XXXX@bundeswehr.org

b) Erreichbarkeiten Übung, Ort (ab XX.XX.XXXX):

ISBÜb
Tel.: folgt.
Mail: folgt.

6. Verwaltungsbestimmungen

Entfällt

7. Personalrat

Der Personalrat wurde beteiligt.

8. Gültigkeitsdatum

Dieser Befehl verliert mit Ablauf des XX.XX.XXXX seine Gültigkeit und ist bis auf ein Dokumentationsexemplar des FF OrgE gemäß ZDv A-1130/2 VS-NfD zu vernichten.

Unterschriftsblock

Verteiler:

Anlage A (Bestellung zum Informationssicherheitsbeauftragten Übung (ISBÜb))

Gemäß Muster der Bestellung(en) Anlage 11.8.4.

Anlage B (Informationsicherheitssbelehrung)

Informationssicherheitsbelehrung für IT-Nutzer der Übung X

[Übungsspezifische Belehrungsinhalte, die über die regelmäßig jährlich durchzuführende Belehrung zur Informationssicherheit hinausgehen, sind in dieser Anlage aufzuführen. Übungsteilnehmer, die nicht der regelmäßig jährlich durchzuführenden Belehrung unterliegen, sind zusätzlich mit den darin enthaltenen Belehrungsinhalten zu belehren.]

Inhaltsverzeichnis:

1. Zuständiges Personal

Funktion	Name, DGrad	Abt.	App.
Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte Übung (ISBÜb)			folgt
stv Informationssicherheitsbauftragter Übung (stv ISBÜb			folgt
Sicherheitsbeauftragter (SichhBeauftr)			folgt
stv Sicherheitsbeauftragter (stv SichhBeauftr)			folgt
Administrativer Datenschutzbeauftragter (ADSB)			folgt

2. Weitere Inhalte bei Bedarf

3. Erklärung zur Kenntnisnahme

I. <u>Erklärung</u> zur Kenntnisnahme der Informationssicherheitsbelehrung (SecOPs):
Ich versichere, dass ich diese Belehrung vollständig gelesen und verstanden habe. Mir ist bewusst, dass die Bedingungen verpflichtend sind und dass ich mich an die beschriebenen Standards zwingend halten werde.

II. <u>Persönliche Nutzerdaten</u>:

Name, Vorname	
Dienstgrad	
Nation	
Übungsbeginn / Übungsende	
Datum, Unterschrift	

Abzugeben beim ISBÜb des XXX oder beim In-processing am Beginn der Übung.

III. Kenntnisnahme des ISBÜb:

Datum, NAME, DG, Unterschrift:	

Anlage C (Verpflichtungs- und Belehrungserklärung IT-Personal)

Gemäß Muster der Verpflichtungs- und Belehrungserklärung(en) Anlage 11.8.6.

Anlage D (Freigaben)

Muster der Freigabe sind der Formulardatenbank im INTRANETBw zu entnehmen.

11.9 Nutzerrichtlinien

11.9.1 Mobile IT

11.9.1.1 Nutzerrichtlinie – Sicherer Umgang mit Mobiler IT

Sicherer Umgang mit Mobiler IT[187]

Im GB BMVg wird sowohl **im Dienst mitgeführte private** als auch **dienstlich bereitgestellte** Mobile IT genutzt. Letztere wird dem IT-Anwender bzw. der IT-Anwenderin durch seinen bzw. ihren Dienstherrn / Arbeitgeber zur dienstlichen Verwendung bereitgestellt und durch diesen bzw. in dessen Auftrag betrieben. Aufgrund der vielfältigen Formen von Mobiler IT werden zur besseren Anwendbarkeit der nachfolgenden Bestimmungen und ohne Anspruch auf eine vollständige Abbildung aller denkbaren Anwendungsfälle aus technischer Sicht folgende Kategorien unterschieden:

- **Kategorie A:** Mobile IT (z. B. Notebooks, Smartphones) mit integrierten oder als Erweiterungsmodul (z. B. WLAN-Stick) durch den IT-Anwender bzw. die IT-Anwenderin aktivierbaren Kommunikationsschnittstellen zu öffentlichen Netzinfrastrukturen, mit der Möglichkeit zur automatisierten und über integrierte Mensch-Maschine-Schnittstellen (z. B. Tastatur, Maus) gesteuerten Dateneingabe, -speicherung oder -verarbeitung sowie der Dateneingabe über technische Sensorik (z. B. Mikrofon oder Kameraoptik bzw. GPS).
- **Kategorie B:** Mobile IT (z. B. speziell konfigurierte Notebooks, Scanner, Kameras) mit den Eigenschaften gemäß Kategorie A, jedoch ohne integrierte oder als Erweiterungsmodul durch den IT-Anwender bzw. die IT-Anwenderin aktivierbare Kommunikationsschnittstellen zu öffentlichen Netzinfrastrukturen.
- **Kategorie C:** Mobile IT (z. B. Speichersticks, DVDs, CDs) mit den Eigenschaften der Kategorie B, jedoch ohne Mensch-Maschine-Schnittstelle zur Steuerung der Dateneingabe und ohne Dateneingabe über technische Sensorik (Ausnahme: Schnittstellen zur Benutzerauthentisierung, wie Fingerprintsensor, PIN-Tastatur oder Verriegelungsvorrichtung).

[187] Dieses Formular ist mit Schutzbereich 1 zu versehen.

1. (**A / B / C) –** Private Mobile IT darf nicht mit dienstlicher IT und dienstliche Mobile IT nicht mit privater IT verbunden werden. Weiterhin ist die Verbindung zu öffentlichen kabelgebundenen Schnittstellen - außer über die zum Gerät gehörenden Stromversorgungsadapter - untersagt (z.B. USB-Ladestationen).
2. **(A / B / C) –** Das Einbringen privater und dienstlicher Mobiler IT in Sperrzonen, sowie die Nutzung von Foto-, Video- und Audioaufnahmefunktionen privater Mobiler IT zur Speicherung / Bearbeitung dienstlicher Informationen ist untersagt.
3. **(A / B / C) –** PINs (Personal Identification Number), Passworte, Chipkarten etc. sind bei der Mitnahme bzw. Nutzung von dienstlich bereitgestellter Mobiler IT sicher aufzubewahren bzw. zu verwenden.
4. **(A / B / C) –** Die Mitnahme (außerhalb der Dienststelle) von VS oder PersDat in elektronischer Form ist ausschließlich auf dienstlich bereitgestellter Mobiler IT im Rahmen der dienstlichen Notwendigkeit zulässig, sofern die betroffenen Dateien entsprechend ihrer Einstufung bzw. ihres Schutzbereichs (SB)[188] mit zugelassener bzw. geeigneter Verschlüsselungstechnik verschlüsselt sind.

   Auf eine Verschlüsselung kann im Ausnahmefall verzichtet werden, wenn die dienstlich bereitgestellte Mobile IT ständiger persönlicher Aufsicht unterliegt **und** lediglich einzelne für einen spezifischen Zweck erforderliche VS-NfD eingestufte Informationen bzw. PersDat mitgeführt werden.
5. **(A / B / C) –** Bei Verdacht auf Manipulation von dienstlich bereitgestellter Mobiler IT ist deren Nutzung einzustellen und umgehend der bzw. die SichhBeauftr und / oder der bzw. die ISB der Dienststelle zu informieren[189].
6. **(A / B / C) –** Bei Verlust / Diebstahl von dienstlich bereitgestellter Mobiler IT ist umgehend der bzw. die SichhBeauftr und / oder der bzw. die ISB der Dienststelle zu informieren.
7. **(A / B / C) –** Dienstlich bereitgestellte Mobile IT darf grundsätzlich nur mit Rechnern / Netzen des IT-SysBw verbunden werden bzw. Daten[190] austauschen. Ausnahme: Ist eine Verbindung bzw. ein Datenaustausch mit Fremdrechnern / -netzen unter Abwägung der Gefahr eines Datenverlustes aus dienstlichen Gründen unabdingbar, so ist die Mobile IT vor erneuter Anbindung bzw. erneutem Datenaustausch manuell oder automatisiert über geschützte Netzübergänge (z. B. Sicherheitsgateway, Schleusen PC) auf Schadsoftware zu überprüfen.

[188] Siehe Bezug Anlage 11.15 (LfdNr. 10)).
[189] Dieser bzw. diese prüft vor Absetzen einer Meldung, ob eine unverzügliche Beteiligung des MAD erfolgen muss (vgl. A-960/1 „Informationssicherheit“, Nr. 821; Das MAD ist unverzüglich über den bzw. die SichhBeauftr einzuschalten, wenn ein Hinweis auf extremistische / terroristische Bestrebungen oder sicherheitsgefährdende oder geheimdienstliche Tätigkeiten vorliegt).“
[190] außer Kurzmitteilungen (z. B. SMS, MMS)

