Inkraftsetzung mit Organisationsverfügung 02/10

Richtlinie IT-Architektur der BStU (RL IT-Architektur)

Inhaltsverzeichnis

1 Allgemeines

1.1 Geltungsbereich und Zweck

Die Richtlinie gilt für das IT-Architekturbüro und den IT-Architekturausschuss. Sie regelt die Verfahrensweise, Aufgaben und Befugnisse des IT-Architekturbüros (IT-AtB) und des IT-Architekturausschusses (IT-AtA) bei der Planung, Erstellung der Vorgaben und Rahmenbedingungen für die IT-Architektur der BStU.

Ziel ist es, die Kompetenzen und Befugnisse des IT-AtB und des IT-AtA transparent zu regeln und zu einer höheren Effizienz und Effektivität bei der Aufgabenerfüllung beizutragen.

Grundlage dieser Richtlinie bilden[1]

OrgVfg. 02/09 – IT-Sicherheitsmanagement (Informationssicherheit)
die Arbeitsanweisung 01/08 ZV - AA IT Projekte ZV 3,
OrgVfg. 08/08 – Richtlinie zum Projektmanagement bei der BStU,
OrgVfg. 08/07 – Änderung der Aufbauorganisation in der Behördenleitung (Einrichtung des IT-Architekturbüros und des IT-Architekturausschusses).

2 Aufgaben und Zusammenarbeit der Beteiligten

2.1 IT-Architekturbüro

Die Aufgaben des IT-Architekturbüros im Sinne dieser Richtlinie umfassen:

die Festlegung der Rahmenbedingungen der IT-Anwendungsarchitektur für IT-Fachanwendungen, insbesondere die Festlegung der funktionalen- und nichtfunktionalen Rahmenbedingungen für IT-Fachanwendungen, die sich in den bestehende IT-Verbund integrieren,
die Bewertung von Fachanforderungen (Lastenheft) hinsichtlich der bestehenden bzw. geplanten IT-Architekturlandschaft sowie deren Abstimmung mit den Fachbereichen,
die Erstellung von Kurzprofilen (Kurzpflichtenheft) für IT-Strategieplanungen,

die Unterstützung bei der Erstellung von Umsetzungsplanungen (technische Planungen),
die Erstellung bzw. Unterstützung bei der Erstellung von Abnahmekatalogen (Testfallkatalogen),
die technisch-inhaltliche Qualitätssicherung und die Durchführung von Marktsichtungen sowie
die Aufnahme und Unterhaltung von Kontakten zu Anbietern und Organisationen.

Das IT-Architekturbüro organisiert federführend die Tätigkeit des IT-Architekturausschusses. Die Beratungen des IT-Architekturausschusses sind grundsätzlich monatlich durchzuführen. Die Ergebnisse werden in einem Protokoll dokumentiert.

Die Entscheidungen des IT-Architekturausschusses werden in das Dokument „Festlegung zur IT-Architektur“ aufgenommen, sind vom Lenkungsausschuss zu bestätigen und werden vom IT-Architekturbüro veröffentlicht.

2.2 IT-Architekturausschuss

Der IT-Architekturausschuss ist ein abteilungsübergreifendes Gremium. Er setzt sich zusammen aus

der Leiterin bzw. dem Leiter des IT-Architekturbüros,
den IT-Koordinatorinnen und IT-Koordinatoren aller Abteilungen,

zusätzlich beratend:

die/der IT-Sicherheitsbeauftragte/r der BStU
einem/ einer Vertreter/-in des IT-Betriebes und
einem/ einer Vertreter/-in der IT-Programmierung.

Im IT-Architekturausschuss werden funktionale und nichtfunktionale Rahmenbedingungen für die IT-Fachanwendungen der BStU beraten. Die IT-Koordinatorinnen und IT-Koordinatoren vertreten ihre Abteilung unter Maßgabe der Fachaufgabe. Das beinhaltet die Abstimmung über die Modellierung von IT-Fachanwendungen in die bestehende IT-Landschaft. Weiterhin erfolgt die übergreifende Beratung von IT-Fachanforderungen im Kontext mit der strategischen IT-Ausrichtung. Bei Erfordernis initiiert das IT-Architekturbüro und der IT-Architekturausschuss die Änderung der IT-strategischen Ausrichtung der BStU.

Berechtigt zur Beschlussfassung im IT-Architekturausschuss sind das IT-Architekturbüro und die IT-Koordinatorinnen und IT-Koordinatoren. Die Vertreter/innen des IT-Betriebs und der IT-Programmierung nehmen beratend teil und müssen gehört werden. Im Falle mangelnden Konsens’ im IT-Architekturausschuss entscheidet grundsätzlich das IT-Architekturbüro in der Sache und informiert alle Beteiligten. Zur Überprüfung dieser Entscheidung besteht die Möglichkeit, über den/die jeweilige/n Abteilungsleiter/in dazu im Lenkungsausschuss vorzutragen und dort eine Revision der Entscheidung herbeizuführen.

Für die Erledigung ihrer Aufgaben sollen die IT-Koordinatorinnen und IT-Koordinatoren, den Sach- und Fachverstand ihrer Abteilung nutzen.

Die dynamischen Prozesse in der IT-Architektur können zeitweilig den Anteil der zu erbringenden Arbeitsaufgaben der IT-Koordinatorinnen und IT-Koordinatoren erhöhen. In diesem Fall sind durch die Abteilungsleitungen fachlich qualifizierte Mitarbeiterinnen und Mitarbeiter den IT-Koordinatorinnen und Koordinatoren zur Unterstützung zuzuordnen.

Die Aufgaben der IT-Koordinatorinnen und IT-Koordinatoren der Abteilungen sind in der Richtlinie zum Projektmanagement (OrgVfg. 08/08, derzeit im Punkt 7.6) beschrieben. Nähere Ausführungen zu Einzelheiten, zu Beteiligungen und zur Kommunikation der IT Koordinatorinnen und IT-Koordinatoren im Sinne dieser Richtlinie sind nachfolgend beschrieben.

2.3 Dokument „Festlegung zur IT-Architektur“

Das Dokument „Festlegung zur IT-Architektur“ ist ein Ergebnis der Tätigkeit des IT-Architekturbüros und des IT-Architekturausschusses. Es werden die verschiedenen Sichtweisen bei der Planung und Erstellung der IT-Architektur strukturiert zusammengefasst und beschrieben. Das Dokument beinhaltet die funktionalen und nichtfunktionalen Rahmenbedingungen für IT-Fachanwendungen. Diese sind durch das IT-Architekturbüro allgemeinverbindlich zu beschreiben und im Intranet der BStU zu veröffentlichen. Änderungen sind in die „Festlegung zur IT-Architektur“ einzuarbeiten und auf dem aktuellen Stand zu halten.

Das Dokument „Festlegung zur IT-Architektur“ ist dem Lenkungsausschuss jährlich vorzulegen. Es gilt verbindlich für die Projektierung, Einführung und den Betrieb von IT-Fachanwendungen bei der BStU.

Auf Basis der „Festlegung zur IT-Architektur“ sind die technischen Parameter durch den IT-Betrieb und die IT-Programmierung (durch interne wie externe Auftragnehmer) zu beachten.

Die „Festlegung zur IT-Architektur“ wird verbindlich angewendet für:

- die Erstellung der Lastenhefte sowie interner Pflichtenhefte für IT-Fachanforderungen
- den IT-Betrieb und
- die IT-Programmierung (durch interne sowie externe Auftragnehmer).

2.4 Zusammenarbeit mit dem Referat Organisation

Das Referat Organisation und das IT-Architekturbüro informieren sich gegenseitig im Rahmen der fachlichen Zusammenarbeit über alle Vorhaben in der Informationstechnik.

Bei Durchführung von IT-Projekten sind die Lastenhefte seitens der IT-Koordinatoren der Fachabteilungen zeitgleich dem Organisationsreferat und dem IT-Architekturbüro zu übermitteln.

2.5 Zusammenarbeit mit der Projektleitung (Großprojekte)

Die Projektleiter von IT-Großprojekten stimmen die Geschäftsprozesse auf mögliche Veränderungen der Rahmenbedingungen mit dem IT-Architekturbüro ab. Erst nach der Bewertung durch das IT-Architekturbüro kann das Lastenheft Bestandteil von Ausschreibungsunterlagen werden.

2.6 Zusammenarbeit mit dem IT-Referat

Im Rahmen der fachlichen Zusammenarbeit gestalten das IT-Referat und das IT-Architekturbüro den Informationsaustausch über alle Planungen und Vorhaben in der Informationstechnik. Die vom Lenkungsausschuss getroffenen Festlegungen zur IT-Architektur haben verbindlichen Charakter und ermöglichen dem IT-Referat, seine IT-Dienstleistungen effizient und effektiv vorzuhalten und zu planen.

Im Rahmen der Erarbeitung von Pflichtenheften sowie der Prüfung der technischen Machbarkeit ist durch das Referat IT/TK besonderes Augenmerk auf mögliches Auswirkungspotential für die bestehende IT-Architektur zu legen.

2.7 Zusammenarbeit mit der/dem IT-SiBe

Die im IT-Sicherheitsmanagement festgelegten Abläufe werden vom IT-Architekturbüro durch einen kontinuierlichen und gegenseitigen Informationsaustausch mit der/dem IT-Sicherheitsbeauftragten (IT-SiBe) unterstützt. Um dies im Vorfeld von IT-Architekturentscheidungen zu gewährleisten, ist eine beratende Teilnahme der/des IT-SiBe zu Themen in ihrer/seiner Zuständigkeit im IT-Architekturausschuss obligatorisch.

3 Prozesse

3.1 Planungsprozess IT-Strategie

Grundlage aller Überlegungen zu diesem Prozess sind die verdichteten Behördenziele, formuliert durch die Behördenleitung unter Berücksichtigung der abteilungsspezifischen Anforderungen. Der Planungsprozess IT-Strategie umfasst zudem die strategische IT-Anwendungs- und Architekturplanung zur Bestimmung von Umfang und Zielrichtung des zukünftigen Handelns. Damit verbunden sind die Vorausplanung und Bewertung zukünftiger Vorhaben und soweit vorhanden Festlegungen für den Geschäftsbereich.

