

• Ministerium für  
Inneres und Sport



**Erlass**  
**Informationssicherheit**  
**im Informationsverbund**  
**der Vollzugspolizei des Saarlandes**

**Ministerium für Inneres und Sport**

Version: 1.0

Stand: 24.08.2016

\* den Anforderungen des Landesgleichstellungsgesetzes zur Gleichstellung der Geschlechter (§ 28 LGG) wird durch Verwendung der sogenannten Gender-Gap Schreibweise Rechnung getragen.

## Inhaltsverzeichnis

1	Vorbemerkung.....	3
2	Geltungsbereich.....	3
3	Ziele, Prinzipien und Strategie der Informationssicherheit.....	4
3.1	Ziele der Informationssicherheit.....	4
3.2	Prinzipien der Informationssicherheit.....	4
3.3	Strategie der Informationssicherheit.....	5
4	Zielgruppen.....	6
4.1	AnwenderInnen.....	6
4.2	Dienststellenleitung.....	6
4.3	Dritte.....	6
4.4	Sonderstellung.....	6
5	Organisation des Informationssicherheitsmanagements.....	7
6	Umsetzung des Informationssicherheitserlasses.....	8
7	Regelungskompetenz und -erfordernis.....	8
7.1	Regelungskompetenz.....	8
7.2	Regelungserfordernis.....	8
8	Rechtsfolgen unzulässigen Verhaltens.....	8
9	Inkrafttreten.....	9

## 1 Vorbemerkung

Polizeiliches Handeln ist ohne Informationstechnik (IT), die IT-Systeme und IT-Verfahren nicht mehr denkbar. Die immer komplexer werdende Nutzung der IT, die vielerlei Risiken mit sich bringt, ist sicher und angemessen zu gestalten.

Mit der Entwicklung von Bund-Länder übergreifenden IT-Verfahren und deren Einführung wurde für die Polizeien in Bund und Ländern durch den Arbeitskreis II (AK II) der Ständigen Konferenz der Innenminister und -senatoren der Länder (IMK) ein einheitlicher Sicherheitsstandard gemäß den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) festgeschrieben<sup>1</sup>. Bei den Regelungen zur Informationssicherheit der Vollzugspolizei des Saarlandes werden die aus der Gremienstruktur der IMK entstandenen Beschlüsse beachtet und entsprechend den Möglichkeiten des Landeshaushaltes umgesetzt. Abweichende oder ergänzende spezialgesetzliche Regelungen bleiben davon unberührt.

Verbindliche Vereinbarungen und Transparenz bei der Umsetzung von gemeinsam beschlossenen Maßnahmen bilden dabei die Grundlage für eine vertrauensvolle Zusammenarbeit der Polizeibehörden und für ein vertrauenswürdiges Verhältnis zum Bürger.

Dieser Erlass schreibt die erforderlichen Rahmenbedingungen für eine rechtmäßige, sichere und störungsfreie Verarbeitung von Daten und die Verantwortlichkeiten im Informationsverbund der Vollzugspolizei des Saarlandes unter Beachtung der darauf anwendbaren einschlägigen Gesetze und Vorschriften fest.

## 2 Geltungsbereich

Der Informationssicherheitserlass ist anzuwenden auf den Informationsverbund der Vollzugspolizei des Saarlandes (IV-SLPOL).

Verantwortlich für die Einhaltung von Maßnahmen und Aufgaben zur Informationssicherheit sind das für die Vollzugspolizei zuständige Ministerium sowie die Leitung der Behörde der Vollzugspolizei des Saarlandes.

Als übergeordnete Einrichtung besteht fachliche Weisungsbefugnis der IT-Koordination des Ministeriums gegenüber der IT-Koordination der Vollzugspolizei des Saarlandes und deren nachgeordneten IT-Fachdienststellen. Die für die jeweilige Behörde zuständige IT-Koordination ergibt sich aus dem jeweils gültigen Organigramm der Behörde.

Die originären Zuständigkeiten und Aufgaben der IT-Fachdienststellen der Vollzugspolizei des Saarlandes sind im Geschäftsverteilungsplan des Landespolizeipräsidiums der Vollzugspolizei des Saarlandes aufgeführt.