8. **(A / B / C) –** Änderungen am übergebenen Konfigurationsstand der dienstlich bereitgestellten Mobilen IT sind nur nach Abstimmung mit der für den Betrieb der Mobilen IT verantwortlichen Stelle zulässig.
9. **(A / B / C) –** Bei der Aufbewahrung von dienstlich bereitgestellter Mobiler IT (z. B. im Rahmen von Dienstreisen oder im häuslichen Umfeld) ist der IT-Anwender bzw. die IT-Anwenderin zu besonderer Sorgfalt und Aufmerksamkeit verpflichtet, um Diebstähle oder unerkannte Manipulationen zu vermeiden. Sofern vorhanden, sind Möglichkeiten zur verschließbaren Aufbewahrung zu nutzen oder es ist zumindest eine sichtbare Lagerung zu vermeiden.
10. **(A / B) –** Bei der Nutzung dienstlich bereitgestellter Mobiler IT der Kategorien A und B sind immer die örtlichen Gegebenheiten zu berücksichtigen. Ist das Mithören oder die Einsichtnahme „Dritter“ nicht zu vermeiden, ist die Nutzung zu unterlassen.
11. **(A / B) –** Aufgrund der Ortungsmöglichkeiten, der Möglichkeiten zum Aufzeichnen von Bewegungsprofilen und der Abhörmöglichkeiten bei Mobiler IT der Kategorie A oder B sind in einem sicherheitsempfindlichen Umfeld die Vorgaben der jeweiligen Dienststellenleiter bzw. Dienststellenleiterin, Kontingentführer bzw. Kontingentführerin, Vorgesetzten bzw. Vorgesetzte und Verantwortungsträger bzw. Verantwortungsträgerin zum Mitführen Mobiler IT zu beachten.
12. **(A / B) –** Die Einbringung und / oder Nutzung von Mobiler IT der Kategorien A und B in Konferenzen / Besprechungen ist grundsätzlich erlaubt, sofern es nicht durch Hinweise / Anordnungen / Verbotsschilder oder durch die Konferenz- / Besprechungsleitung explizit untersagt wird.
13. **(A / B) –** Das Einbringen von Mobiler IT der Kategorien A und B in bestimmte Sicherheitsbereiche (z. B. DFmA[191], sonstige Sperrzonen) ist grundsätzlich untersagt. Entsprechende Hinweise / Anordnungen / Verbotsschilder sind zu beachten, Ausnahmegenehmigungen sind zu erfragen.
14. **(A) –** Bei Verlust / Diebstahl von dienstlich bereitgestellter Mobiler IT der Kategorie A ist unverzüglich die Sperrung des Mobilfunkanschlusses zu veranlassen:
    - Bei von der BWI verwalteter Mobiler IT unmittelbar unter:
      UHD BWI IT: **90-44444 (BMVg: 090-44444); 0800-44444-29**.
    - Bei nicht von der BWI verwalteter Mobiler IT ist der Help Desk des
      BtrbZ IT-SysBw anzurufen: **90-55555 (BMVg: 090-55555); 02226/882-4990**
      Zudem ist der bzw. die zuständige SichhBeauftr und / oder der bzw. die ISB der Dienststelle zu informieren.
15. **(A) –** Die Sprachübertragung von VS-NfD eingestuften Informationen oder PersDat mit dienstlich bereitgestellter Mobiler IT der Kategorie A ohne entsprechend zugelassene bzw. geeignete Verschlüsselung ist nur dann zulässig, wenn die Erledigung der Angelegenheit dringlich ist und die schriftliche oder sonstige sichere Übertragung einen unvertretbaren Zeitverlust bedeuten würde. Dabei sind die zu übertragenden Nachrichten / Informationen möglichst so abzufassen, dass sie

[191] Dienstbereich Fernmelde-Aufklärung

keinen unmittelbaren Rückschluss auf ihren VS- oder PersDat-Charakter zulassen. Die Sprachübertragung von Informationen des Geheimhaltungsgrades VS-VERTRAULICH und höher mit bereitgestellter mobiler IT der Kategorie A ist immer unzulässig.

_____

IT-Anwender bzw. IT-Anwenderin (Datum und Unterschrift)

11.9.1.2 Handlungshinweise für Vorgesetzte und Verantwortungsträger zum Umgang mit Mobiler IT im sicherheitsempfindlichen Umfeld

Die vorliegenden Handlungshinweise richten sich an Dienststellenleiter bzw. Dienststellenleiterin, Kontingentführer bzw. Kontingentführerin sowie alle Vorgesetzten bzw. Vorgesetzte und Verantwortungsträger bzw. Verantwortungsträgerin im Zusammenhang mit der Nutzung von Mobiler IT im sicherheitsempfindlichen Umfeld. Sie berücksichtigen Gefährdungen, die aus den Möglichkeiten der Ortung und Aufzeichnung von Bewegungsprofilen sowie durch Abhören oder Aufzeichnen von Gesprächen im Umfeld allein durch das Mitführen Mobiler IT der Kategorie A oder B erwachsen. Dabei umfasst Mobile IT in der Bw sowohl im Dienst mitgeführte private, als auch dienstlich bereitgestellte Mobile IT.

Das **Mitführen** von Mobiler IT ist in den folgenden Anwendungsszenarien **grundsätzlich zu untersagen:**

Szenario 1: Mobile IT der Kategorie A in Einsatzsituationen, wenn zum Schutz von Personen, Patrouillen, Gefechtsständen, Fahrzeugen usw. der Standort verdeckt zu halten ist.

Szenario 2: Mobile IT der Kategorie A im Bereich des Personenschutzes, wenn der jeweilige Aufenthaltsort unbedingt verschleiert bleiben muss.

Szenario 3: Mobile IT der Kategorien A oder B bei Konferenzen / Dienstbesprechungen, wenn geheimhaltungsbedürftige Inhalte (VS-VERTRAULICH oder höher sowie vergleichbare NATO- / EU-Einstufungen bzw. Einstufungen anderer Nationen, sonstiger überstaatlicher Organisationen oder „MISSION“[192] oder besonders sensitive Gesprächsinhalte[193], die nicht eingestuft werden dürfen) besprochen werden.

In Zweifelsfällen, wenn z. B. die Eignung bestimmter Mobiler IT hinsichtlich der Ausnahmen im konkreten Fall nicht verifiziert werden kann, ist in allen genannten Szenarien das Mitführen der Mobilen IT zu untersagen.

Ausnahmen:

Das Mitführen der Mobilen IT kann in allen genannten Szenarien erlaubt werden, wenn eine Notsituation vorliegt bzw. eine Trennung von der Stromversorgung möglich ist und diese Trennung zuverlässig vorgenommen wurde.

[192] „MISSION“ ist der Platzhalter für eine spätere konkrete Benennung und setzt eine sog. *Security Policy* für den beabsichtigten Einsatz voraus. Insofern ist z.B. MISSION SECRET keine gültige Einstufung, sondern z. B. NATO / ISAF SECRET oder NATO SECRET Releasable to ISAF.

[193] Der bzw. die verantwortliche Besprechungsleiter bzw. Besprechungsleiterin, entscheidet über die Geheimhaltungsbedürftigkeit der Gesprächsinhalte einer Besprechung auf der Grundlage der Vorgaben gemäß A-1130/2 VS-NfD „Militärische Sicherheit in der Bundeswehr - Verschlusssachen“ (siehe Bezug Anlage 11.15 (LfdNr. 15). Im Falle von „besonders sensitiven Gesprächsinhalten“, die nicht eingestuft werden dürfen, entscheidet er bzw. sie im Einzelfall nach eigenem Ermessen.

Das Mitführen der Mobilen IT kann im Szenario 3 erlaubt werden, wenn dieses Szenario in den Zulassungsbestimmungen für die Mobile IT explizit enthalten ist, darin das Mitführen oder die Nutzung als zulässig bewertet wurde und die Regelungen der Zentralen Dienstvorschrift A-1130/2 VS-NfD „Militärische Sicherheit in der Bundeswehr - Verschlusssachen“ (siehe Bezug Anlage 11.15 (lfdNr. 15 darin Anlage B-10) eine Ausnahme zulassen.

11.9.2 Nutzerrichtlinie – Zehn Regeln zur Informationssicherheit am Arbeitsplatz

Zehn Regeln zur Informationssicherheit (InfoSichh) am Arbeitsplatz[194]

1. Informieren Sie sich, wer Ihr zuständiger ISB bzw. Ihre zuständige ISB, Sicherheitsbeauftragter bzw. Sicherheitsbeauftragte, Administrator bzw. Administratorin, Nutzerbetreuer bzw. Nutzerbetreuerin und Verantwortlicher bzw. Verantwortliche für den Schutz von PersDat ist.

	DGrad / ABez	Name	Einheit	Gebäude	Telefon
ISBDSt					
Nutzerbetreuer					
ADSB					

2. Informieren Sie sich darüber hinaus regelmäßig über aktuelle Regelungen mit Informationssicherheitsbezug (siehe dazu den Intranetauftritt http://infosichh.bundeswehr.org, „Fachinformationen / Regelungen“).

3. Versuchen Sie nicht, Informationssicherheitsprobleme ohne die Hilfe der unter 1. genannten Rollenträgerinnen und Rollenträger zu lösen. Melden Sie alle informationssicherheitsrelevanten Vorfälle unverzüglich dem bzw. der ISBDSt.

4. Beachten Sie die Bestimmungen zu Verschlusssachen (Zentrale Dienstvorschrift A-1130/2 VS-NfD „Militärische Sicherheit in der Bundeswehr - Verschlusssachen“), wenn Sie mit diesen Informationen umgehen. Achten Sie auf die Einhaltung der gesetzlichen Bestimmungen des Bundesdatenschutzgesetzes, der A-2122/4 „Datenschutz“ und der sonstigen datenschutzrechtlichen Regelungen, wenn Sie PersDat erheben, verarbeiten und nutzen.

5. Geben Sie niemals Ihr persönliches Passwort weiter. Verhindern Sie, dass andere auf Ihre IT-Ausstattung und Datenträger und somit auf Ihre Informationen zugreifen können. Das gilt vor allem bei – auch kurzfristigem – Verlassen des Arbeitsplatzes.

6. Schützen Sie IT-Gerät und Datenträger vor Beschädigung, Verlust, Diebstahl und unbefugter Nutzung.

7. Stellen Sie sicher, dass jede ONLINE / OFFLINE empfangene Datei und jeder Datenträger vor der Nutzung mit dem dienstlich beschafften Virensuchprogramm geprüft wurde. Melden Sie Anomalien unverzüglich dem bzw. der ISBDSt. Schalten Sie bei auftretenden Anomalien Ihren PC nicht aus.