Das IT-Architekturbüro und der IT-Architekturausschuss unterstützen die Ergebnisse des Planungsprozesses IT-Strategie mit dem Abgleich und der Priorisierung des Anforderungskatalogs und der Umsetzung der daraus resultierenden funktionalen und nichtfunktionalen

Rahmenbedingungen in der „Festlegung zur IT-Architektur“.

Die IT-Koordinatorinnen und IT-Koordinatoren unterstützen den Planungsprozess der IT-Strategie. Die IT-Sicherheitsbeauftragten der Fachabteilungen (IT-SiBe-F) übermitteln abteilungsspezifische Anforderungen und unterstützen den Prozess der Vorausplanung aus Sicht der Fachabteilung unter Informationssicherheitsaspekten.

Im IT-Architekturbüro erfolgt die Koordinierung, Verdichtung und Auswertung der abteilungsspezifischen IT-Fachanforderungen. Unter Beachtung der bestehenden IT-Architektur und der strategischen IT-Fachanforderungen erfolgt ein Soll – Ist Vergleich. Im Resultat entsteht ein Modell der IT-Landschaft.

Der IT-Strategieprozess wird grundsätzlich am Anfang eines Kalenderjahres nach Abschluss der vorangegangenen Haushaltsplanung für die neue Haushaltsplanungsperiode gestartet. Am Ende des Planungsprozesses IT-Strategie wird das IT-Rahmenkonzept unter der Federführung des Referates Organisation erstellt. Die Ergebnisse des IT-Architekturausschusses fließen in das IT-Rahmenkonzept ein, die sich an den Sicherheitsrichtlinien und den verabschiedeten Sicherheitsrichtlinien der BStU orientieren.

3.2 Einstufung Projekte

Das IT-Architekturbüro spricht eine Empfehlung (Einstufung) für die Projektkategorie als Standard- oder Großprojekt aus und übermittelt diese an die Projektservicestelle.

Zur Anwendung kommen die Kriterien für IT-Projekte aus der jeweils gültigen Fassung der Richtlinie zum Projektmanagement. Der Lenkungsausschuss beschließt hierzu abschließend.

3.3 Projektprozess Großprojekt / Standardprojekte

Dieser Prozess beschreibt den Ablauf von Groß- und Standardprojekten. Grundlage dieses Prozesses ist die neue Anforderung einer Abteilung zur Erstellung, Änderung, Optimierung und Neueinführung einer IT-Fachanwendung.

Das IT-Architekturbüro erhält Lesezugriff auf alle Projektunterlagen. Ergeben sich während der Durchführung von Standardprojekten Anhaltspunkte, die IT-strategische Belange tangieren, erhält das IT-Architekturbüro ein umfassendes Informations- und Konsultationsrecht. Änderungen an den funktionalen und nichtfunktionalen Rahmenbedingungen sind mit dem IT-Architekturbüro zu analysieren. Im Ergebnis dessen entscheidet der Lenkungsausschuss abschließend.

Das IT-Architekturbüro unterstützt die IT-Projektleiterinnen und IT-Projektleiter bei der Abstimmung des Lastenheftes (Mengengerüste, Einschätzungen aus Fachbereichssicht). Des

Weiteren können sich die IT-Projektleiterinnen und IT-Projektleiter jederzeit zur Unterstützung an das IT-Architekturbüro wenden.

Dem Architekturbüro obliegen im Besonderen bei Großprojekten die Abstimmungen zu sowie die Durchführung und Bewertung von Marktsichtungen. Bei Bedarf kann Unterstützung durch Fachexpertisen in der Fachabteilung eingeholt werden.

4 Schulung und Fortbildung sowie Sachmittelbedarfsprüfung

Die Initiierung von aufgabenbezogenen Schulungsmaßnahmen für die Mitglieder des IT-Architekturausschusses kann durch das IT-Architekturbüro erfolgen.

Die Sachmittelbedarfsprüfung erfolgt durch das Referat Organisation.

5 Übergangsbestimmungen und Inkraftsetzung

Nach Inkraftsetzung erfolgt mit sofortiger Wirkung die Anwendung dieser Richtlinie für alle neu eingereichten IT-Fachverfahren.

Für bereits in der Realisierung und Einführung befindliche IT-Fachverfahren wird die Anwendung dieser Regelung mit den zuständigen Projektleiterinnen und Projektleitern und dem IT-Architekturbüro festgelegt.

Anlage Begriffsbestimmungen

1 IT-Strategie

Die IT-Strategie stellt die mittel – und langfristige Ausrichtung der IT-Landschaft der BStU zur Unterstützung der Aufgaben und Geschäftsprozesse dar.

2 IT-Architektur

Die IT-Architektur der BStU stellt die Gesamtheit aller Komponenten, Technologien und organisatorischen Maßnahmen dar, die die in der Behörde vorkommenden Funktionen, Prozesse und Daten abbilden und deren Zusammenspiel ermöglichen[2].

3 Funktionale- und nichtfunktionale Rahmenbedingungen der IT-Architektur

Funktionale- und nichtfunktionale Rahmenbedingungen sind durch das IT-Architekturbüro festgelegte, allgemeinverbindliche Vorgaben zur Realisierung von IT-Fachanforderungen und IT-Fachverfahren, die auf der IT-Strategie und der IT-Ausrichtung der BStU basieren.

4 Festlegungen zur IT-Architektur

Die Festlegungen zur IT-Architektur beschreiben allgemeinverbindlich die funktionalen und nichtfunktionalen Rahmenbedingungen für IT-Fachverfahren bei der BStU.

5 Anforderungskatalog

Der Anforderungskatalog entsteht im Planungsprozess IT-Strategie. Es werden die zukünftigen IT-Fachanforderungen der Abteilungen, die mit Kurzprofilen untersetzt werden, priorisiert dargestellt.

6 IT-Anwendungsarchitektur

Unter IT-Anwendungsarchitektur wird die aufgabenbezogene strukturelle Umsetzung bzw. der strukturelle Lösungsansatz eines IT-Fachverfahrens verstanden.

7 IT-Fachverfahren / IT-Fachanwendungen

IT-Fachverfahren / IT-Fachanwendungen sind die aus Fachanforderungen erstellten Produkte, Strukturen in der Informationstechnik. Diese können sich in der Planungs-, Realisierungs- oder Betriebsphase befinden.

8 Kernfachverfahren / Kernanwendung

Als Kernfachverfahren / Kernanwendung wird ein IT-Fachverfahren bezeichnet, welches einen zentralen Platz bei der Realisierung der aus dem StUG abgeleiteten Fachaufgaben einnimmt.

9 Fachanforderung/ Lastenheft

Unter einer Fachanforderung/ Lastenheft wird die Gesamtheit der in einem zentralen Dokument beschriebenen und zu realisierenden (Änderungs-)Anforderungen für eine zu erstellende Software-Lösung verstanden oder ein Komplex von Anforderungen im Kontext mit der Informationstechnik. Die Anforderungsbeschreibung erfolgt aus Sicht des Auftraggebers. Das Lastenheft gliedert sich in:

Ausgangssituation und Zielsetzung, funktionale Anforderungen, nichtfunktionale Anforderungen, Risikoakzeptanz, Lebenszyklus der Gesamtarchitektur der Anwendung, Lieferumfang und Abnahmekriterien.

10 Funktionale Anforderungen

Die funktionalen Anforderungen sind Bestandteil eines Lastenheftes. Sie beschreiben die Funktion der Anwendung, die Verarbeitung der prozessrelevanten Daten, die Eigenschaften der Daten sowie die Schnittstellen zu Nachbarsystemen.

11 Nichtfunktionale Anforderungen

Die nichtfunktionalen Anforderungen sind Bestandteil eines Lastenheftes. Unter nichtfunktionalen

Anforderungen sind die Rand- oder Rahmenbedingungen der funktionalen Anforderungen zu verstehen. Das beinhaltet zum Beispiel die Leistungsanforderungen, Qualitätsanforderungen und Realisierungsanforderungen. Die Abgrenzung zwischen funktionalen und nichtfunktionalen Anforderungen ist nicht immer scharf.

---

[1] In der jeweils aktuellen Fassung

[2] Sascha Krüger, Jörg Seelmann-Eggebert, IT-Architektur-Engineering, Galileo Computing, 2003, S.29

Der Bundesbeauftragte für die Unterlagen
des Staatssicherheitsdienstes der ehemaligen
Deutschen Demokratischen Republik

Geschäftszeichen	Telefon	Datum
ZV 3 - 041331/02.09	7410	19.03.2009

IT-Sicherheitsmanagement (Informationssicherheit), IT-Sicherheitsverantwortlichkeiten (Rollen und Prozesse), Grundsätze

Organisationsverfügung 02/09

Mit sofortiger Wirkung werden die Grundsätze zur Festlegung der IT-Sicherheitsverantwortlichkeiten im Rahmen des IT-Sicherheitsmanagements bei der BStU (Informationssicherheit) in Kraft gesetzt.

In Vertretung

Hans Altendorf

Anlage:

- IT-Sicherheitsmanagement (Version 2.0 vom 13.03.2009)

Die Bundesbeauftragte für die Unterlagen
des Staatssicherheitsdienstes der ehemaligen
Deutschen Demokratischen Republik

IT-Sicherheitsmanagement

IT-Sicherheitsverantwortlichkeiten (Rollen und Prozesse)

Grundsätze

Version: 02.00

Verfasser: IT-Sicherheitsbeauftragte/r
Stand: 13.03.2009

Inhaltsverzeichnis

1. Ziele

Um der behördlichen Verantwortung für die Informationssicherheit insbesondere unter den Rahmenbedingungen des StUG gerecht zu werden, werden IT-Sicherheitsverantwortlichkeiten in der BStU bestimmt und aufsetzend auf den Empfehlungen nach IT-Grundschutz des BSI[1] etabliert. Ihre Ziele sind:

- Umsetzen der Sicherheitsanforderungen entsprechend StUG
- Abstimmung der Informationssicherheit mit den Behördenzielen und den Vorgaben des BSI
- Umsetzung der IT-Sicherheitspolitik[2] und der Regelungen und Anweisungen zur Informationssicherheit
- Bereitstellung von Informationen zum Status der Informationssicherheit für die Behördenleitung
- Überprüfung und Aktualisierung sowie Kontrolle der Regelungen und Maßnahmen zur Informationssicherheit

Im vorliegenden Konzept werden die Rollen und Funktionen der IT-Sicherheitsverantwortlichkeiten innerhalb der BStU beschrieben. Dazu gehören die Aufgaben, die Einbindung in die Organisation der BStU und ihrer Schnittstellen untereinander. Weiterhin beinhaltet es die Definition von Rollen externer Behörden und Dienstleister und deren Abgrenzung bzw. Schnittstellen zu den IT-Sicherheitsverantwortlichkeiten der BStU.