---

<sup>1</sup> Beschlussniederschrift 190. Sitzung des Arbeitskreises II TOP 16.2

### 3 Ziele, Prinzipien und Strategie der Informationssicherheit

Die Ziele und Prinzipien der Informationssicherheit orientieren sich an den Vorgaben und Ausführungen des BSI zum IT-Grundschutz. Der IT-Grundschutz gibt somit die Standards für die Informationssicherheit der Datenverarbeitung im IV-SLPOL vor.

#### 3.1 Ziele der Informationssicherheit

Für die Vollzugspolizei des Saarlandes werden folgende Informationssicherheitsziele vorgegeben:

- Gewährleistung der Grundwerte Verfügbarkeit, Vertraulichkeit und Integrität der Geschäftsprozesse zur Sicherstellung der Aufgabenerfüllung der Vollzugspolizei des Saarlandes.
- Betrieb der für die Geschäftsprozesse notwendigen IT-Systeme auf dem Niveau des für den Geschäftsprozess festgelegten Schutzbedarfes der Grundwerte. Festlegung von technischen und organisatorischen Maßnahmen im IV-SLPOL insbesondere unter Beachtung des Saarländischen Datenschutzgesetzes (SDSG) und/oder der Verschlusssachenanweisung für das Saarland (VSA Saarland).
- Adäquater Umgang mit der anvertrauten Technik zur Vermeidung von physikalischen Schäden.
- Schaffung einer strategischen Vorsorge- und Ausfallplanung zur Minimierung von Risiken sowie zur Gewährleistung eines angemessenen und effektiven Krisen- und Notfallmanagements bei IT-Verfahren, -Systemen und -Netzen.

Es soll eine kontinuierliche Verbesserung des sicheren Umgangs mit Informationen und Informationstechnik in den jeweiligen Verantwortungsbereichen erreicht werden.

#### 3.2 Prinzipien der Informationssicherheit

- **Sicherheit vor Verfügbarkeit**  
Im Falle erkannter Schadensrisiken für die IT der Vollzugspolizei des Saarlandes wird zum Erhalt von Funktionsfähigkeit und Aufgabenerfüllung der Vollzugspolizei dem Schutz der Informationen Vorrang eingeräumt.  
Zeitweilige Einschränkungen bei der IT- Nutzung müssen hingenommen werden. Insbesondere kann es zu Verbindungsunterbrechungen zu anderen Netzen kommen.
- **Maximalprinzip**  
Der Schutzbedarf polizeilicher IT (Anwendungen, Systeme und Netze) orientiert sich an den Informationen mit dem höchsten Schutzbedarf.
- **Minimalprinzip**  
Je höher der ermittelte Schutzbedarf für den Grundwert Vertraulichkeit, desto restriktiver ist der Zugriff auf die gespeicherten Informationen zu prüfen.

### 3.3 Strategie der Informationssicherheit

Nur eine den Zielen und Prinzipien der Informationssicherheit angepasste Strategie gewährleistet die durch den Betrieb des IV-SLPOL entstehenden Risiken zu minimieren und somit auf einem tragbaren Niveau zu halten. Daraus resultieren unter anderem nachfolgende technische und organisatorische Mindestanforderungen:

- Alle Maßnahmen orientieren sich am Stand der Technik und den in den zuständigen Gremien verabschiedeten Vereinbarungen.
- Der IV-SLPOL ist durch Sicherheitsgateways von anderen Netzen zu trennen.
- Alle ein-und ausgehenden Verbindungen des IV-SLPOL zu anderen Netzen sind über Sicherheitsgateways zu führen.
- Der IV-SLPOL ist durch vorbeugende Maßnahmen gegen die Einschleusung von Schadcode zu schützen z.B. durch
  - Nutzung eines Virenschutzprogramm
  - Regelungen zur Nutzung endgerätespezifischer Schnittstellen
  - Monitoring.
- Jede IT-Nutzung im IV-SLPOL, die gegen geltendes Recht verstößt, den Interessen der Vollzugspolizei des Saarlandes oder deren Ansehen in der Öffentlichkeit schaden könnte, ist unzulässig. Dies gilt insbesondere für ein Verhalten von Anwendern im IV-SLPOL, das
  - gegen datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstößt,
  - von beleidigendem, verleumderischem, verfassungsfeindlichem, rassistischem, sexistischem, pornografischem oder diskriminierendem Inhalt ist,
  - kommerziell oder rein der Unterhaltung dienend ausgelegt ist.
- Für jeden im IV-SLPOL relevanten<sup>2</sup> IT-gestützten Geschäftsprozess ist orientiert an der Vorgehensweise der gültigen Standards des BSI ein Sicherheitskonzept zu erstellen.