8. Der Einsatz privater Hard- und Software zu dienstlichen Zwecken ist grundsätzlich verboten. Dienstliche Hard- und Software darf nur zu dienstlichen Zwecken genutzt werden.

[194] siehe FormulardatenbankBw - Formularnummer Bw/2939, Schutzbereich 1

9. Speichern Sie Ihre Daten immer im Ihnen zugewiesenen Netzlaufwerk, da hier eine regelmäßige Datensicherung durchgeführt wird. Haben Sie einen mobilen Arbeitsplatzrechner, speichern Sie die von Ihnen während der Trennung vom Netz erstellten / geänderten Daten nach Wiederanschluss an das Netz immer im Ihnen zugewiesenen Netzlaufwerk. Falls Ihr Arbeitsplatz nicht vernetzt ist und Sie daher Ihre Daten ständig auf einer lokalen Festplatte ablegen müssen, führen Sie regelmäßig Datensicherungen durch. Lagern Sie Sicherungskopien möglichst nicht in Ihrem Arbeitszimmer, sondern baulich getrennt von Ihrem Arbeitsplatz.

10. Alle Bestimmungen gelten auch für bewegliche IT. Schützen Sie diese besonders beim Einsatz außerhalb der Dienststelle vor Beschädigung, Verlust, Diebstahl und unbefugter Nutzung.

11.10 Weisung zur Löschung / Vernichtung von eingestuften Datenträgern

11.10.1 Allgemeines

1. Für das Löschen und Vernichten von Verschlusssachen auf Datenträgern jeglicher Art ist die Technische Leitlinie des BSI TL 03420 „Leitlinie für das Löschen und Vernichten von Verschlusssachen auf Datenträgern“[195] (siehe Bezug Anlage 11.15 (lfdNr. 56)) in seiner aktuellen Fassung **bindend**.

2. Die zuständigen Rollenträgerinnen und Rollenträger in allen Anwendungsbereichen (siehe Nr. 402), die IT für die Nutzung bereitstellen (z.B. in Projekten), sind im Rahmen ihrer Verantwortlichkeit für den gesamten Lebenszyklus („von der Wiege bis zu Bahre“) auch dafür zuständig, einen regelkonformen Weg zur Löschung / Vernichtung der in ihrem System genutzten, eingestuften Datenträger aufzuzeigen und dies im InfoSichhK zu dokumentieren.

3. Für die Vernichtung von VS des Geheimhaltungsgrades VS-VERTRAULICH und höher macht die Zentrale Dienstvorschrift A-1130/2 VS-NfD „Militärische Sicherheit in der Bundeswehr - Verschlusssachen“ (siehe Bezug Anlage 11.15 (lfdNr. 15), dort Abschnitt 14) zusätzliche Vorgaben organisatorischer und personeller Art, die bei einer Vernichtung durch die Dienststelle zu beachten sind und bei einer Vernichtung durch Firmen eine Mitwirkung der Dienststelle erfordert.

4. Häufig liegt die Umsetzung der Maßnahmen für die Löschung / Vernichtung von Datenträgern bei der nutzenden Dienststelle.

5. Zur Durchführung / Unterstützung können Dienstleistungsverträge über die jeweils zuständigen BwDLZ abgeschlossen werden.

6. Rücklieferungen von Krypto- / VS-Material zur Aussonderung und Verwertung sind ab sofort an das MatLgr NECKARZIMMERN und nicht mehr an das MatLgr WEENER zu steuern.

11.10.2 Rahmenvertrag

7. Unter der Vertragsnummer B/T1AV/IA062/3V001 wurde durch das BAAINBw am 10. Oktober 2018 bereitet ein Rahmenvertrag geschlossen, der die **Vernichtung** ausgesonderter Kryptogeräte und jeglicher eingestufter VS-Datenträger den Regeln der TL 03420 entsprechend für den GB BMVg ermöglicht. Die Laufzeit dieses Vertrages beläuft sich auf drei Jahre ab Vertragsunterzeichnung.

8. Um Leistungen aus diesem Rahmenvertrag in Anspruch zu nehmen, veröffentlicht BAAINBw T2.5 für logistischen Bereiche entsprechende Informationen zur Verwertung im INTRANETBw unter http://baainbw/ain im Bereich „Fachinformationen / Aussonderung und Verwertung“.

[195] http://infosichh.bundeswehr.org im Bereich „Fachinformationen / BSI / Technische Leitlinien“

11.11 Begriffsbestimmungen

Allgemeine Typzulassung / Produktzulassung	Eine Produktzulassung kann für IT-Sicherheitsprodukte für allenationalen Geheimhaltungsgrade ausgesprochen werden. Das BSI kann Zulassungen bis NATO CONFIDENTIAL bzw. CONFIDENTIEL UE / EUCONFIDENTIAL aussprechen, sofern die Produkte die NATO bzw. EU Anforderungen erfüllen. Zulassungen für Produkte, die über den genannten Zulassungsgraden liegen, können nur durch die NATO bzw. die EU auf Antragund unter Beteiligung des BSI erteilt werden. Es gibt Unterschiede zwischen deutschen, NATO- und EU-Anforderungen.Deshalb sind manche Produkte, die für nationale VS zugelassen sind, nichtfür EU Cryptographic Items (CI) und/oder NATO CI zulassungsfähig oder umgekehrt. Generell gilt: Das zugelassene Produkt ist allgemein nur im Rahmen der mitder Zulassung erteilten Auflagen (Einsatz- und Betriebsbedingungen/COMSECDoctrine/SecOps) einsetzbar. Die Produktzulassung ist grundsätzlich zeitlich befristet, ggf. mit einer längeren Laufzeit.
Amtsverschwiegenheit	Alle dienstlichen Angelegenheiten (auch für nicht eingestufte Informationen) unterliegen der **Amtsverschwiegenheit** (für Soldaten bzw. Soldatinnen gemäß § 14 Soldatengesetz, für Beamte bzw. Beamtinnen gemäß § 61 Bundesbeamtengesetz). Ob und in welchem Umfang eine der Pflicht zur Verschwiegenheit unterworfene Information zur Weitergabe / Veröffentlichung freigegeben werden kann, entscheidet die herausgebende Stelle der Information unter Berücksichtigung der dienstlichen Notwendigkeit. Die Verletzung der Verpflichtung zur Verschwiegenheit kann u. a. disziplinarrechtliche, arbeitsrechtliche und strafrechtliche Konsequenzen nach sich ziehen.
Angriff	Ein **Angriff** ist ein bewusst herbeigeführter und unberechtigter Zugriff auf Informationen in IT sowie unberechtigter Zugang zur IT mit dem Ziel, die Informationssicherheit zu brechen. Die Grundwerte der Informationssicherheit Vertraulichkeit,

	Verfügbarkeit und Integrität können dabei als Teil oder als Ganzes verletzt sein. Gleiches gilt für die Gewährleistungsziele.
Auditing	Im Bereich der Informationssicherheit versteht man unter **Auditing** eine regelmäßige oder ereignisbezogene Prüfung und Auswertung von Protokolldaten der IT bzgl. Einhaltung festgelegter Regeln und Vorgaben.
Außentäter	Täter bzw. Täterin, der bzw. die keinen genehmigten Zugang zu bzw. Zugriff auf Einrichtungen, Systeme(n), Geräte(n) und Informationen besitzt, jedoch durch Spionage oder Sabotage auf sie einwirkt. Daneben gibt es Täter, die aus kriminellen Gründen (auch organisierte Kriminalität), Frustration, Eigennutz oder Selbstdarstellung in IT eindringen.
Authentisierung	Vorgang des Nachweises der eigenen Identität. **Anmerkung:** Im Englischen wird zwischen Authentisierung und Authentifizierung (authentication) nicht unterschieden. Dementsprechend werden die beiden Ausdrücke im Deutschen oft (ungenau) synonym verwendet. Im Deutschen wird mit Authentifizierung in der Regel der Nachweis einer behaupteten Eigenschaft bezeichnet, die Authentisierung bezeichnet in der Regel den Vorgang des Nachweises der behaupteten Eigenschaft mit dem Ergebnis einer Erlaubnis oder eines Verbotes, bestimmte Aktionen durchzuführen.
Datenauslagerung	Unter **Datenauslagerung** werden alle Verfahren verstanden, bei denen aktuell nicht mehr benötigte Daten aus operationeller IT zum Zweck der Entlastung der operationellen IT bei gleichzeitiger Gewährleistung ihrer weiteren Verfügbarkeit entnommen werden.
Datensicherung	Unter **Datensicherung** (auch Backup) versteht man das teilweise oder gesamte Kopieren der in IT vorhandenen Daten auf ein alternatives (häufig transportables) Speichermedium. Die auf dem Speichermedium gesicherten Daten werden als Sicherungskopie bezeichnet. Das Ziel ist, den Datenverlust bei Systemausfällen zu begrenzen.