2. Geltungsbereich

Die IT-Sicherheitspolitik und die aus ihnen abgeleiteten Richtlinien und Dienstanweisungen gelten für die BStU. Es ist das erklärte Ziel der BStU, dass alle externen Dienstleister bei der Zusammenarbeit mit der BStU konforme Grundsätze besitzen, einhalten und veröffentlichen.
Bei externen Dienstleistern sind Regelungen und Vertragsergänzungen vorzusehen, die den Sinn und den Inhalt der IT-Sicherheitspolitik und der daraus folgenden Regelungen enthalten. Kann die IT-Sicherheitspolitik bei externen Dienstleistern nicht oder nur teilweise umgesetzt werden, sind die erforderlichen Schnittstellen zu externen Dienstleistern präzise zu definieren und bezüglich der Einhaltung der Informationssicherheit zu überwachen.
Die Aufgaben, Rechte und Pflichten, die die/der behördliche Datenschutzbeauftragte gemäß Bundesdatenschutzgesetz wahrnimmt, bleiben unberührt und werden im Weiteren nicht erwähnt.
Eine zukünftige IT-Revision[3] wird wichtige Aufgaben im Bereich Prüfung im Umfeld der Informationssicherheit übernehmen. Die originären Aufgaben der IT-Revision bleiben unberührt und werden hier im Weiteren nicht erwähnt.

3. Minimalanforderungen

Aus dem BSI IT-Grundschutzhandbuch, den BSI-Standards und den ISO-Normen 17799 leiten sich Minimalanforderungen für die IT-Sicherheitsverantwortlichkeiten der BStU ab:

---

[1] BSI: Bundesamt für die Sicherheit in der Informationstechnik

[2] Die IT-Sicherheitspolitik beschreibt die durch die Behördenleitung vorgegebenen IT-Sicherheitsziele und umzusetzenden Rahmenbedingungen einschließlich des anzustrebenden IT-Sicherheitsniveaus in der BStU. Die IT-Sicherheitspolitik der BStU orientiert sich an den Vorgaben des BSI, konkret an den BSI-Grundschutz-Standards (Standard 100-1 bis 100-4). In den vom BSI veröffentlichten Grundschutzkatalogen werden detailliert Gefährdungen und Risiken mit Bezug zur Informationssicherheit aufgezeigt und konkrete Maßnahmen zur Risikominimierung vorgeschlagen. Die IT-Sicherheitsleitlinie der BStU basiert auf dem BSI Standard 100-2, IT-Grundschutzvorgehensweise.

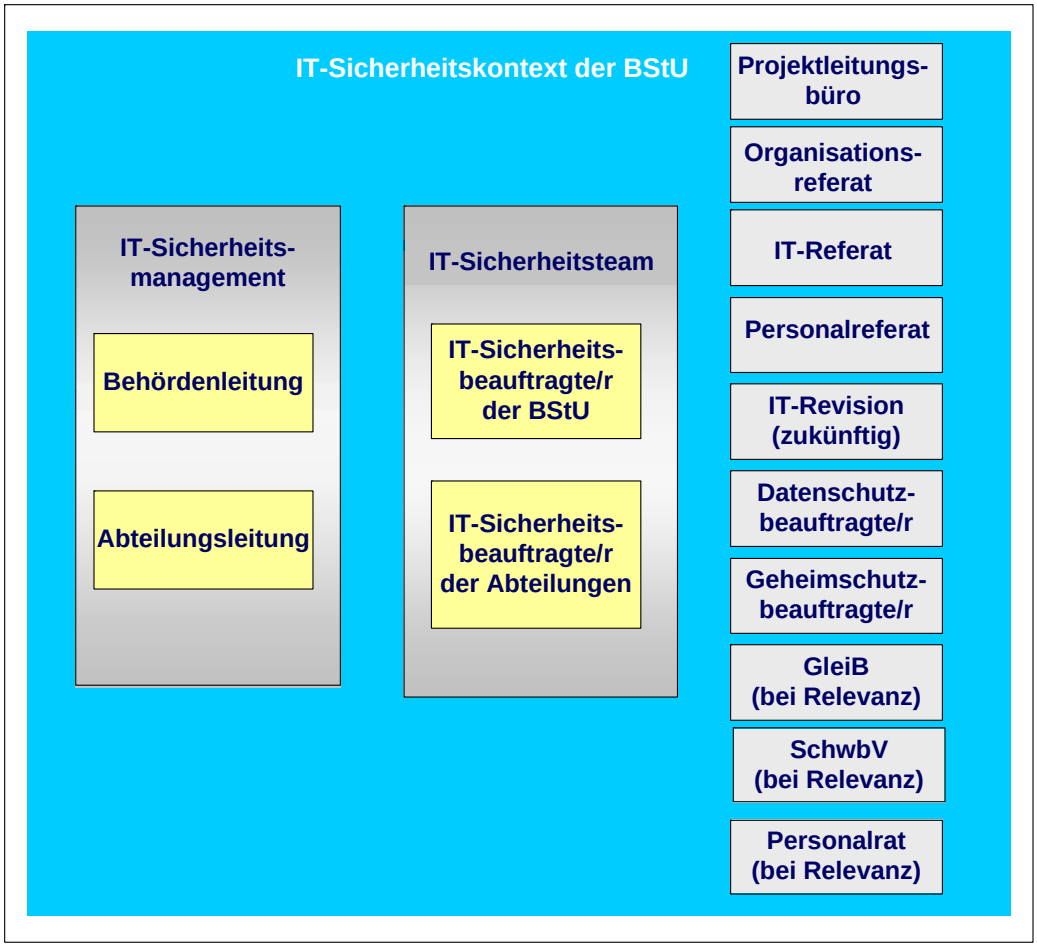
[3] siehe auch Kapitel 6.5

1. Die Gesamtverantwortung für die ordnungsgemäße und sichere Aufgabenerfüllung (und damit für die Informationssicherheit) verbleibt bei der Behördenleitung.
2. Die Verantwortung für die Informationssicherheit am einzelnen Arbeitsplatz ist in gleicher Weise zu delegieren wie die Verantwortung für die originäre Aufgabe.
3. Die IT-Sicherheitsverantwortlichkeiten umfassen mindestens die/den IT-Sicherheitsbeauftragte/n als zentralen Ansprechpartner und das IT-Sicherheitsmanagement auf Behördenleitungsebene.
4. Die IT-Sicherheitsverantwortlichkeiten sollten in der bestehenden Organisationsstruktur verankert sein.
5. Informationen über den IT-Sicherheitsstatus sind Behördenleitungsinformationen. Sie sind der Behördenleitung regelmäßig und zusätzlich bei Bedarf zur Verfügung zu stellen.
6. Alle Maßnahmen müssen regelmäßig überprüft werden. Die Prüfung und Kontrolle durch die/den IT-Sicherheitsbeauftragte/n ist personell von der Konzeption und der Durchführung der Maßnahmen zu trennen.

4. Funktionen IT-Sicherheitsorganisation

4.1 Übersicht Aufbau

Die folgende Abbildung zeigt die schematische Struktur der IT-Sicherheitsverantwortlichkeiten innerhalb der BStU:



Darstellung der IT-Sicherheitsverantwortlichkeiten im IT-Sicherheitskontext der BStU

4.2 IT-Sicherheitsmanagement

Die Behördenleitung und die Abteilungsleitungen der BStU übernehmen die Rolle des IT-Sicherheitsmanagements. Das Thema Informationssicherheit ist bei Bedarf Tagesordnungspunkt in der Sitzung der Behördenleitung mit den Abteilungsleitungen; ggf. wird gesondert geladen.
Das IT-Sicherheitsmanagement stellt die Umsetzung der IT-Sicherheitspolitik der BStU sicher.

4.3 IT-Sicherheitsbeauftragte/r (IT-SiBe)

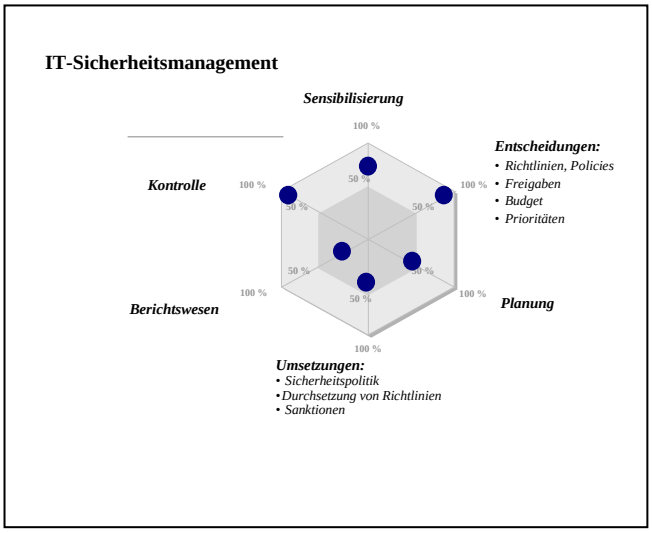
Die/der IT-Sicherheitsbeauftragte wird von der Behördenleitung ernannt.
Um Unabhängigkeit und das entsprechende Berichtsrecht zu gewährleisten, erfolgt das Berichtswesen der/des IT-Sicherheitsbeauftragten direkt an die Behördenleitung der BStU.
Die/der IT-Sicherheitsbeauftragte koordiniert die IT-Sicherheitsprozesse innerhalb der BStU im jeweiligen Auftrag des IT-Sicherheitsmanagements.