---

<sup>2</sup> Relevant ist jeder IT –gestützte Geschäftsprozess aufgrund rechtlicher Vorgaben aus den §§ 7 und 9 DSGVO, anderer gesetzlicher Vorgaben oder aufgrund organisatorischer Entscheidung durch die Dienst- und Fachaufsicht oder Behördenleitung auf Vorlage durch das ISMT.

## 4 Zielgruppen

### 4.1 Anwender\_innen

Betroffen sind alle Anwender\_innen der IT im IV-SLPOL.

Jede\_r Anwender\_in trägt die persönliche Verantwortung für den sicheren und rechtmäßigen Umgang mit den Informationen, die sie oder er im IV-SLPOL verarbeitet. Daher ist jede\_r Anwender\_in im Umgang mit den eingesetzten IT-Systemen und IT-Verfahren vor der Nutzung zu informieren, einzuweisen oder zu beschulen.

Anwender\_innen haben sich im Rahmen ihrer Möglichkeiten über Sicherheitsrisiken, die dem IV-SLPOL durch die Nutzung von IT-Geräten/IT-Verfahren drohen, zu informieren.

### 4.2 Dienststellenleitung

Der Dienststellenleitung obliegt für ihren Geschäftsbereich die Verantwortung für den ordnungsgemäßen Einsatz der Informationstechnik insbesondere unter Beachtung der daten- und geheimhaltungszurechtlichen Vorschriften.

### 4.3 Dritte

Bei entsprechender Relevanz für den IV-SLPOL sind Dritte, wie z. B. Vertrags- und Geschäftspartner (Privatwirtschaft/Behörden), auf die Einhaltung der im IV-SLPOL gültigen Sicherheitsbestimmungen, Vertragspartner aus der Privatwirtschaft darüber hinaus auch auf die VSA Saarland, durch den Auftraggeber vertraglich zu verpflichten.

### 4.4 Sonderstellung

- **Administratoren\_innen** haben im Informationsverbund der Vollzugspolizei des Saarlandes eine besondere Stellung, da ihnen die Betreuung zentraler Systeme und Verfahren obliegt.
- **Lokale IT-System- und Anwenderbetreuer\_innen** sind keine Administratoren\_innen<sup>3</sup>. Sie wirken unter anderem an der Wartung und Instandhaltung der IT-Systeme und an der Nutzung der Software bei den Dienststellen der Vollzugspolizei des Saarlandes mit und sind somit direkte Ansprechpartner\_innen der IT-Anwender\_innen der Vollzugspolizei des Saarlandes vor Ort.

Ein verantwortliches, vertrauliches und sicherheitskonformes Verhalten ist für beide Gruppen zwingende Voraussetzung. Sie sind für ihre Aufgabengebiete zu schulen. Das dabei erlernte und erarbeitete Wissen ist durch regelmäßige, auch eigenverantwortliche Fortbildung auf einem aktuellen Wissensniveau zu halten bzw. zu vertiefen. Details sind durch den zuständigen IT-Fachdienst und die Dienststellenleitung zu regeln.

---

<sup>3</sup> vgl. Erlass über die Auswahl, die Aufgaben und den Einsatz von System- und Anwenderbetreuern/-betreuerinnen in der IT der saarländischen Vollzugspolizei

## 5 Organisation des Informationssicherheitsmanagements

Die Dienst- und Fachaufsicht über die Informationssicherheit der Vollzugspolizei des Saarlandes, sowie deren Koordination erfolgt durch das für die Vollzugspolizei zuständige Ministerium. Zur Aufgabenwahrnehmung beruft das Ministerium eine\_n Strategische\_n Informationssicherheitsbeauftragte\_n für die Vollzugspolizei des Saarlandes (SIS).

Ansprechpartner der IT-Koordination des Ministeriums ist die dem Ministerium nachgeordnete Behörde der Vollzugspolizei des Saarlandes.