Echtdaten	**Echtdaten** sind Livedaten, die nicht pseudonymisiert bzw. anonymisiert sind.
Einzelzulassung	Eine **Einzelzulassung** kann für IT-Sicherheitsprodukte für alle deutschenVS-Gradeausgesprochen werden. NATO- und EU-Vorschriften sehen keineEinzelzulassung vor. Die **Einzelzulassung** ist auf ein bestimmtesEinsatz-Szenario beschränkt und berücksichtigt die in diesemZusammenhang realisierten IT-Sicherheits-Maßnahmen. Eine Einzelzulassung ist zeitlich kürzer befristet und wird ausgesprochen, wenn das Produktnicht alle Sicherheitsleistungen für eine allgemeine Einsetzbarkeiterfüllt. In Abhängigkeit vom Einsatz-Szenario verbleiben Risiken.
Fernwartung	Unter **Fernwartung** versteht man den Fernzugriff von technischem Personal auf Systeme zu Wartungs- und Reparaturzwecken. Unter **externer Fernwartung** wird die Durchführung der Arbeiten an IT der Bw durch Dritte, z. B. durch vertraglich hierzu verpflichtete Auftragnehmer, verstanden (keine Betriebsaufgaben). Bei **interner Fernwartung** handelt es sich um Fernwartung durch Bundeswehrangehörige.
Freigabeempfehlung	Eine **Freigabe-Empfehlung** ist die Empfehlung des BSI für den Einsatz eines IT-Sicherheitsproduktes für deutsche VS in schriftlicher Form. Die Projektleitung bzw. die Dienststellenleitung kann in eigener Verantwortung die Freigabe für seinen Verantwortungsbereich erteilen. Eine Freigabe-Empfehlung inklusive Risikobewertung wird i.d.R. vom BSI erstellt, wenn für das benötigte Einsatzszenario (noch) kein zugelassenes Produkt existiert. Die Grundlage einer Freigabe ist §36 der VSA.
Fremdnetz	Siehe Netzübergang
Gefährdung	Eine **Gefährdung** ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt (oder seines Umfeldes) einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene

	Schwachstelle zur Gefährdung für ein Objekt mit der Möglichkeit des Eintretens eines Schadens.
Informationsraum	Der **Informationsraum** ist der Raum, in dem Informationen generiert, verarbeitet, verbreitet, diskutiert und gespeichert werden. Ein wirkungsvolles Informationsmanagement mit der Möglichkeit zur ebenengerechten Filterung, Maßnahmen zur Zugriffskontrolle und einer bedarfsgerechten Darstellung sind unabdingbare Voraussetzung für die Nutzung dieses Informationsraums insbesondere für die vernetzte Operationsführung (NetOpFü).
Informationssicherheitsfunktion	Bei einer **InfoSichh-Funktion** handelt es sich um in IT implementierte technische InfoSichh-Maßnahmen (Hard- / Software).
Informationssicherheitslücke	Eine **InfoSichh-Lücke** liegt vor bei drohendem Verlust mindestens eines Grundwertes der Informationssicherheit oder eines Gewährleistungszieles durch unzureichende Umsetzung bestehender Vorgaben und Maßnahmen der InfoSichh oder dem Bekanntwerden einer neuen Gefährdung, der nicht zeitnah mit angemessenen InfoSichh-Maßnahmen begegnet werden kann.
Informationssicherheitspersonal	Personen, die mit der Herstellung und Überwachung der Informationssicherheit beauftragt sind, werden als **InfoSichh-Personal** bezeichnet. Hierzu zählen u. a.: • ISB, • Informationssicherheitsgehilfen, • InfoSichh-Auditoren, • Kryptopersonal[196] und • Fachpersonal der zentralen InfoSichhOrg.
Informationssicherheitsverfahren	Unter **InfoSichh-Verfahren** werden im Rahmen dieser Zentralen Dienstvorschrift die Prozesse und die darin durchzuführenden Tätigkeiten im Rahmen der Evaluierung, Zertifizierung, Zulassung und Anerkennung von InfoSichh-Produkten, der Akkreditierung, der Freigaben zur Nutzung von IT und der Bestellung von Informationssicherheitsbeauftragten verstanden.

[196] Personal, welches zum Umgang mit Kryptomitteln ermächtigt ist.

Informationssicherheitsverstoß	Ein **InfoSichh-Verstoß** liegt vor bei eingetretenem und vermutetem Verlust mindestens eines Grundwertes der Informationssicherheit oder eines Gewährleistungszieles.
Informationssicherheitsvorkommnis	Ein **InfoSichhVork** liegt vor, wenn die InfoSichh durch • eine Informationssicherheitslücke, • einen Informationssicherheitsverstoß oder • ein Sicherheitsvorkommnis im Kryptowesen beeinträchtigt bzw. gefährdet wird.
Informationstechnik	**Informationstechnik (IT)** umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen. IT-Systeme, IT-Produkte oder Systeme mit IT-Anteilen werden ebenfalls unter diesem Begriff zusammengefasst.
Innentäter	Täter bzw. Täterin, der bzw. die einen nicht genehmigten Zugang zu und Zugriff auf zumindest Teile von Einrichtungen, Systeme(n), Geräte(n) und Informationen hat. Seine bzw. ihre Tatmotive können neben Sabotage oder Spionage solche sein wie Frustration, Eigennutz, kriminelle Gründe (auch organisierte Kriminalität) und Selbstdarstellung.
Integrität	**Integrität** ist der Zustand, der unbefugte und unzulässige Veränderungen von Informationen in / an IT oder -Komponenten oder bei der Übertragung ausschließt oder erkennbar macht bzw. in dem geforderte oder zugesicherte Eigenschaften oder Merkmale von Informationen und Übertragungsstrecken sowohl für die IT-Anwender und -Anwenderinnen eindeutig feststellbar als auch Dritten gegenüber beweisbar sind.
IT-Abschirmung MAD	IT-Abschirmung ist Teil des durch den MAD zu erfüllenden gesetzlichen Abschirmauftrages für die Bw und umfasst alle Maßnahmen zur Abwehr von extremistischen / terroristischen Bestrebungen sowie sicherheitsgefährdenden oder nachrichtendienstlichen Tätigkeiten im Cyber- und Informationsraum. Die

	IT-Abschirmung trägt damit wesentlich zum Schutz der Informationssicherheit in der Bw bei. Zur Erfüllung ihrer Aufgaben sind die Verantwortlichen der Informationssicherheit und des MAD auf eine vertrauensvolle Zusammenarbeit angewiesen.
IT-Anwender	Vom Personenkreis der IT-Fachkräfte abzugrenzen sind **IT-Anwender**, die zur Wahrnehmung ihrer jeweiligen Aufgaben lediglich die zur Verfügung gestellte IT-Ausstattung benutzen. In dieser Zentralen Dienstvorschrift wird bei der Anwendung von IT von Nutzung gesprochen.
IT-Fachkräfte	Personal, das in der Informationstechnik (IT) tätig ist und IT-Management- / IT-Administrations- oder IT-Ausbildungsaufgaben wahrnimmt, gehört zu den **IT-Fachkräften**. Dies sind vor allem: • IT-Administratoren, • InfoSichh-Personal, • IT-Ausbilder, • IT-Verantwortliche, • IT-Koordinatoren, • IT-Führungspersonal, • IT-Betriebspersonal. Dienststellenleiter bzw. Dienststellenleiterinnen, Kommandeure bzw. Kommandeurinnen sowie sonstige Vorgesetzte und die IT-Anwender bzw. IT- Anwenderinnen gehören nicht zu den IT-Fachkräften.
IT-Governance	**IT-Governance** dient der Steuerung der IT. Sie besteht aus Führung, Organisationsstrukturen und Prozessen und liegt in der Gesamtverantwortung des CIO.
IT-Personal	**IT-Personal** umfasst militärische und zivile IT-Fachkräfte aller OrgBer, die Aufgaben in den Bereichen Konzeption, Beschaffung, Nutzung, Einsatz, Betrieb und Weiterentwicklung von IT im GB BMVg wahrnehmen.
IT-Risikolandkarte	**IT-Risikolandkarte** mit der Mittels einer Risikomatrix, die Wahrscheinlichkeit des Auftretens eines unerwünschten

	Ereignisses (dem Risiko) gegenüber dessen Auswirkung tabellarisch ins Verhältnis gesetzt.
IT-Risikomanagement	**IT-Risikomanagement** erkennt, analysiert, bewertet und überwacht die verschiedenen IT-Risiken. Es begleitet den gesamten System-Lebenszyklus der IT und stellt Gegenmaßnahmen oder Notfallpläne für verschiedene Szenarien bereit. Der BSI-Standard 200-3 bildet hierbei die Grundlage.
IT-Risikomanager	**IT-Risikomamager** koordiniert die Aktivitäten zur Lenkung und Steuerung seines Anwendungsbereiches in Bezug auf Risiken.
IT-System der Bundeswehr	Das **IT-SysBw** umfasst als ganzheitliches System die personellen, organisatorischen, infrastrukturellen und materiellen Elemente zur Weiterentwicklung und Einsatz / Betrieb der durch die Bw genutzten Informationstechnik einschließlich des führungsrelevanten IT-Anteils in Waffensystemen / Systemen.
Sicherheitsvorkommnis im Kryptowesen	Ein **Sicherheitsvorkommnis im Kryptowesen** liegt vor, wenn Sicherheitsvorschriften, Betriebsanweisungen und Sicherheitsbestimmungen im Kryptowesen nicht beachtet werden. Bei Vorliegen eines Sicherheitsvorkommnisses im Kryptowesen ist gemäß den Vorgaben der Zentralen Dienstvorschrift A-961/1 VS-NfD „Kryptosicherheit in der Bundeswehr“ zu verfahren. Sind NATO-Kryptomittel betroffen, sind zusätzlich die Vorgaben der SDIP 293/1 NATO RETRICTED „Instructions for the control and safeguarding of NATO cryptomaterial“ zu beachten.
Mobile IT	Aufgrund der vielfältigen Formen von **Mobiler IT** werden zur besseren Anwendbarkeit der nachfolgenden Bestimmungen und ohne Anspruch auf eine vollständige Abbildung aller denkbaren Anwendungsfälle aus technischer Sicht folgende Kategorien unterschieden: **Kategorie A:** Mobile IT (z. B. Notebooks, Smartphones) mit integrierten oder als Erweiterungsmodul (z. B. WLAN-Stick) durch den IT-Anwender bzw. die IT-Anwenderin aktivierbaren Kommunikationsschnittstellen zu öffentlichen Netzinfrastrukturen, mit der Möglichkeit zur automatisierten und über integrierte Mensch-Maschine-Schnittstellen (z. B. Tastatur,