4.4 IT-Sicherheitsteam

Das IT-Sicherheitsteam besteht neben der/dem IT-Sicherheitsbeauftragten aus den jeweiligen IT-Sicherheitsbeauftragten der Abteilungen, die als Ansprechpartner für die Informationssicherheit in diesen Abteilungen zuständig sind[4]. Der/dem IT-Sicherheitsbeauftragten obliegt die fachliche Steuerung des IT-Sicherheitsprozesses.

5 Aufgaben

5.1 IT-Sicherheitsmanagement



IT-Sicherheitsmanagement – Darstellung der prozentualen Gewichtung der Tätigkeiten im IT-Sicherheitsprozess

Aufgaben des IT-Sicherheitsmanagements sind:

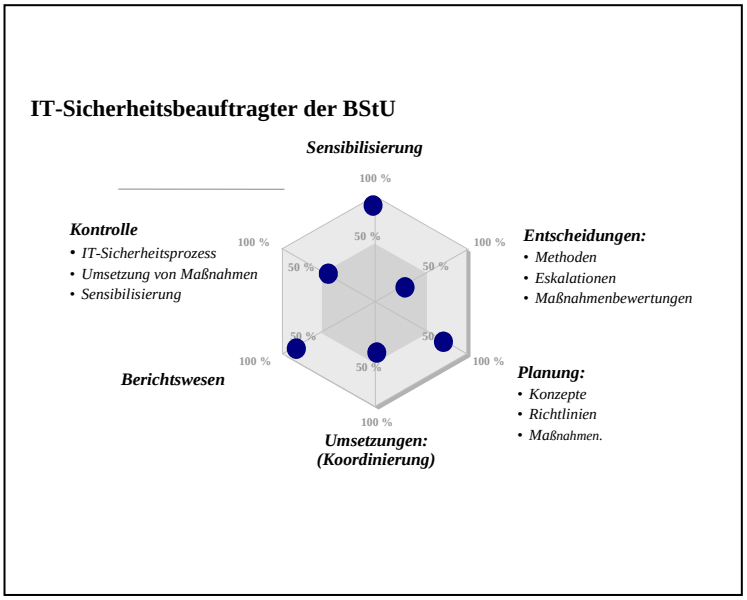
- IT-Sicherheitsziele und -strategien zu bestimmen, sowie die IT-Sicherheitspolitik zu entwickeln und fortzuführen (**Planung**)[5],

[4] Die Aufgaben der/des IT-Sicherheitsbeauftragten der Abteilungen kann auch vom IT-Koordinator bzw. von der IT-Koordinatorin in der Abteilung wahrgenommen werden.

[5] Die/der IT-Sicherheitsbeauftragte erarbeitet die Vorschläge, die durch das IT-Sicherheitsmanagement beschlossen werden.

- Grundlegende und übergeordnete **Entscheidungen** in Bezug auf die Informationssicherheit zu treffen,
- **Kontrollen** der Umsetzung der IT-Sicherheitsgrundsätze und daraus folgender Anweisungen zu veranlassen,
- den IT-Sicherheitsprozess zu initiieren, zu **steuern und zu kontrollieren,** sowie
- den Realisierungsplan für die IT-Sicherheitsmaßnahmen inkl. Schulungs- und Sensibilisierungsprogramme zu **genehmigen** und die erforderlichen Ressourcen zur Verfügung zu stellen,
- **Freigabe und Durchsetzung** von Richtlinien und Regelungen bzw. Dienstanweisungen,
- die/den IT-Sicherheitsbeauftragte/n in sicherheitsrelevante **Entscheidungen** mit einzubeziehen.

5.2 IT-Sicherheitsbeauftragte/r der BStU (IT-SiBe)

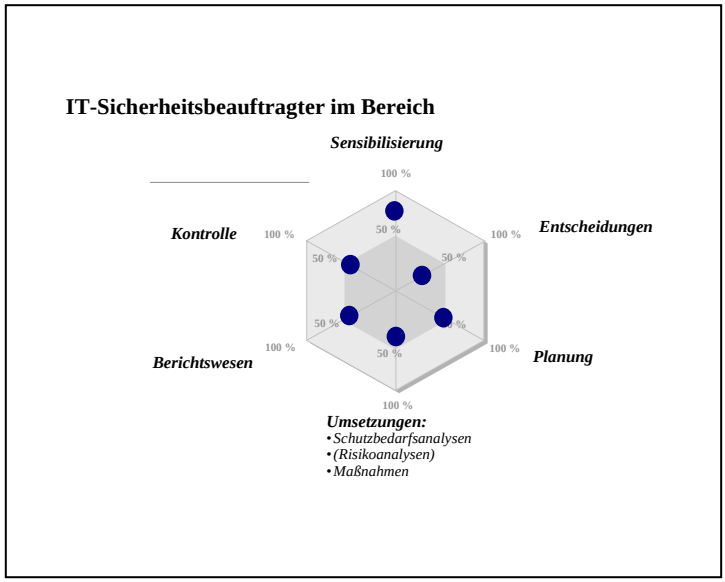


IT-Sicherheitsbeauftragte/r der BStU – Darstellung der prozentualen Gewichtung der Tätigkeiten im IT-Sicherheitsprozess

Aufgaben der/des IT-Sicherheitsbeauftragten sind:

- im gesamten IT-Sicherheitsprozess (**Planung, Umsetzung, Überwachung und Anpassung**) mitzuwirken und Vorschläge zu erarbeiten,
- alle Anforderungen an die Informationssicherheit zusammenzustellen, insbesondere die IT-Sicherheitsanforderungen an IT-Projekte **(Planung)**,
- ist verantwortlich für die Aktualität der IT-Sicherheitsdokumente (Grundsätze, Regelwerke die aus den IT-Sicherheitsleitlinien (Policies) abgeleitet werden),
- Vorschläge für IT-Sicherheitsleitlinien (Policies), Regelungen und Dienstanweisungen, die aus den Anforderungen der Informationssicherheit entstehen, zu entwickeln und über die Behördenleitung bzw. die Sitzungen der Abteilungsleitungen mit den Abteilungen der BStU abzustimmen,
- die Erstellung von IT-Sicherheitskonzepten zu koordinieren,
- die Erstellung des Realisierungsplans für IT-Sicherheitsmaßnahmen und die Initiierung und Überprüfung der Realisierung zu koordinieren,
- das fachliche Führen des IT-Sicherheitsteams,
- die Beratung bei IT-Projekten zum Thema Informationssicherheit zu koordinieren,
- Berichterstattung an die Behördenleitung,
- den jährlichen Sicherheitsbericht zu erarbeiten und direkt an die Behördenleitung weiterzuleiten,
- den Informationsfluss zwischen den verschiedenen Ansprechpartnern zum Thema Informationssicherheit sicherzustellen,
- die Beschäftigten in geeigneter Form zum Thema Informationssicherheit zu informieren und zu beraten,
- auftretende sicherheitsrelevante Zwischenfälle festzustellen, zu melden, zu dokumentieren und die Untersuchung in Abstimmung mit der Behördenleitung zu koordinieren,
- Abstimmungen mit der/dem Datenschutzbeauftragten durchzuführen.

5.3 IT-Sicherheitsbeauftragte/r in den Fachabteilungen (IT-SiBeF)

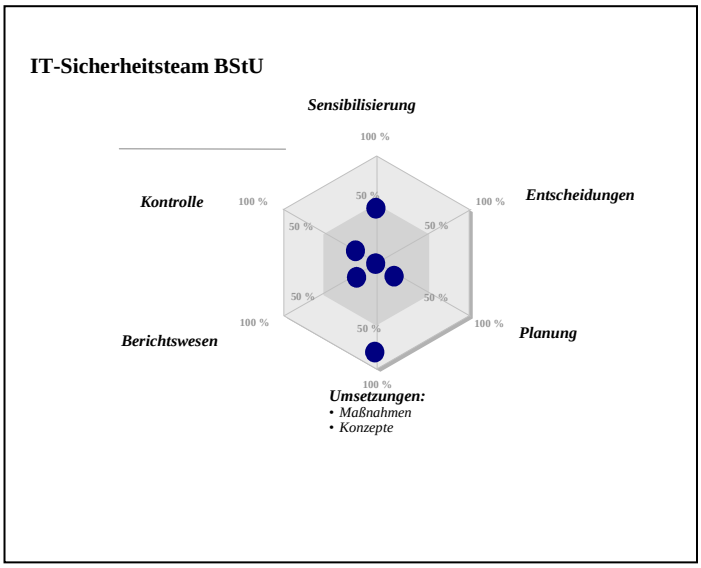


IT-Sicherheitsbeauftragte/r der Fachabteilungen der BStU – Darstellung der prozentualen Gewichtung der Tätigkeiten im IT-Sicherheitsprozess

Die Aufgaben der/des IT-Sicherheitsbeauftragten in den Fachabteilungen sind:

- die Unterstützung bei Umsetzung der Vorgaben des IT-Sicherheitsmanagements in der Fachabteilung,
- Mitarbeit im IT-Sicherheitsteam,
- die Beschäftigten der Fachabteilung für Informationssicherheit zu **sensibilisieren**,
- als Ansprechpartner/in der Beschäftigten in der Fachabteilung zu dienen,
- die Unterstützung bei der Umsetzung von IT-Sicherheitsmaßnahmen in der Fachabteilung und die Umsetzung zu **kontrollieren**,
- bei der Auswahl angemessener IT-Sicherheitsmaßnahmen mitzuwirken **(Planung)**,
- Informationen über Schulungs- und/oder Sensibilisierungsbedarf der Beschäftigten des Bereichs aufzunehmen und mit der/dem IT-Sicherheitsbeauftragten abzustimmen **(Planung)**,
- Relevante Sicherheitsinformationen zusammenzufassen und an das IT-Sicherheitsmanagement und im Rahmen des IT-Sicherheitsteams an die/den IT-Sicherheitsbeauftragten **zu berichten**,
- sicherheitsrelevante Vorfälle an die/den IT-Sicherheitsbeauftragte/n zu melden,
- Regelungen zur Informationssicherheit, in Abstimmung mit der/dem IT-Sicherheitsbeauftragten, zu initiieren und umzusetzen.