Die Bearbeitung und Koordination aller Belange der Informationssicherheit und deren Integration in der nachgeordneten Behörde erfolgt durch das Informationssicherheits-Management-Team (ISMT). Die Befugnisse und Aufgaben orientieren sich am jeweils gültigen „Standard für das Informationssicherheitsmanagement bei den Polizeien des Bundes und der Länder.“

Dem ISMT gehören mindestens an

- a. Strategische\_r Informationssicherheitsbeauftragte\_r für die Vollzugspolizei des Saarlandes (SIS)
- b. Operative\_r Informationssicherheitsbeauftragte\_r für die Vollzugspolizei des Saarlandes (OISM)
- c. Behördliche\_r Datenschutzbeauftragte\_r (bDSB)
- d. Geheimschutzbeauftragte\_r (GB)
- e. IT-Notfallbeauftragte\_r (IT-NFB).
- f. für die Strategie der polizeilichen IT Verantwortliche\_r
- g. für den Betrieb der polizeilichen IT Verantwortliche\_r.

Die vollständige Zusammensetzung des ISMT und dessen Aufgaben sind in einer Geschäftsordnung zu regeln. Das ISMT tagt unter dem Vorsitz des\_r Strategischen Informationssicherheitsbeauftragten.

Die unter b-e genannten Mitglieder werden zum Zwecke der Aufgabenwahrnehmung durch die nachgeordnete Behörde der Vollzugspolizei des Saarlandes benannt.

## **6 Umsetzung des Informationssicherheitserlasses**

Im IV-SLPOL sind die Ziele dieses Erlasses zu beachten. Er ist den Mitarbeiter\_innen der Vollzugspolizei des Saarlandes zur Kenntnis zu geben. Darauf basierende Dokumente (Richtlinien, Dienstanweisungen und Leitfäden) sind allen Mitarbeiter\_innen in geeigneter Weise zur Verfügung zu stellen.

## **7 Regelungskompetenz und -erfordernis**

### **7.1 Regelungskompetenz**

Die Behörde der Vollzugspolizei des Saarlandes kann im Sinne dieses Erlasses bzw. darauf beruhender Richtlinien (RL) des Ministeriums Detailregelungen in Form einer Dienstanweisung (DA) oder eines Leitfadens (LF) erstellen. Diese dürfen den Grundsätzen dieses Erlasses und darauf basierender Richtlinien nicht widersprechen. Sie sind in enger Zusammenarbeit mit dem Informationssicherheitsmanagement zu erarbeiten und vor Inkrafttreten der Polizeiabteilung im Ministerium zur Zustimmung vorzulegen.

Verantwortliche Stellen<sup>4</sup> der Vollzugspolizei des Saarlandes können aufgrund betrieblicher/technischer Umsetzungsnotwendigkeiten entsprechende Leitfäden, unter Beteiligung des ISMT erarbeiten. Werden diese durch die Dienststellenleitung in Kraft gesetzt, sind sie als Anlage zum jeweiligen Hauptdokument (RL oder DA) aufzunehmen.

### **7.2 Regelungserfordernis**

Die aufgrund dieses Erlasses weiteren Regelungserfordernisse (Richtlinien, Dienstanweisungen, Handlungsanleitungen) für das Ministerium und die Behörde der Vollzugspolizei des Saarlandes ergeben sich aus den Grundschutzkatalogen des BSI.

## **8 Rechtsfolgen unzulässigen Verhaltens**

Verstöße gegen diesen Erlass und/oder darauf beruhender Richtlinien, Dienstanweisungen oder Handlungsanleitungen können abhängig von Art, Schwere und Umfang des unzulässigen Verhaltens dienstrechtliche, disziplinarrechtliche, arbeitsrechtliche und/oder strafrechtliche Konsequenzen nach sich ziehen.

---

<sup>4</sup> vgl. GO-LPP

## 9 Inkrafttreten

Der Erlass Informationssicherheit im Informationsverbund der Vollzugspolizei des Saarlandes tritt mit Datum vom 24.08.2016 in Kraft und setzt den

- Erlass zu IT-Sicherheit und Datenschutz bei der Vollzugspolizei des Saarlandes vom 01.01.2009

sowie die

- Informationssicherheitsleitlinie der Vollzugspolizei des Saarlandes vom 07.05.2010
- außer Kraft.

Saarbrücken, den 24.08.2016  
Im Auftrag

Ulrich Schmal