	Maus) gesteuerten Dateneingabe, -speicherung oder -verarbeitung sowie der Dateneingabe über technische Sensorik (z. B. Mikrofon oder Kameraoptik). **Kategorie B:** Mobile IT (z. B. speziell konfigurierte Notebooks, Scanner, Kameras) mit den Eigenschaften gemäß Kategorie A, jedoch ohne integrierte oder als Erweiterungsmodul durch den IT-Anwender bzw. die IT-Anwenderin aktivierbare Kommunikationsschnittstellen zu öffentlichen Netzinfrastrukturen. **Kategorie C:** Mobile IT (z. B. Speichersticks, DVDs, CDs) mit den Eigenschaften der Kategorie B, jedoch ohne Mensch-Maschine-Schnittstelle zur Steuerung der Dateneingabe und ohne Dateneingabe über technische Sensorik (Ausnahme: Schnittstellen zur Benutzerauthentisierung, wie Fingerprintsensor, PIN-Tastatur oder Verriegelungsvorrichtung).
Netzkopplung	Mit **Netzkopplung** ist die Verbindung zweier (Teil-)Netze über beliebige dazwischen geschaltete (eines oder mehrere) Transportnetze gemeint.
Netzkopplungspunkt	Bei der Netzkopplung ist der **Netzkopplungspunkt** die Schnittstelle zwischen dem eigenen Netz und dem Transportnetz.
Netzübergang	In IT-Netzen bildet ein **Netzübergang** die Schnittstelle zwischen zwei unterschiedlichen Netzwerken. Eine solche Schnittstelle passt auf den jeweiligen Schichten des OSI 7-Schichten-Modells je nach Funktionsumfang die physikalischen Übertragungsmedien sowie die Netzwerk-, Transport- und Anwendungsprotokolle an. In der Regel wird ein solcher Netzübergang von einem Gateway gebildet. Unter **externen** Netzübergängen werden alle Übergänge zwischen dem IT-SysBw und Fremdnetzen verstanden, d. h. IT-Netzen, die nicht in Verantwortung der Bw liegen oder durch die BWI IT im Auftrag der Bw betrieben werden. Sie werden für den Austausch von Informationen zwischen der Bw und Externen benötigt und sind in weiten Bereichen operativ notwendig.

	Netzübergänge innerhalb des IT-SysBw werden als **interne** Netzübergänge bezeichnet. Grundsätzlich werden die Übergänge zu Fremdnetzen **zentral** über Demilitarisierte Zonen (DMZ) geführt. Als zentrale DMZ sind die Übergänge in Strausberg und Porz-Wahn eingerichtet. Alle weiteren Übergänge werden als **dezentrale** Netzübergänge betrachtet. Weitere zentrale Netzübergänge werden auf Antrag des Betreibers eines Netzüberganges zu Fremdnetzen durch den bzw. die CISOBw genehmigt und im Intranet Bw unter http://infosichh.bundeswehr.org bekannt gegeben.
Nutzer	Siehe IT-Anwender.
Revisionssichere Protokollierung	Sichere, unveränderbare und vollständige Speicherung von Protokolldaten, um Sachverhalte verlustfrei reproduzier- und recherchierbar zu erhalten mit dem möglichen Ziel der späteren gerichtsverwertbaren Auswertung sicherheitsrelevanter Ereignisse.
Risiko	Ein **Risiko** ist die Kombination, aus der Wahrscheinlichkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens. Im Unterschied zu „Gefährdung“ umfasst der Begriff „Risiko“ bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.
Rolle	Der Begriff **Rolle** bezeichnet Personen mit besonderen Funktionen in der IT oder der Informationssicherheit (z. B. Administratoren, Auditoren oder ISB) bzw. die konkrete Aufgabe einer Person im Kontext der betrachteten IT.
Rot	Gemäß SDIP 29-1, Nr. 3.1.1 (siehe Bezug Anlage 11.15 (lfdNr. 34)) Bezeichnung nach dem Rot / Schwarz-Prinzip für • Leitungen, die schutzbedürftige Informationen oder Signale ungeschützt übertragen, • Geräte oder Systeme, die schutzbedürftige Informationen oder Signale ungeschützt verarbeiten oder speichern, • Geräte, die einen Übergang zwischen Rot und Schwarz bilden (z. B. Sicherheitsgateways) sowie

	• Bereiche, in denen sich diese Leitungen, Systeme oder Geräte mit ihren Verbindungs- und Zusatzeinrichtungen befinden.
Rot / Schwarz-Prinzip	Prinzip gemäß SDIP 29-1, Nr. 3.1.1 (siehe Bezug Anlage 11.15 (lfdNr. 34)) nach dem Leitungen, Bauteile, Geräte, Systeme etc., die als VS eingestufte Informationen oder Signale unkryptiert übertragen oder verarbeiten (rot), von solchen getrennt werden, die kryptierte oder nicht als VS eingestufte Informationen oder Signale verarbeiten oder übertragen (schwarz). Das Rot / Schwarz-Prinzip wird benutzt, um spezielle Maßnahmen für die Zuordnung und Abgrenzung der genannten Einrichtungen sowie der Bereiche zu verdeutlichen, in denen sie sich befinden.
Schaden	Ein **Schaden** im Sinne dieser Zentralen Dienstvorschrift ist der Verlust oder die Minderung von mindestens einem der drei Grundwerte bzw. eines der Gewährleistungsziele der Informationssicherheit mit der Folge möglicher negativer Auswirkungen auf das IT-SysBw (einschließlich eines möglichen Ansehensverlustes in der Öffentlichkeit).
Schwachstelle	Eine **Schwachstelle** ist ein sicherheitsrelevanter Fehler in der IT oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird bzw. die Informationssicherheit nicht mehr gegeben ist. Eine Schwachstelle entsteht auch immer dann, wenn zu einer möglichen Gefährdung keine hinreichend wirksamen InfoSichh-Maßnahmen existieren oder umgesetzt werden.
Schwarz	Gemäß SDIP 29-1, Nr. 3.1.1 (siehe Bezug Anlage 11.15 (lfdNr. 34)) Bezeichnung nach dem Rot / Schwarz-Prinzip für • Leitungen, die schutzbedürftige Informationen oder Signale kryptiert oder nicht schutzbedürftige Informationen oder Signale übertragen,

	• Geräte oder Systeme, die schutzbedürftige Informationen oder Signale kryptiert oder nicht schutzbedürftige Informationen oder Signale verarbeiten oder speichern sowie • Bereiche, in denen keine schutzbedürftigen Informationen oder Signale auftreten.
Sicheres IT-Umfeld	Das **Sichere IT-Umfeld** umfasst organisatorische, personelle und infrastrukturelle InfoSichh-Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen im unmittelbaren Umfeld der betrachteten IT. Übergeordnete Maßnahmen zum Schutz der IT-Betriebsumgebung vor Sabotage, Umwelteinflüssen, Ausfall von Versorgungssystemen und zur Bereitstellung von vertrauenswürdigem und ausgebildetem Personal sind nicht Bestandteil des sicheren unmittelbaren IT-Umfeldes.
Sicherheitsgateway	Gemäß IT-Grundschutz des BSI (Baustein B 3.301) ist ein **Sicherheitsgateway** (oft auch Firewall genannt) ein System aus soft- und hardwaretechnischen Komponenten, um IP-Netze sicher zu koppeln. Dazu wird die technisch mögliche auf die in einer IT-Sicherheitsleitlinie ordnungsgemäß definierte Kommunikation eingeschränkt. Sicherheit bei der Netzkopplung bedeutet hierbei die ausschließliche Zulassung erwünschter Zugriffe oder Datenströme zwischen verschiedenen Netzen. Die Verwendung des Begriffs Sicherheitsgateway soll verdeutlichen, dass zur Absicherung von Netzübergängen heute oft nicht mehr ein einzelnes Gerät (z.B. Firewall) verwendet wird, sondern eine ganze Reihe verschiedener IT, die unterschiedliche Aufgaben übernimmt. Beispiele sind: • Firewall (Paketfilter, Application Layer Gateway) zur Kontrolle des Datenstroms auf Paket- bzw. Applikationsebene, • Virenschutz, • Authentifizierung zur Berechtigungsprüfung, • Protokollierung zur Dokumentation der übertragenen Daten, • Datendiode zur Einschränkung des Datenstroms, • Labelling zur Kontrolle der übertragenen Daten und • IDS / IPS zur Überwachung des Netzverkehrs.