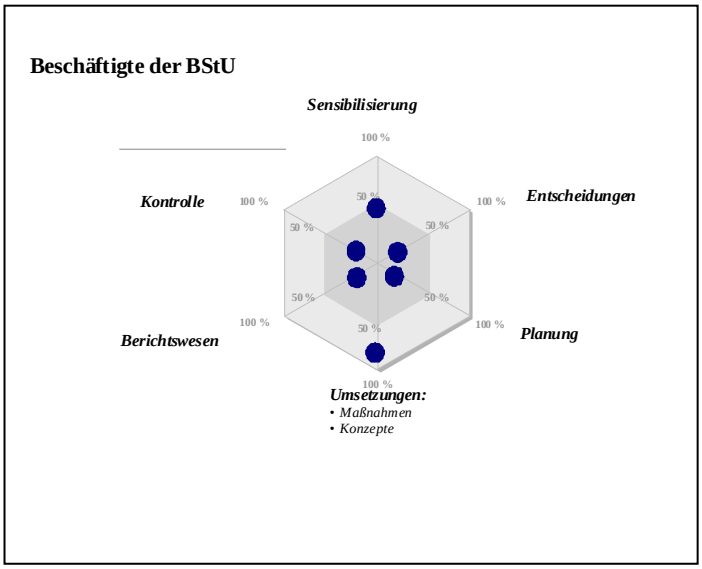
5.4 IT-Sicherheitsteam der BStU



IT-Sicherheitsteam der BStU – Darstellung der prozentualen Gewichtung der Tätigkeiten im IT-Sicherheitsprozess

Das IT-Sicherheitsteam gewährleistet einen zeitnahen Austausch von Informationen und stellt die entsprechende Abstimmung mit den verschiedenen Anforderungen der Beteiligten sicher. Es trifft sich regelmäßig und nutzt zwischen den Treffen die BStU-internen Kommunikationswege zur Abstimmung.

5.5 Beschäftigte der BStU



Beschäftigte der BStU – Darstellung der prozentualen Gewichtung der Tätigkeiten im IT-Sicherheitsprozess

Die Aufgaben der Beschäftigten sind:

- die **eigenverantwortliche Umsetzung** der Vorgaben des IT-Sicherheitsmanagements in seinem Aufgabenbereich,
- die **Umsetzung** der in seinem Aufgabenbereich geplanten Maßnahmen,
- die Mitwirkung bei der Auswahl angemessener Maßnahmen in seinem Aufgabenbereich,
- die Meldung sicherheitsrelevanter Vorfälle in seinem Bereich.

6 Schnittstellen im IT-Sicherheitskontext

6.1 Projektleitungsbüro

Das Projektleitungsbüro und das diesem zugeordnete IT-Architekturbüro gewährleisten die Umsetzung der Regelungen zur Informationssicherheit für IT-Großprojekte. Sie informieren das IT-Sicherheitsteam über geplante Änderungen/Neuerungen im IT-Sicherheitskontext und erhalten vom IT-Sicherheitsteam die erforderlichen Informationen zum aktuellen Stand der Informationssicherheit.

6.2 Organisationsreferat

Das Organisationsreferat gewährleistet die Umsetzung der Regelungen zur Informationssicherheit für IT-Standardprojekte.

Es erarbeitet im Rahmen der Geschäftsverteilung bei der BStU Regelungen zur Informationssicherheit.

6.3 IT-Referat

Das IT-Referat erarbeitet im Rahmen der Geschäftsverteilung bei der BStU Regelungen zur Informationssicherheit und gewährleistet im Geschäftsbetrieb die Umsetzung dieser. Zu Fragen der Informationssicherheit wird das Referat IT/TK durch die/den IT-Sicherheitsbeauftragte/n beraten.

6.4 Personalreferat

Das Personalreferat wird bei Bedarf bzgl. der Informationssicherheit einbezogen. [6]

6.5 IT-Revision

Die zukünftige IT-Revision hat eine wichtige Rolle im IT-Sicherheitsmanagement, da sie im Rahmen ihrer regelmäßigen Prüfungen auch Überprüfungen und Kontrollen im Hinblick auf Informationssicherheit vornimmt. Die/der IT-Sicherheitsbeauftragte ist direkter Ansprechpartner für die IT-Revision in allen Fragen der Informationssicherheit.

Die/der IT-Sicherheitsbeauftragte stellt, in Abstimmung mit dem IT-Sicherheitsmanagement, alle Informationen der IT-Revision zur Verfügung.

Bis zur Einrichtung der IT-Revision nimmt die/der IT-Sicherheitsbeauftragte deren Aufgaben wahr.

[6] Hierzu zählen u. a. die jährlichen IT-Sicherheitsbelehrung oder abzustimmende Maßnahmen bei wiederholten oder vorsätzlichen Verstößen gegen die Informationssicherheit

6.6 Datenschutzbeauftragte/r

Die Schnittstelle zur/zum Datenschutzbeauftragten ist durch Ihre Einbindung in den Sicherheitskontext der BStU gegeben. Der/die IT-Sicherheitsbeauftragte stimmt sich mit dem/der Datenschutzbeauftragten ab.

6.7 Geheimschutzbeauftragte/r

Die Schnittstelle zur/zum Geheimschutzbeauftragten ist durch ihre/seine Einbindung in den Sicherheitskontext der BStU gegeben. Der/die IT-Sicherheitsbeauftragte stimmt sich mit dem/der Geheimschutzbeauftragten ab.

6.8 Gleichstellungsbeauftragte

Die GleiB wird in mitbestimmungspflichtige Entscheidungen bzgl. der Informationssicherheit einbezogen.

6.9 Schwerbehindertenvertretung

Die Schwerbehindertenvertretung (SchwbV) wird bei Entscheidungen bzgl. der Informationssicherheit immer dann beteiligt, wenn diese Entscheidungen Interessen der schwerbehinderten Menschen berühren und ggf. direkte Auswirkungen auf das Arbeitsumfeld der schwerbehinderten Menschen haben.

6.10 Personalrat

Der Personalrat wird in mitbestimmungspflichtige Entscheidungen bzgl. der Informationssicherheit einbezogen.

6.11 Externe Dienstleister

Externe Dienstleister sind beauftragte Firmen oder Institutionen und externe Personen, die Zugriff auf IT-Systeme der BStU erhalten. Die Dauer der Beauftragung ist dabei unbedeutend. Bei der Zusammenarbeit mit bzw. Beauftragung von externen Dienstleistern und Unternehmen müssen die IT-Sicherheitsgrundsätze erfüllt werden. Die Kontrolle obliegt den insoweit fachlich verantwortlichen Beschäftigten sowie den IT-Sicherheitsbeauftragten der jeweiligen Fachabteilung. Über die Zusammenarbeit mit externen Dienstleistern und Unternehmen wird die/der IT-Sicherheitsbeauftragte informiert und in die Abstimmung der IT-Sicherheitsanforderungen einbezogen.

7 Prozesse

Im Folgenden werden die wichtigsten Prozesse als Muster definiert. Im Einzelfall müssen sie angemessen detailliert werden. Es werden die folgenden Abkürzungen für Rollen verwandt:

Behördenleitung / IT-Sicherheitsmanagement	**BHL**
Lenkungsausschuss	**LA**
Datenschutzbeauftragte/r	**DSB**
Geheimschutzbeauftragte/r	**GSB**
IT-Revision	**Rev**
IT-Sicherheitsbeauftragte/r	**IT-SiBe**
IT-Sicherheitsbeauftragte/r Bereich	**IT-SiBeF**
Projektleitungsbüro	**PLB**
Organisationsreferat	**ZV 3**

Personalreferat	**ZV 1**
Personalrat	**PR**
Gleichstellungsbeauftragte	**GleiB**
Schwerbehindertenvertretung	**SchwbV**

Es werden die folgenden Abkürzungen für Beteiligungen verwandt:

Verantwortlich	**V**
Mitarbeit	**M**
Wird informiert	**I**
Entscheidet	**E**

Ist die Beteiligung nur in Einzelfällen sinnvoll (optional) oder wird sie durch die/den IT-Sicherheitsbeauftragte/n einzeln angefordert, so ist dieses in Klammern dargestellt.

7.1 Berichtswesen

Das Berichtswesen dient der Bereitstellung von relevanten Informationen über den IT-Sicherheitsstatus für die Behördenleitung.

Berichtswesen	**IT-SiBe**	**IT-SiBeF**	**DSB**	**GSB**	**Rev**	**ZV 1**	**GleiB**	**SchwbV**	**PR**	**BHL**
Definition der Inhalte	**V**	**(M)**	**(I)**	**(I)**	**(I)**		**(I)**	**(I)**	**(I)**	
Beauftragung	**V**									**E**
Bericht in den Bereichen erstellen (bedarfsweise)	**I**	**V**								
Berichte sammeln und aggregieren	**V**	**M**								
Maßnahmen entwickeln und empfehlen	**V**	**(M)**	**(M)**		**(I)**	**(I)**	**(I)**	**(I)**	**(I)**	
Bericht und Empfehlungen weiterleiten	**V**	**I**	**I**		**I**		**(I)**	**(I)**	**(I)**	
Prüfung des Berichts und der Empfehlungen	**I**	**I**	**I**	**I**	**I**		**(I)**	**(I)**	**(I)**	**V/E**
Koordinieren der Umsetzung	**V**	**M**	**(I)**	**(I)**	**(I)**					

V=Verantwortlich M=Mitarbeit I=Wird informiert E=Entscheidet

Das Berichtswesen durch die/den IT-Sicherheitsbeauftragte/n erfolgt direkt an die Behördenleitung.