Technische Informationssicherheit	Technische Informationssicherheit umfasst technische Maßnahmen • zum Schutz der IT bzw. der mit ihr zu verarbeitenden und zu übertragenden Informationen vor unberechtigten Zugriffen (**Vertraulichkeit**) und unberechtigten Veränderungen sowie zum Schutz der Beweisbarkeit und Echtheit (**Integrität**) sowie • der zeitgerechten und vollständigen Bereitstellung der Information (**Verfügbarkeit**).
Tolerierbares Risiko	Ein Risiko (siehe dort) gilt als **tolerierbar**, wenn der Aufwand zur Minimierung des Risikos durch Realisierung weiterer InfoSichh-Maßnahmen in keinem angemessenen Verhältnis zum Schutzbedarf der Informationen und damit zu dem möglicherweise eintretenden Schaden steht.
Verfügbarkeit	**Verfügbarkeit** ist der Zustand, der die erforderliche und zugesicherte Nutzbarkeit von Informationen sowie der IT sicherstellt.
Vertraulichkeit	**Vertraulichkeit** ist der Zustand, der unbefugte Informationsgewinnung / -beschaffung ausschließt.
Wechseldatenträger	Ein **Wechseldatenträger** im Sinne dieser Zentralen Dienstvorschrift ist mobile IT der Kategorie C.
Zugang	Einleitung der Nutzung von IT oder eines Kommunikationsnetzes. Der Zugang kann über Leitungen, Terminals und Geräte (physikalischer Zugang) oder durch Programme (logischer Zugang) erfolgen.
Zugriff	Die Benutzung von Informationen in IT im Sinne von Lesen, Schreiben, Ändern, Löschen direkt und / oder über Kommunikationswege (Netze) bzw. das Ausüben von Rechten auf IT-Ressourcen und -Anwendungen.
Zulassung, allgemein	Die Zulassung ist eine formale Genehmigung für die Verwendung von InfoSichh-Produkten zur Verarbeitung und Übertragung von staatlich geschützten Verschlusssachen. Die Zulassung wird durch einen Zulassungsnachweis des BSI bestätigt. Produkte mit allgemeiner Zulassung können ohne

	weitere Rücksprache mit dem BSI verwenden werden, solange die verbindlichen Bestimmungen für den Einsatz und den Betrieb eingehalten werden. Zulassungen sind gewöhnlich zeitlich befristet.
Zutritt	**Zutritt** ist der Vorgang des Überschreitens der Grenze einer Raumzone (Raum, Gebäude, Bereich, Werk, Standort etc.).

11.12 Abkürzungsverzeichnis

A	ABez	Amtsbezeichnung
	ACP	Allied Communications Publication
	ADSB	Administrativer Datenschutzbeauftragter
	Aft	Approval for Testing
	AIN	Ausrüstung, Informationstechnik und Nutzung
	AllgUmdr	Allgemeiner Umdruck
	AN	Auftragnehmer
	APC	Arbeitsplatzcomputer
	APersDat	Allgemeine Arten personenbezogener Daten
	APZBw	Abstrahlprüfzentrum der Bundeswehr
	ATK	Aufgaben- und Tätigkeitskatalog
	ATO	Approval to Operate
	AWE	Auswahlentscheidung
	Az	Aktenzeichen
B	BAAINBw	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr
	BAIUDBw	Bundesamt für Infrastruktur, Umwelt und Dienstleistungen der Bundeswehr
	BAMAD	Bundesamt für den Militärischen Abschirmdienst
	BAPersBw	Bundesamt für Personalmanagement in der Bundeswehr
	BDSG	Bundesdatenschutzgesetz
	BesBehKZ	Besonderes Behandlungskennzeichen
	BtrbZ IT-SysBw	Betriebszentrum IT-System der Bundeswehr
	BfDBw	Beauftragter bzw. Beauftragte für den Datenschutz in der Bundeswehr
	BFR	Baufachliche Richtlinien
	BKA	Bundeskriminalamt
	Bl	Billigung
	BMI	Bundesministerium des Innern
	BMWi	Bundesministerium für Wirtschaft und Energie
	BMVg	Bundesministerium der Verteidigung
	BPersDat	Besondere Kategorien personenbezogener Daten
	BSI	Bundesamt für Sicherheit in der Informationstechnik
	BSIG	BSI-Gesetz
	Bt	Beteiligung
	BV	Besonderes Vorkommnis oder
		Bevollmächtigter Vertreter bzw. Bevollmächtigte Vertreterin

	BVA	Bundesverwaltungsamt
	Bw	Bundeswehr
	BwDLZ	Bundeswehr-Dienstleistungszentrum
	BWI	BWI Informationstechnik GmbH
	BZBw	Bereitschaftszentrum der Bundeswehr
C	CaP	Capability Panel
	CD	Compact Disk
	CD&E	Concept, Development and Experimentation
	CDMB	Cyber Defence Management Board
	CERTBw	Computer Emergency Response Team Bundeswehr
	CISO	Chief Information Security Officer
	CPM	Customer, Product, Management
	CSC	EU Council Security Committee
	CSCI	EU Council Security Committee on INFOSEC
	CSOCBw	Cyber Security Operation Center der Bundeswehr
	CSRS	Community Security Requirement Statement
D	DDVBM	Dialog Datenbank Verwertung Bundeswehrmaterial
	DEUmilSAA	Deutsche militärische Security Accreditation Authority
	DFmA	Dienstbereich Fernmelde-Aufklärung
	DGrad	Dienstgrad
	DigAHM	Digitale Ausbildungshilfsmittel
	DIN	Deutsche Industrie Norm
	DMZ	Demilitarisierte Zone
	DSL	Digital Subscriber Line
	DSt	Dienststelle
	DStLtr	Dienststellenleiter bzw. Dienststellenleiterin
	DStNr	Dienststellennummer
	DVD	Digital Video Disk
E	EinsFüKdoBw	Einsatzführungskommando der Bundeswehr
	EinsStO	Einsatzstandort
	EntgeltG	Entgeltgruppe
	EU	Europäische Union
F	F&T	Forschung und Technologie
	FF	Federführung
	FFF	Fähigkeitslücke und Funktionale Forderung
	FFF (S)	Fähigkeitslücke und Funktionale Forderung (Sofortinitiative)
	FüInfoSysSK	Führungsinformationssystem Streitkräfte
	FüUstg	Führungsunterstützung

G	GeNu	Genehmigung zur Nutzung
	GF	Geschäftsfeld
	GIF	Grundsätzliche Infrastrukturforderung
	GSC	General Secretariat of the Council
H	HF	Hochfrequenz
I	IATO	Interim Approval to Operate
	IN	Integrität
	IPT	Integriertes Projektteam
	ISO	International Standardization Organization
	IT	Informationstechnik
	IT-BtrbEinr	IT-Betriebseinrichtung
	IT-BtrbFüEinr	IT-Betriebsführungseinrichtung
	ISB	Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte
	ISBAN	Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte Auftragnehmer
	ISBBtrb	Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte Betrieb
	ISBBMVg	Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte für das Bundesministerium der Verteidigung
	ISBDSt	Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte Dienststelle
	ISBEinsatz	Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte Einsatz
	ISBGBW	Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte Geheimschutzbetreute Wirtschaft
	ISB i.E.	Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte im Einsatz
	ISBMAD	Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte des Militärischen Abschirmdienstes
	ISBOrgBer	Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte Organisationsbereich
	ISBProj	Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte Projekt
	ISBSKB	Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte Streitkräftebasis
	ISBÜb	Informationssicherheitsbeauftragter bzw. Informationssicherheitsbeauftragte Übung
	InfoSichhBef	Informationssicherheitsbefehl
	InfoSichhDok	Informationssicherheitsdokumentation

	InfoSichhIn	Informationssicherheitsinspektion
	InfoSichhInB	Informationssicherheitsinspektionsbericht
	InfoSichhK	Informationssicherheitskonzept
	InfoSichhKDSt	Informationssicherheitskonzept Dienststelle
	InfoSichhKFW	Informationssicherheitskonzept für Wehrtechnische Forschung & Technologie sowie sonstige Forschungsvorhaben, Erprobungen, Truppenversuche und Wehrtechnische Aufträge und für WissUstg NT
	InfoSichhKtr	Informationssicherheitskontrolle
	InfoSichhKProj	Informationssicherheitskonzept Projekt
	InfoSichhPrfg	Informationssicherheitsprüfung
	InfoSichhVork	Informationssicherheitsvorkommnis
	IT-RM	IT-Risikomanagement
	IT-SysBw	IT-System der Bundeswehr
	IUD	Infrastruktur, Umweltschutz und Dienstleistungen
K	KBL	Kryptobereichsleitstelle
	KdoCIR	Kommando Cyber- und Informationsraum
	KdoITBw	Kommando Informationstechnik der Bundeswehr
	Kdr	Kommandeur bzw. Kommandeurin
	KKG	Konfigurationskontrollgruppe
	KtgtFhr	Kontingentführer bzw. Kontingentführerin
L	LuK	Lenkungs- und Kontrollreferat
M	MAD	Militärischer Abschirmdienst
	MADG	Gesetz über den Militärischen Abschirmdienst
	MilSichh	Militärische Sicherheit
	Mz	Mitzeichnung
N	NAMILCOM	NATO Military Committee
	NATO	North Atlantic Treaty Organization
	NBwA	Nicht Bundeswehrangehörige
	NCIRC	NATO Computer Incident Response Capability
	NCDA	National Cyber Defence Authority
	NCSA	National Communication Security Authority
	NDA Germany	National Distribution Agency Germany
	NetOpFü	Vernetzte Operationsführung
	NOC	Network Operation Center
	NÜ	Netzübergang
O	ODP	Organisations- und Dienstpostenplan
	OrgBer	Organisationsbereich
P	PC	Personalcomputer

	PDCA-Modell	Plan-Do-Check-Act-Modell
	PersDat	Personenbezogene Daten
	PIN	Persönliche Identifikationsnummer
	PK	Personenkennziffer
	PKIBw	Public Key Infrastructure der Bundeswehr
	ProjLtr	Projektleiter bzw. Projektleiterin
	PlgABw	Planungsamt der Bundeswehr
	PZITSichhBw	Prüfzentrum für IT-Sicherheit in der Bundeswehr
R	RAID	Redundant Array of Independent Disks
	ReFNÜ	Verfahren zur Registrierung und Freigabe von dezentralen Netzübergängen
S	SAA	Security Accreditation Authority
	SB	Schutzbereich
	SDIP	SECAN Doctrine and Information Publication
	SECAN	Military Committee Communication and Information Systems Security and Evaluation Agency
	SecOps	Security Operating Procedures
	SichhBeauftr	Sicherheitsbeauftragter bzw. Sicherheitsbeauftragte
	SigG	Signaturgesetz
	SigV	Signaturverordnung
	SISRS	System Interconnection Security Requirement Statement
	SLA	Service-Level Agreement
	SoC	Statement of Compliance
	SPECAT	Special Category
	SSRS	System-Specific Security Requirement Statement
	ST&E Plan	Security Test & Evaluation Plan
	StGB	Strafgesetzbuch
	Stv	Stellvertreter bzw. Stellvertretende
	SÜG	Sicherheitsüberprüfungsgesetz
	Sw	Software
T	TABw	Technische Architektur IT-System der Bundeswehr
	TE / ZE	Teileinheit / Zeile
	TK	Telekommunikation
	TSK	Teilstreitkraft / Teilstreitkräfte
	TVöD	Tarifvertrag öffentlicher Dienst
U	UHD	User Help Desk
	UP-Bund	Umsetzungsplan Bund
	UrhG	Urheberrechtsgesetz

	USB	Universal Serial Bus
V	VF	Verfügbarkeit
	VHF	Very High Frequency
	VMBl	Ministerialblatt des Bundesministers der Verteidigung
	VorgV	Vorgesetztenverordnung
	VS	Verschlusssache
	VSA	Verschlusssachenanweisung
	VS-NfD	VS-NUR FÜR DEN DIENSTGEBRAUCH
	VS-Vertr.	VS-VERTRAULICH
	VT	Vertraulichkeit
W	WAN	Wide Area Network
	WANBw	Wide Area Network der Bundeswehr
	WDO	Wehrdisziplinarordnung
	WLAN	Wireless Local Area Network
	WTA	Wehrtechnischer Auftrag
	WTD	Wehrtechnische Dienststelle
Z	ZDv	Zentrale Dienstvorschrift
	ZV	Zusatzvermerk

11.13 Übergang IT-Sicherheitsanforderungen bzw. Informationssicherheits-Anforderungen

11.13.1 Allgemeines

Die alte Liste mit IT-Sicherheitsanforderungen und Anforderungspaketen zum IT-Basisschutz, erweiterten IT-Basisschutz, VS-Verarbeitung Bw sowie weitergehendem Schutz (in der ZDv 54/100, Anlage 21 bzw. A-960/1, Version 1, Anlage 16) ist grundsätzlich nicht mehr zu nutzen.

Im Ausnahmefall darf sie jedoch gemäß den Festlegungen in der Übergangregelung in Abschnitt 1.2 noch vorläufig und im Ausnahmefall für noch nicht nach der Methodik dieser Zentralen Dienstvorschrift zu erstellende bzw. fortzuschreibende IT-Sicherheitskonzepte bzw. Informationssicherheitskonzepte verwendet werden. Daher wird sie nicht mehr in dieser Regelung, sondern nur noch übergangsweise in einer redaktionell angepassten Version im IntranetBw unter http://infosichh.bundeswehr.org im Bereich „Fachinformationen / Regelungen / A-960/1“ zur Verfügung gestellt.

Inhaltlich werden diese alten IT-Sicherheitsanforderungen nicht mehr gepflegt und sind daher bei der übergangsweisen Anwendung für die Fortschreibung von InfoSichhK auf notwendige Ergänzungen von InfoSichh-Anforderungen und –Maßnahmen (spätestens im Rahmen der Ergänzenden Sicherheitsanalyse bzw. Risikoanalyse) zu prüfen.

11.14 Strafbarkeitsrisiko bei unterlassener Verpflichtung mitwirkender Personen zur Geheimhaltung

11.14.1 Vorüberlegungen

Die Berufsgeheimnisträger haben nur dann eine Pflicht, Dritte zur Geheimhaltung zu verpflichten, wenn deren Heranziehung als „Mitwirkung“ im Sinne von § 203 Absatz 3 Satz 2 StGB anzusehen ist und keine Verpflichtung zur Geheimhaltung aus anderen Gründen besteht. Sind diese beiden Voraussetzungen aus Sicht der zuständigen Stelle nicht sicher erfüllt, **sollte im Zweifel eine „Verpflichtung zur Geheimhaltung“ vorgenommen werden**[197]. Im Einzelnen:

(1) Die zuständigen Stellen haben also in einem ersten Schritt zu bewerten, ob die Tätigkeiten, die von Dritten ausgeführt werden sollen, als Mitwirkung im Sinne von § 203 Absatz 3 StGB anzusehen sind. Eine Mitwirkung an der beruflichen Tätigkeit ist anzunehmen, wenn Dritte unmittelbar mit der beruflichen Tätigkeit des Berufsgeheimnisträgers oder deren Vorbereitung, Durchführung, Auswertung und Verwaltung befasst sind. Der Sache nach handelt es sich demnach um im Wesentlichen die Berufsausübung des Berufsgeheimnisträgers unterstützende Tätigkeiten, wie z.B. die Erledigung von Schreibarbeiten, die Annahme von Telefonanrufen oder die Einrichtung und Wartung bzw. Fernwartung informationstechnischer Anlagen.

(2) Ist der Vertragsgegenstand als mitwirkende Tätigkeit anzusehen, ist in einem zweiten Schritt zu prüfen, ob die mitwirkenden Personen bereits einer Verschwiegenheitspflicht nach § 203 Absatz 1 oder 2 StGB unterliegen. Dies sind beispielsweise andere Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete (vgl. Zentrale Dienstvorschrift A-2100/15 – Förmliche Verpflichtung nichtbeamteter Personen). Eine Verpflichtung zur Geheimhaltung ist insoweit entbehrlich; ein Strafbarkeitsrisiko besteht nicht.

(3) Sind nach dem Vorstehenden die mitwirkenden Personen (noch) zur Geheimhaltung zu verpflichten, muss in einem dritten Schritt überlegt werden, ob die zuständige Stelle diese Aufgabe selbst übernimmt oder auf den Vertragspartner delegiert. Ersteres wird eher in Betracht kommen, soweit die Anzahl der zu verpflichtenden Mitarbeiter überschaubar ist und diese „gut erreichbar“ sind, beispielsweise bei einem regelmäßigen persönlichen Kontakt „vor Ort“. In anderen Fällen dürfte diese Lösung dagegen wenig praktikabel und die vertragliche Verpflichtung des Vertragspartners daher vorzuziehen sein.

11.14.2 Individuelle Verpflichtung

Hat die zuständige Stelle entschieden, die konkret an der Vertragserfüllung mitwirkenden Personen selbst zur Geheimhaltung zu verpflichten, sind diese über ihre Pflicht zur Geheimhaltung zu belehren. Dabei kann das als Anlage beigefügte Muster verwendet werden[198].

Es empfiehlt sich für die zuständigen Stellen, über die vorgenommenen Verpflichtungen zur Geheimhaltung einen zentralen Nachweis zu führen. Die Niederschriften sollten im Hinblick auf die strafrechtliche Verjährung bis zum Ablauf des fünften Kalenderjahres nach Beendigung der mitwirkenden Tätigkeit aufbewahrt werden.

[197] Soweit die abschließende Klärung eines Einzelfalls notwendig werden sollte, erfolgt diese durch BMVg R I 5 auf dem Dienstweg.

[198] Sollte die mitwirkende Person die Unterschrift verweigern, so genügt es, wenn die zuständige Stelle die Durchführung der Belehrung unter Hinweis auf diesen Umstand aktenkundig dokumentiert.

11.14.3 Vertragliche Verpflichtung des Vertragspartners

Alternativ kann die zuständige Stelle eine Strafbarkeit des letztlich verantwortlich zeichnenden Berufsgeheimnisträgers ausschließen, wenn dafür Sorge getragen wird, dass die konkret mitwirkenden Personen zur Geheimhaltung verpflichtet werden. Dazu kann mit dem Vertragspartner vertraglich bestimmt werden, dass dieser die ausführenden Mitarbeiter oder ggf. auch weitere Unterauftragnehmer auf gleiche Weise zur Geheimhaltung verpflichtet.

Soweit möglich sollte der Vertrag folgende Vorgaben erfüllen bzw. Regelungen enthalten:

- Der Vertrag ist schriftlich, zumindest aber in Textform, abzuschließen.
- Es ist zu vereinbaren, dass die vertraglich geschuldete Leistung eine „mitwirkende Tätigkeit“ im Sinne von § 203 Absatz 3 Satz 2 StGB darstellt.
- Der Vertragspartner ist unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung – auch über die Vertragslaufzeit hinaus – zur Geheimhaltung zu verpflichten.
- Es ist festzulegen, dass der Vertragspartner sich nur insoweit Kenntnis von fremden Geheimnissen verschaffen darf, als dies zur Vertragserfüllung erforderlich ist.
- Der Vertrag hat eine Regelung zu enthalten, ob und in welchem Umfang der Vertragspartner befugt ist, weitere Personen, insbesondere eigene Mitarbeiter oder Unterauftragnehmer, zur Erfüllung des Vertrags heranzuziehen; der Vertragspartner ist dabei zu verpflichten, diese Personen schriftlich oder in Textform zur Geheimhaltung zu verpflichten und dies dem Bund unaufgefordert nachzuweisen bzw. zumindest zu bestätigen[199].

Weiterhin wird empfohlen, im Vertrag ein Sonderkündigungsrecht für den Fall vorzusehen, dass der Vertragspartner seinen o.a. Pflichten nicht nachkommt.