7.2 Sicherheitsrelevante Vorfälle

Ein geordneter Meldeweg von sicherheitsrelevanten Vorfällen ist die Voraussetzung für eine effektive Abwehr und die schnelle und zielgerichtete Entwicklung und Umsetzung von Maßnahmen zur Verringerung von Risiken. Hierzu ist ein Konzept zu erstellen, in dem – basierend auf den jeweiligen sicherheitsrelevanten Vorfällen – eine Beschreibung des Meldeweges und der Zuständigkeiten erfolgt. Zur Verkürzung der Reaktionszeiten und zur sachkundigen Bearbeitung der Vorfälle ist der/dem IT-Sicherheitsbeauftragten eine mit dem erforderlichen Sachverstand ausgestattete “Task-Force“ zur Seite zu stellen.

Relevante Vorfälle	IT-SiBe	IT-SiBeF	DSB	GSB	Rev	ZV 1	GleiB	SchwbV	PR	BHL
Entgegennehmen von Meldung und Weiterleitung	**V**	**V**	**M**	**V**	**M**	**M**	**M**	**M**	**M**	**M**
Untersuchung und Empfehlung von Maßnahmen	**V**	**(M)**	**(M)**	**(M)**	**(M)**	**(M)**				
Bericht an BHL	**V**	**I**	**I**	**I**	**I**	**(I)**[7]	**(I)**[6]	**(I)**[6]	**(I)**[6]	**I**
Entscheidung über Maßnahmen	**I**	**I**	**I**	**(I)**	**I**	**(I)**[6]	**(I)**[6]	**(I)**[6]	**(I)**[6]	**E**
Koordinieren der Umsetzung	**V**	**(M)**	**I**	**(M)**	**I**	**(I)**[6]	**(I)**[6]	**(I)**[6]	**(I)**[6]	

V=Verantwortlich M=Mitarbeit I=Wird informiert E=Entscheidet

7.3 IT-Projekte

Jede Änderung oder Neuerung von IT-Objekten oder damit zusammenhängenden Richtlinien kann das IT-Sicherheitsniveau senken bzw. erhöhen. Deshalb ist jede beabsichtigte Änderung oder Neuerung der/dem IT-Sicherheitsbeauftragten möglichst frühzeitig zu melden und dort im Hinblick auf die Informationssicherheit zentral zu bewerten. Diese Meldung ist nicht erforderlich, wenn das IT-Vorhaben in die beim Organisationsreferat elektronisch geführte Projektliste aufgenommen worden ist. Der/dem IT-Sicherheitsbeauftragten ist ein „Lesezugriff“ auf diese Liste einzurichten.
Für die sich anschließende Projektphase gilt:

- Für den Teilaspekt Informationssicherheit trägt die Projektleitung die Verantwortung und ist Ansprechpartner für die/den IT-Sicherheitsbeauftragte/n der Fachabteilung.
- Die Projektleitung ist für die Einbindung der/des IT-Sicherheitsbeauftragten, die Umsetzung der notwendigen IT-Sicherheitsmaßnahmen und deren Bericht verantwortlich.

Projekte	IT-SiBe	IT-Si-BeF	DSB	GSB	Rev	ZV 1	GleiB	SchwbV	PR	BHL	LA	ZV 3[8]	PLB[9]
Melden von geplanten Änderungen / Neuerungen an den IT-SB	**I**	**V**	**I**	**I**	**(I)**	**(I)**					**V**	**(V)**	**(V)**
Freigabe vorab	**V**	**(M)**	**(I)**	**(I)**	**(I)**					**(I)**	**(I)**	**(I)**	**(I)**
Bewerten der Meldungen	**V**	**(M)**	**(M)**	**(I)**	**(I)**	**(I)**[10]	**(I)**[7]	**(I)**[7]	**(I)**[7]	**I**	**I**	**(I)**	**(I)**

[7] (I): die Information erfolgt bei personenbezogenen oder organisatorischen Maßnahmen

[8] für IT-Standardprojekte, die durch das Projektmanagement ZV 3 abgebildet werden

[9] für IT-Großprojekte, die durch das PLB abgebildet werden

Projekte	IT-SiBe	IT-SiBeF	DSB	GSB	Rev	ZV 1	GleiB	SchwbV	PR	BHL	LA	ZV 3[11]	PLB[12]
Empfehlung von Maßnahmen	**V**	**(M)**	**(M)**	**I**	**(I)**	**(I)**[7]	**(I)**[7]	**(I)**[7]	**(I)**[7]	**I**	**I**	**(M)**	**(M)**
Entscheidung über Maßnahmen	**V**	**M**	**I**	**E**[13]	**I**	**(I)**[7]	**(I)**[7]	**(I)**[7]	**(I)**[7]	**E**	**E**	**(I)**	**(I)**
Bericht zur Umsetzung von Maßnahmen	**V**	**I**	**I**	**E**[8]	**I**	**(I)**[7]	**(I)**[7]	**(I)**[7]	**(I)**[7]	**I**	**I**	**(I)**	**(I)**

V=Verantwortlich M=Mitarbeit I=Wird informiert E=Entscheidet

Anmerkung: Die Einbindung der/des Datenschutzbeauftragten in Projekten erfolgt entsprechend einer gemäß Bundesdatenschutzgesetz notwendigen Vorabkontrolle. Die formale Freigabe erfolgt durch den Lenkungsausschuss der BStU.

7.4 Kontrolle

Das IT-Sicherheitsmanagement und damit die IT-Sicherheitsverantwortlichen müssen sich den ständig ändernden Anforderungen der IT anpassen. Dazu werden die Maßnahmen regelmäßig auf Akzeptanz und Wirksamkeit kontrolliert. Das geschieht durch die Aktualisierung der IT-Sicherheitskonzepte (Aktualisierung von Maßnahmen und Soll/Ist-Vergleich liefern die notwendigen Maßnahmen) und durch die Einarbeitung von Änderungsvorschlägen.

Kontrolle	IT-SiBe	IT-SiBeF	DSB	GSB	ZV 1	GleiB	Rev	SchwbV	PR	BHL
Kontrolle von Sicherheitsmaßnahmen	**I**	**V**	**(M)**	**(I)**	**(I)**[14]	**I**	**(M)**	**I**	**I**	**M**
Kontrolle beauftragen	**V**									**E**
Maßnahmenkatalog aktualisieren	**V**	**(M)**	**I**	**(I)**	**(I)**[8]	**(I)**[8]	**I**	**(I)**[8]	**(I)**[8]	
Soll/Ist-Vergleich	**V**	**M**					**(M)**			
Änderungsvorschläge einholen	**V**	**M**					**(M)**			
Vorschläge zusammenstellen und bewerten	**V**	**M**	**(M)**	**(I)**						

[10] (I): die Information erfolgt bei personenbezogenen oder organisatorischen Maßnahmen

[11] für IT-Standardprojekte, die durch das Projektmanagement ZV 3 abgebildet werden

[12] für IT-Großprojekte, die durch das PLB abgebildet werden

[13] E: Entscheidet, bewertet und verfolgt alle Maßnahmen in seinem Verantwortungsbereich

[14] (I): die Information erfolgt bei personenbezogenen oder organisatorischen Maßnahmen

Kontrolle	IT-SiBe	IT-SiBeF	DSB	GSB	ZV 1	GleiB	Rev	SchwbV	PR	BHL
Abstimmung mit anderen Beteiligten	**V**	**I**	**I**	**(I)**	**I**	**(I)**[8]	**I**	**(I)**[8]	**(I)**[8]	**I**
Erstellen eines IT-Sicherheitskonzept aus Änderungsvorschlägen und Delta des Soll/Ist-Vergleichs	**V**	**(M)**		**(I)**						
Konzept vorlegen und beschließen	**V**	**I**	**I**		**(I)**[8]	**(I)**[8]	**I**	**(I)**[8]	**(I)**[8]	**E**

V=Verantwortlich M=Mitarbeit I=wird informiert E=Entscheidet

8 Schulung und Sensibilisierung

Für die Schulung und Sensibilisierung von Beschäftigten sind grundsätzlich deren Vorgesetzte verantwortlich. Diese achten darauf, dass

- die Einweisungen neuer Beschäftigten, bzw. von Beschäftigten in neue Tätigkeiten, einen ausreichenden Anteil zu Aspekten der Informationssicherheit enthält,
- den Beschäftigten alle Regelungen zum Thema Informationssicherheit bekannt gemacht werden,
- die Beschäftigten diese Regelungen einhalten und
- Schulungen von Beschäftigten die relevanten Informationssichheitsthemen enthalten.

Die/der IT-Sicherheitsbeauftragte steht zur Beratung zu diesen Themen zur Verfügung. Sie/er stellt die zu vermittelnden Inhalte bereit.
Die/der IT-Sicherheitsbeauftragte hat die Verantwortung, allen Beschäftigten relevante Informationen zum Thema Informationssicherheit in geeigneter Weise zugänglich zu machen.

9 Dokumente und Standards

- Stasi-Unterlagen-Gesetz (StUG)
- IT-Grundschutzkataloge des BSI
- IT-Sicherheitshandbuch des BSI
- ISO 17799 – Information technology – Code of practice for information security management
- ISO 27001 – Information security management systems (Requirements)

Der Bundesbeauftragte für die Unterlagen
des Staatssicherheitsdienstes der ehemaligen
Deutschen Demokratischen Republik

Geschäftszeichen	Telefon	Datum
ZV 3 - 041331/08.08	7410	24.11.2008

Richtlinie zum Projektmanagement bei der BStU

Organisationsverfügung 08/08

Mit sofortiger Wirkung wird für alle bei der BStU laufenden Projekte im Sinne der Geschäftsordnung der BStU die Richtlinie zum Projektmanagement in Kraft gesetzt.

Gleichzeitig wird die Organisationsverfügung 04/04 - Richtlinie zum Projektmanagement bei der BStU vom 25.06.2004 außer Kraft gesetzt.

In Vertretung
Hans Altendorf

Anlage:

- Richtlinie zum Projektmanagement

Organisationsvermerk:

Die Richtlinie gilt nicht für Forschungsprojekte der Abteilung Bildung und Forschung.