Ebenso wird angeregt, den Vertragspartner zum Ersatz für diejenigen Schäden zu verpflichten, die dem Bund durch eine schuldhafte Verletzung der Geheimhaltungspflicht der mitwirkenden Personen entstehen. Alternativ kann eine angemessene, pauschale Vertragsstrafe vereinbart werden, um eventuelle Beweisschwierigkeiten zu vermeiden.

Bei mehrstufigen Vertragsverhältnissen ist schließlich darauf zu achten, dass eine lückenlose Vertragskette zwischen dem Berufsgeheimnisträger und der letztlich tätig werdenden „sonstigen mitwirkenden Person“ besteht.

[199] Diese Verpflichtung ist für mehrstufige Vertragsverhältnisse sinngemäß anzuwenden.

11.14.4 Muster der Verpflichtung zur Geheimhaltung

Hat Ich bin heute von (*zuständige Stelle*) ausdrücklich darüber belehrt worden, dass ich gemäß § 203 des Strafgesetzbuches zur Geheimhaltung über alle mir im Rahmen meiner mitwirkenden Tätigkeit bekanntwerdenden Umstände und Vorgänge verpflichtet bin.

Ich verpflichte mich, insoweit zur Geheimhaltung.

Mir ist bekannt, dass

1. sich meine Pflicht zur Geheimhaltung auf alle für mich fremden Geheimnisse erstreckt, namentlich auf die zum persönlichen Lebensbereich gehörenden Geheimnisse sowie Betriebs- oder Geschäftsgeheimnisse,
2. die Verschwiegenheitspflicht gegenüber jedermann besteht, so auch gegenüber Familienangehörigen und gegenüber Arbeitskolleginnen und Arbeitskollegen, und
3. meine Pflicht zur Geheimhaltung auch nach Beendigung der mitwirkenden Tätigkeit fortbesteht.

Den Gesetzestext (§ 203 StGB) sowie eine Ausfertigung dieser Erklärung habe ich erhalten.

_____, den _____ _____

Unterschrift Mitarbeiter/in

Bestätigt:

_____

(*Vertreterin bzw. Vertreter der zuständigen Stelle*werden.

11.15 Bezugsjournal

(Nr.) Bezugsdokumente	Titel
1. SÜG	Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz)
2. BDSG	Bundesdatenschutzgesetz
3. VDG	Vertrauensdienstegesetz
4. MADG	Gesetz über den Militärischen Abschirmdienst (MAD-Gesetz)
5. StGB	Strafgesetzbuch
6. UrhG	Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz)
7. BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)
8. VorgV	Verordnung über die Regelung des militärischen Vorgesetztenverhältnisses (Vorgesetztenverordnung)
9. WDO	Wehrdisziplinarordnung
10. Weisung zur A-2122/4 vom 25.05.2018	Datenschutz - Ausführungsbestimmung zur Europäischen Datenschutzgrundverordnung und dem Bundesdatenschutzgesetz
11. VSA	Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz(Verschlusssachenanweisung) vom 31.03.2006 in der Fassung vom 26.04.2010 (GMBl 2010, S. 846)
12. A-1500/3	Customer Product Management
13. K-10/2	IT-Strategie des Geschäftsbereichs BMVg
14. A-1130/1 VS-NfD	Militärische Sicherheit in der Bundeswehr – Militärische Sicherheit
15. A-1130/2 VS-NfD	Militärische Sicherheit in der Bundeswehr – Verschlusssachen
16. A-1130/3	Militärische Sicherheit in der Bundeswehr – Personeller Geheim- und Sabotageschutz
17. A-200/5 VS-NfD	Meldewesen der Bundeswehr
18. A-2640/34 VS-NfD	Meldewesen Innere und Soziale Lage der Bundeswehr
19. A-2160/6	Wehrdisziplinarordnung und Wehrbeschwerdeordnung
20. A-961/1 VS-NfD	Kryptosicherheit in der Bundeswehr
21. A-962/1 VS-NfD	Abstrahlsicherheit
22. A-500/3 VS-NfD	Behandlung und Archivierung von Unterlagen
23. C-1800/114	Allgemeine baufachliche Vorgaben für die Durchführung von Baumaßnahmen der Bundeswehr
24. C1-1810/0-6000 VS-NfD	Grundsätzliche Militärische Infrastrukturforderung für bauliche Absicherungsmaßnahmen im Bereich der Bundeswehr
25. C-1800/121	Infrastrukturbearbeitung
26. Allgemeiner Umdruck 175	Handbuch bauliche Absicherung (HB BAbsich)

(Nr.) Bezugsdokumente	Titel
27. C1-1810/0-6002	Grundsätzliche Infrastrukturforderung für eine Truppenunterkunft
28. NATO PO(2014) 0358	Enhanced NATO Policy on Cyber Defence
29. NATO C-M(2002) 0049	Security within the North Atlantic Treaty Organisation, Enclosure „F" – CIS – Security
30. NATO AC/35-D/2004-REV3; AC/322-D/0052-REV3	Primary Directive on CIS Security
31. NATO AC-35/D/2005-REV2	INFOSEC Management Directive for Communication and Information Systems (CIS)
32. NATO AC/322-D/0048-Rev2	Infosec Technical and Implementation Directive for Computer and Local Area Network (LAN) Security, Enclosure 1
33. NATO SDIP 293/1 NATO RESTRICTED	Instructions for the control and safeguarding of NATO cryptomaterial
34. NATO SDIP 29-1 NATO RESTRICTED	Facility Design Criteria and Installation of Equipment for the Processing of Classified Information
35. EU 2001/264/EC	Council Decision adopting the Council's Security Regulations
36. EU GEN-P	General INFOSEC Policy (Entwurf), vom 19.12.2007
37. ACP 127 GE SUPP-1(B)	Allied Communications Publication 127 German Supplement-1(B) - Fernschreibbetriebsverfahren, vom Mai 1991
38. ISO 27001	ISO-Standard 27001 „Information Technology – Security techniques – Information security management systems requirements specification"
39. Ressortvereinbarung BMI / BMVg	Regelungen der Verantwortlichkeit bei der Prüfung der IT-Sicherheit im Rahmen von Projekten, die klassifizierte NATO-Informationen verarbeiten, vom 03.07.2006
40. BMVg Staatssekretär/IT 3 – Az 62-09-03-02/2749 vom 03.05.2006	Rahmendienstvereinbarung über die Protokollierung informationstechnischer Systeme zwischen dem Bundesministerium der Verteidigung und dem Hauptpersonalrat beim Bundesministerium der Verteidigung
41. C-1130/12 VS-NfD	Meldungen bei Sicherheitsvorkommnissen sowie bei Vorkommnissen und Erkenntnissen, die mit der regionalen Sicherheitslage erfasst werden
42. Erlass BMVg M II / IT 2, Az 15-04-00 vom 28.12.2010	Rechtmäßigkeit der bzw. rechtliche Voraussetzungen für die Durchsuchung (dienstlich bereitgestellter) PC von Beschäftigten der Bundeswehr
43. GHB	Geheimschutzhandbuch - Handbuch für den Geheimschutz in der Wirtschaft, BMWi, vom November 2004
44. Cyber-Sicherheitsstrategie	Cyber-Sicherheitsstrategie für Deutschland, BMI, vom November 2016
45. Umsetzungsplan Bund 2017	Leitlinie für Informationssicherheit in der Bundesverwaltung
46. BSI-Standard 200-2	IT-Grundschutz-Methodik, BSI, von 2017
47. A-960/15 VS-NfD	IT-Krisenmanagement in der Bundeswehr
48. A-960/11	Registrierung und Freigabe von dezentralen Netzübergängen
49. B1-1500/6-7001 VS-NfD	Technische Architektur des IT-Systems Bundeswehr
50. BSI – GZ 225-552-13-00-07	Zulassung der Fa. JADE-STAHL, vom 08.08.2007

(Nr.) Bezugsdokumente	Titel
51. A1-900/0-1 VS-NfD	Kurierdienst in der Bundeswehr
52. NCIA Directive 90-9	Stand 01.07.2012
53. IT-Grundschutz-Kataloge	https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf– 2016, http://bsi.bund.de/, BSI, vom Januar 2016
54. A-960/16	Inspektionsteams mit erweiterten technischen Fähigkeiten
55. B-1100/14 VS-NfD	Sicherheitsbestimmungen für die Fernmeldeaufklärung der Bundeswehr (SichBestFmAufkl Bw)
56. BSI TL 03420 Version 2.2 März 2016	Leitlinie für das Löschen und Vernichten von Verschlusssachen auf Datenträgern
57. A1-250/0-1 VS-NfD	Aufgaben im Standortbereich
58. A-1100/8 VS-NfD	Verarbeitung personenbezogener Daten im Militärischen Nachrichtenwesen
59. A-960/5 VS-NfD	Behandlung von Informationssicherheitsvorkommnissen und Unterstützung von disziplinaren und strafrechtlichen Ermittlungen
60. A-550/1	Regelungsmanagement
61. B1-960/0-7000	Anbindung von externen Rechnern und Rechnernetzen an das IT-SysBw
62. A-229/2 VS-NfD	Übungswesen der Bundeswehr
63. B-1130/32 VS-NfD	Melde-, Berichts- und Informationswege zur Erstellung der Militärischen Sicherheitslage der Bundeswehr
64. A2-1130/1-0-1 VS-NfD	Militärische Sicherheit in der Bundeswehr – Arbeitshilfe Sichherheitsvorkommnise
65. Europäische Datenschutzgrundverordnung (EU-DSGVO)	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46

11.16 Änderungsjournal

Version	Gültig ab	Geänderter Inhalt
1 A-960/1	20.01.2016	• Formale Überführung • Erstveröffentlichung
2 A-960/1	Vorläufig 05.03.2019	• Inhaltliche Überarbeitung gesamt