Der Bundesbeauftragte für die Unterlagen
des Staatssicherheitsdienstes der ehemaligen
Deutschen Demokratischen Republik

Inkraftsetzung mit Organisationsverfügung 08/08

Richtlinie zum Projektmanagement bei der BStU

Inhaltsverzeichnis

1. Allgemeines und Geltungsbereich

Diese Richtlinie regelt die Verfahrensweisen bei der Planung, Durchführung und dem Abschluss der

Bearbeitung von Projekten.

Die Richtlinie verfolgt das Ziel, den Projektbeteiligten mehr Orientierung und Sicherheit bei der Projektgruppenarbeit zu vermitteln und damit insgesamt zu einer höheren Effizienz und Effektivität bei der Aufgabenerfüllung beizutragen.

Grundlage bilden Vorgaben, die das BMI in einem „Praxisleitfaden Projektmanagement“ * für die Bundesverwaltung zusammengefasst hat.
Danach ist Projektmanagement ein systematischer Prozess zur Führung komplexer Vorhaben. Es umfasst die Organisation, Planung, Steuerung und Überwachung aller Aufgaben und Ressourcen, die notwendig sind, um die Projektziele zu erreichen.

Des Weiteren gelten die Festlegungen für IT-Projektabläufe der BStU. Diese sind zusammengefasst im Intranet der BStU unter „Projekt IT-Analyse“ veröffentlicht.

Diese Richtlinie gilt für alle Beteiligten, die gemäß diesen Bestimmungen im Rahmen einer Projektorganisation mitwirken.

Die vertretungsrechtlichen Beteiligungstatbestände gemäß den gesetzlichen Bestimmungen bleiben von der Richtlinie unberührt.
Den zuständigen Personalvertretungen, der Gleichstellungsbeauftragten und der Schwerbehindertenvertretung ist die Möglichkeit einer frühzeitigen Einbindung in die Projektarbeit einzuräumen.

2. Projektarten

Projekte sind einmalige, zeitlich begrenzte Vorhaben mit besonderen Aufgabenschwerpunkten gemäß Geschäftsordnung (
GO
BStU
).

Quelle
BStU

IT-Projekte sind Vorhaben, die überwiegend die Einführung neuer IT-Prozesse und/oder IT-Programme bzw. erhebliche Änderungen bestehender IT-Prozesse und/oder IT-Programme als Zielstellung haben.

Fachprojekte sind Vorhaben, die überwiegend aufbau- und/oder ablauforganisatorische

Änderungen ohne wesentliche Änderungen in den bestehenden IT-Fachanwendungen als Zielstellung haben.

Standardprojekte sind kleine und mittlere Vorhaben.

Großprojekte sind Vorhaben,

- die nur mit einem Zeit- und Personalaufwand von mehr als drei Monaten realisiert werden können oder/und
- die eine wesentliche Änderung der Aufbauorganisation (große Teile der Dienststelle) beinhalten und/oder einen wesentlichen Wandel der IT-Anwendungsarchitekturlandschaft durch Einführung neuer großer IT-Fachanwendungen bzw. umfassende Änderung bestehender IT-Fachanwendungen beinhalten oder/und
- die Haushaltsmittel von mehr als 50 T€ erfordern oder/und
- die Abstimmung abteilungsübergreifender Fachanforderungen beinhalten und Entscheidungen des Lenkungsausschusses erfordern.

Die Einstufung von Vorhaben in Großprojekte erfolgt durch den Lenkungsausschuss. Die Kriterien sind Indikatoren für eine Empfehlung an den Lenkungsausschuss durch die Projektservicestelle.

3. Projektorganisation bei der BStU

3.1 Einrichtung von Projektgruppen

Projekte werden durch Projektgruppen als **Auftragnehmer** realisiert.

Projektgruppen für Großprojekte werden durch die Behördenleitung auf Empfehlung des Lenkungsausschusses eingerichtet.

Projektgruppen für Standardprojekte werden durch die Leiterin/den Leiter des Referates Organisation eingerichtet.

Für Großprojekte können eigenständige Organisationseinheiten gem. GO BStU gebildet werden. Diese sind im Organisationsplan auszuweisen.

Die Projektorganisation ist bei der Projektvorbereitung festzulegen.

3.1 Projektservicestelle für IT-Projekte

Im Referat Organisation ist für IT-Projekte eine Projektservicestelle eingerichtet.

Zu ihren Aufgaben gehört:

Die Projektregistratur und -beratung, d. h. insbesondere:
- formale Prüfung der Projektanträge,
- ggf. die Beteiligung weiterer Organisationseinheiten,
- Klärung offener Probleme der Projektorganisation

das IT-Projektcontrolling (Projektüberwachung) nach Terminen, Ergebnissen, Aufwand und Kosten, d. h. insbesondere:
- die Erhebung und Darstellung von Soll – Ist Vergleichen
- die Ressourcenplanung und Erstellung von Schwachstellenanalysen im Sinne eines Multi-Projekt-Controllings auf Basis der in der Projektservicestelle erfassten Daten.

Von der Projektservicestelle werden Entscheidungsvorlagen für den Lenkungsausschuss erstellt.

4. Initiierung von Projekten (Auftraggeber)

Projekte können von außen auf Grund von Gesetzen, Verordnungen oder Erlassen initiiert werden. Für Projekte, die von außen initiiert werden, ist der Direktor der Auftraggeber.

Projekte können von innen bei Problemen in der Aufbau- und Ablauforganisation, zur Umsetzung von Verbesserungsvorschlägen im Rahmen des Vorschlagwesens sowie sonstigen Angelegenheiten von den Abteilungsleitern als Auftraggeber initiiert werden. Bei IT-Projekten kann dieser/diese durch den IT-Koordinator/die IT-Koordinatorin der auftraggebenden Abteilung vertreten werden.

Die Entscheidung über die Durchführung eines Projekts trifft grundsätzlich die Behördenleitung auf Empfehlung des Lenkungsausschusses.

5. Projektantrag und Lastenheft (Fachanforderung)

Der Projektantrag (Vd.-Nr. BStU 15-001) wird vom Auftraggeber beim Referat Organisation eingereicht.

Dem Projektantrag ist ein Lastenheft (Vd.-Nr. BStU 15-002) beizufügen. Das Lastenheft wird vom Auftraggeber erarbeitet und beinhaltet die Fachanforderung.

Der Projektantrag wird in der Projektservicestelle registriert und dem Lenkungsausschuss zur Kenntnisnahme und Bestätigung vorgelegt.

6. Projektauftrag und Pflichtenheft (Auftragnehmer/Leistungsangebot)

Für jedes bestätigte Projekt ist ein Projektauftrag (Vd.-Nr. BStU 15-003) durch den Auftragnehmer zu erstellen. Auftragnehmer ist bei Großprojekten das Projektleitungsbüro, bei Standardprojekten das Referat Organisation.

Des Weiteren ist ein Pflichtenheft (Vd.-Nr. BStU 15-004) zu erarbeiten, soweit keine externe Vergabe als Werkvertrag erfolgt. Das Pflichtenheft beinhaltet die Projektumsetzungsplanung und die Projektziele, d. h. die als Leistungsangebot konkretisierten Fachanforderungen auf der Basis des Lastenheftes.

Das Pflichtenheft wird grundsätzlich durch den Auftragnehmer erarbeitet.

Für IT-Großprojekte wird das Pflichtenheft bzw. das erweiterte Lastenheft (interne Ausschreibungsunterlagen und IT Anforderungen) in Zusammenarbeit mit dem IT-Architekturbüro und dem Projektleitungsbüro erarbeitet.

Ist geplant, das Projekt durch externe Vergabe als Werkvertrag umzusetzen, sind Ausschreibungsunterlagen als erweitertes Lastenheft vom fachlich Verantwortlichen für das Projekt zu erstellen. Die Erstellung des Pflichtenheftes erfolgt in diesen Fällen durch den externen Auftragnehmer.

Bei externer Vergabe der Leistung kann das Pflichtenheft abweichen von den Vorgaben für die BStU Pflichtenhefte. Für IT-Projekte kommt das V Modell XT zur Anwendung.

Der Projektauftrag ist nach Bestätigung durch den Auftraggeber der Projektservicestelle zur Registrierung und Projektkontrolle zuzuleiten.

7. Projektbeteiligte

7.1 Lenkungsausschuss

Der Lenkungsausschuss ist die fachliche Entscheidungsinstanz für das Projekt und entscheidet in allen Fach- und Planungsfragen, die außerhalb der Kompetenz der Projektgruppe liegen und bei Konflikten im Projektmanagement.

Er unterstützt das Projekt bei der Sicherstellung erforderlicher Zuarbeiten aus allen Organisationseinheiten sowie bei der Umsetzung der Projektergebnisse.

Der Lenkungsausschuss entscheidet über:

- Projektauftrag und -ziele,
- alle Beschluss- und Änderungsanträge hinsichtlich der Projektziele, Projekttermine und Projektumfang in Abstimmung mit der Projektleiterin/dem Projektleiter,
- Projektunterbrechung und -abbruch,
- die fachliche Beurteilung und Abnahme der Arbeitsergebnisse des Projekts vom Projektauftrag bis zum Projektabschluss,

Qualitätsstandards für Projektergebnisse,
Entlastung der Projektleiterin/des Projektleiters und Auflösung der Projektgruppe nach Abschluss des Projekts bei Großprojekten.

Des Weiteren fördert er die Akzeptanz der Projektarbeit in der Linie, unterstützt bei der Beschaffung von Informationen aus anderen Organisationseinheiten und bei der Suche nach Konsultationspartnern.

7.2 Projektleitungsbüro

Aufgaben des Projektleitungsbüros sind das Projektmanagement für Großprojekte sowie die Leitungs- und Berichtsverantwortung für Großprojekte bei der BStU gegenüber der Behördenleitung und dem Lenkungsausschuss. Es ist verantwortlich für die Erstellung von Pflichtenheften bei Großprojekten.

Durch das Projektleitungsbüro erfolgt die Vorbereitung, Organisation sowie Protokollierung der Lenkungsausschusssitzungen.

7.3 Projektleitung

Die Projektleiterin/der Projektleiter ist für die Leitung der Projektgruppe, die Klärung aller organisatorischen Probleme, die Koordinierung und terminliche Kontrolle der Aufgaben zuständig.

Die Projektleiterin/der Projektleiter für ein Großprojekt wird von der Behördenleitung auf Empfehlung des Lenkungsausschusses berufen. Projektgruppen für Großprojekte werden organisatorisch vom Projektleitungsbüro geleitet.

Die Projektleiterin/der Projektleiter für ein Standardprojekt wird von der Leiterin/dem Leiter des Referates Organisation eingesetzt. Projektgruppen für Standardprojekte werden organisatorisch vom Referat Organisation geleitet.

Die Projektleitung ist verantwortlich für die Erarbeitung und Erreichung der im Projektauftrag und Pflichtenheft bestimmten Projektziele. Sie hat das Recht, Entscheidungsvorlagen für den Lenkungsausschuss zu erarbeiten.

Aufgaben der Projektleitung sind:

die Erarbeitung des Projekthandbuches und des Pflichtenheftes,
die Erarbeitung der Vorschläge für die Benennung
der Verantwortlichen für die fachliche Durchführung und Umsetzung der Teilprojekte bzw. Teilaufgaben und
die weitere Zusammensetzung der Projektgruppe,

ggf. der Entwurf des Projektstrukturplanes, das Ableiten der Arbeitspakete und die Aufgabenverteilung in der Projektgruppe,
die Organisation und Moderation der Projektgruppensitzungen und das Festlegen der Projektarbeitsregeln,
die ständige Prüfung und Abnahme der Arbeitsergebnisse der Projektgruppenmitglieder (Qualitätssicherung),
die Präsentation der fachlichen Ergebnisse im Lenkungsausschuss,
die Prüfung der Beteiligung der Personalvertretung, der Gleichstellungsbeauftragten, der Schwerbehindertenvertretung,
die Dokumentation aller wichtigen Projektergebnisse.

7.4 Projektmitarbeiterinnen und -mitarbeiter

Projektmitarbeiterinnen und -mitarbeiter sind alle Personen, die auf Vorschlag der Projektleiterin/des Projektleiters nach Bestätigung des Projektauftrags der Projektgruppe zugeordnet sind.
Der Projektgruppe ständig zugeordnete Mitarbeiterinnen und Mitarbeiter werden gem. GO BStU für die Dauer der Projekte ganz oder teilweise von Aufgaben des laufenden Tagesgeschäftes freigestellt und für das Projekt fachlich ausschließlich der Projektleiterin/dem Projektleiter unterstellt.

Die prozentuale Verfügbarkeit von nur zeitlich begrenzt dem Projekt zugeordneten Projektmitarbeiterinnen oder -mitarbeitern ist mit deren direkten Vorgesetzten (ab Referatsebene) abzusprechen und im Projektauftrag zu dokumentieren.

Bei Konflikten entscheidet der Lenkungsausschuss.

7.5 Referat Organisation

Die Leiterin/der Leiter des Referats Organisation ist verantwortlich für die Planung, Organisation und Umsetzung von Standardprojekten.

Auf Grundlage der eingereichten Projektanträge werden die Projektorganisation als Standard- oder Großprojekt festgelegt und die Entscheidungsvorlagen für den Lenkungsausschuss erarbeitet.

7.6 IT-Koordinatoren

In jeder Fachabteilung ist für alle IT-Abstimmungen mit der Abteilung ZV und für IT-Projekte ein IT-Koordinator eingesetzt und ein Stellvertreter festgelegt. Dieser ist als Ansprechpartner des Auftraggebers für alle IT-spezifischen Anfragen und Abstimmungen im Rahmen von IT-Projekten zuständig.

Aufgaben sind:

die abteilungsinterne Abstimmung und Vorbereitung der Initiierung von IT-Projekten
die Erstellung und Abstimmung von fachlichen Anforderungskatalogen (Lastenheft),
die Prüfung der Vollständigkeit und fachlichen Richtigkeit der Pflichtenhefte,
die fachliche Unterstützung des IT-Architekturbüros,
die fachliche Unterstützung bei Ausschreibungsverfahren,
die Koordinierung von Anwendertests und Inbetriebnahmeverfahren,
die Sicherstellung, dass Lastenhefte, Pflichtenhefte und Abnahmedokumente durch die Abteilungsleitung freigegeben werden.

7.7 IT-Architekturbüro und IT-Architekturausschuss

Das IT-Architekturbüro setzt sich zusammen aus einem oder zwei Spezialisten für IT-Anwendungsarchitekturen.

Das IT-Architekturbüro leitet den IT-Architekturausschuss. Diesem gehören neben dem IT-Architekturbüro die IT-Koordinatorinnen und IT-Koordinatoren der Abteilungen und darüber hinaus beratende Vertreter mit fachlicher Entscheidungskompetenz des IT-Referates an.

Aufgaben sind:

die Festlegung der IT-Anwendungsarchitektur für IT-Fachanwendungen,
die Bewertung von Fachanforderungen (Lastenheft) und deren Abstimmung mit der Fachabteilung über den IT-Koordinator,
die Erstellung des Teils des Pflichtenheftes für IT-Großprojekte bezüglich der IT-Infrastruktur,
die fachliche Unterstützung und Bewertung bei Erstellung von Ausschreibungsunterlagen,
die Unterstützung bei der Erstellung von Umsetzungsplanungen und Abnahmekatalogen,
die technisch-inhaltliche Qualitätssicherung,
die Durchführung von Marktsichtungen, Herstellung von Kontakten zu Anbietern und Behörden.

8. Wirtschaftlichkeitsuntersuchung und Vergabevorschriften

Für alle finanzwirksamen Maßnahmen sind angemessene Wirtschaftlichkeitsuntersuchungen durchzuführen. Hierzu sind die Vorschriften der VV Nr. 2 bis 2.4.4 zu § 7 BHO zu beachten.

Für die Erstellung der Wirtschaftlichkeitsbetrachtung ist diejenige oder derjenige verantwortlich, der das Pflichtenheft oder das erweiterte Lastenheft für die Ausschreibungsunterlagen erarbeitet. Dies gilt auch für die Wirtschaftlichkeitsbetrachtung, die im Fall der externen Vergabe der Leistung im Vorfeld zu erbringen ist.

Das Verfahren zur Durchführung der Wirtschaftlichkeitsbetrachtung ist gesondert geregelt.

Die Zustimmung der Titelverwalter und/oder der bzw. des Beauftragten für den Haushalt für die in Anspruch zu nehmenden Leistungen ist von der Projektleiterin bzw. dem Projektleiter einzuholen.

Bei Inanspruchnahme von Leistungen im Rahmen eines Projekts, die nach den geltenden Vergabebestimmungen auszuschreiben bzw. gemäß der „Richtlinie für Beschaffungsvorhaben“ (Erlass Z 5 – 007 634 112/52 vom 14. März 2003) die Beteiligung des Beschaffungsamtes beim BMI vorsehen, sind die dafür erforderlichen Zeiträume (Mindestvorlauf grundsätzlich 18 Monate) bei der Projektplanung zu berücksichtigen.

9. Projektstart und Projektdokumentation

Ein Projekt startet grundsätzlich mit einer Eröffnungsveranstaltung (Projekt-Kick-Off), die der Projektgruppe Gelegenheit gibt, sich kennen zu lernen, die Projektziele zu erörtern, die Regeln der Zusammenarbeit festzulegen sowie einen gemeinsamen Informationsstand für alle Projektbeteiligten herzustellen.

Über den gesamten Projektverlauf ist von der Projektgruppe eine Projektdokumentation zu erstellen.

Die Projektdokumentation enthält zumindest:

- den Projektantrag Vd.-Nr. BStU 15-001,
- das Lastenheft Vd.-Nr. BStU 15-002 (Fachanforderung)
- den bestätigten Projektauftrag Vd.-Nr. BStU 15-003,
- das Projekthandbuch,
- das Pflichtenheft Vd.-Nr. BStU 15-004 (Leistungsangebot)
- die Wirtschaftlichkeitsuntersuchung,
- die Sachstandsberichte (Statusberichte),
- die Sitzungsprotokolle,
- die Abnahmedokumentation,
- die Betriebsübergabeprotokolle,
- den Abschlussbericht.

Der notwendige weitere Inhalt der Projektdokumentation ist mit der Projektservicestelle abzustimmen.

Für das Projekt ist durch das Referat Informations- und Telekommunikationstechnik ein Projektordner auf einem Gruppenlaufwerk mit Zugriffsrechten für alle am Projekt Beteiligten anzulegen.

10. Projektabschluss

Zum Abschluss jedes Projekts ist ein Projektabschlussbericht zu fertigen. Darin wird gegenüber dem Lenkungsausschuss Rechenschaft über Verlauf und Ergebnisse des Projekts abgelegt.

Soweit das Projektergebnis nicht im Konsens der Projektgruppenmitglieder entwickelt wurde, sind abweichende Stellungnahmen Einzelner zu dokumentieren und dem Projektabschlussbericht beizufügen.

Der Projektabschlussbericht bildet die Voraussetzung für die Projektabnahme durch den Lenkungsausschuss. Mit der Projektabnahme ist das Projekt formal abgeschlossen, wird die Projektleiterin/der Projektleiter von ihrem/seinem Auftrag entbunden, die Projektgruppe aufgelöst und die Projektgruppenmitglieder aus ihrer Projektverantwortung entlassen.

Die Projektdokumente sind in der Projektservicestelle zur Ablage zu bringen.

11. Übergangsbestimmungen und Inkraftsetzung

Nach Inkraftsetzung dieser Richtlinie sind ggf. noch nicht erfasste IT-Projekte im Sinne dieser Richtlinie vom Auftraggeber bzw. Projektverantwortlichen innerhalb einer Frist von 4 Wochen der Projektservicestelle zur Registrierung anzuzeigen.

Gleichzeitig wird die Organisationsverfügung 04/04 - Richtlinie zum Projektmanagement bei der BStU vom 25.06.2004 außer Kraft gesetzt.

---

* Praxisleitfaden Projektmanagement (in der jeweils aktuellen Fassung)