Polizei
SAARLAND

Handlungsempfehlung zum Umgang mit Informationen

-Langfassung-

Landespolizeipräsidium

Präsidialstab

Az.: PS1-99.00-37/2014

Stand: **Juli 2015**

Die vorliegende Handlungsempfehlung zielt darauf ab, die Mitarbeiterinnen und Mitarbeiter des Landespolizeipräsidiums (LPP)

- für den verantwortungsvollen Umgang mit Informationen zu sensibilisieren,
- über Möglichkeiten der Informationsklassifizierung zu informieren,
- bei der Umsetzung von Maßnahmen zum Schutz von Informationen zu unterstützen,

und somit die Handlungssicherheit beim Umgang mit Informationen zu erhöhen.

Bereichsspezifische Reglungen, insbesondere die Verschlusssachenanweisung für das Saarland, werden von der vorliegenden Handlungsempfehlung nicht berührt.

Informationsklassifizierung
Grundlage für Maßnahmen zum Schutz einer Information ist die Festlegung der richtigen Schutzklasse. Hierfür bietet sich folgendes Raster an:

- Öffentlich (allgemein zugänglich, offen)
  Die Information ist öffentlich verwendbar und allgemein zugänglich, bspw. über den Internetauftritt der Polizei.
  Beispiele: Veröffentlichte Pressemitteilungen, Statistiken, Broschüren, polizeiliche Handlungsempfehlungen im Rahmen der Prävention.

- Intern (für Berechtigte zugänglich, geschlossen)
  Die Information steht allen Mitarbeiterinnen und Mitarbeitern des LPP bzw. benachbarten/vorgesetzten Behörden und Organisationen (z. B. Staatsanwaltschaft, andere Polizeibehörden) zur Verfügung und ist zum internen Gebrauch bestimmt. Das „Öffentlichmachen“ der Information kann zu einer Beeinträchtigung der polizeilichen Aufgabenerledigung führen.
  Beispiele: Gesamttelefonverzeichnis des LPP, Organigramme mit personenbezogenen Daten, Mitarbeiterbriefe, Bekanntmachungen im Intranet, Dienstanweisungen, Organisationskennzahlen, Lagebilddaten einer PI.

- Schutzwürdig (eingeschränkt für Berechtigte zugänglich, verschlossen)
  Die Offenlegung der Information kann negative Konsequenzen für die polizeiliche Aufgabenerledigung nach sich ziehen und zu einem Schaden für das LPP führen.
  Beispiele: Erkenntnisse aus polizeilichen Dateien (z. B. POLIS), Personaldaten, POLADIS-Rapporte, Bewerbertableaus, Personalstärken, taktische Konzepte, Einsatzbefehle.

- Besonders schutzwürdig (grundsätzlich nicht zugänglich, versiegelt)
  Die Information steht nur einem eng begrenzten, berechtigten Personenkreis zur Verfügung. Die Veröffentlichung der Information kann schwerwiegende negative Konsequenzen für die polizeiliche Aufgabenerledigung nach sich ziehen bzw. einen großen Schaden für das LPP verursachen.
  Beispiele: PKS vor Veröffentlichung, Vergabeverfahren für Dienst-Kfz, Kennzahlen mit Personenbezug, Personal- und Krankheitsakten, geschützter POLADIS-Vorgang, verdeckte Ermittlungen.

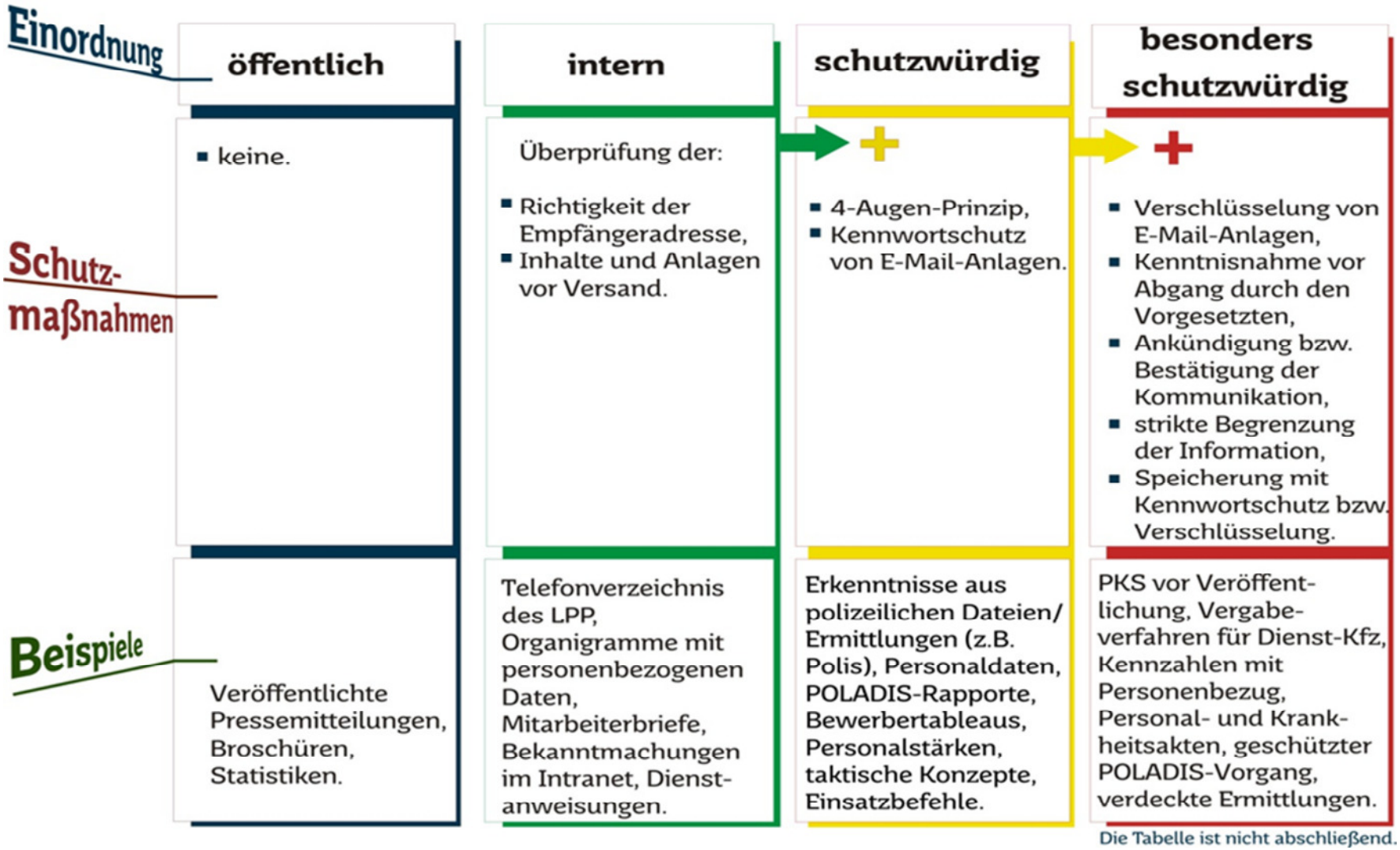
Maßnahmen zum Schutz von Informationen
Für den Umgang mit Informationen gilt der Grundsatz: Je größer der mögliche Schaden, desto umfangreicher die zu ergreifenden Schutzmaßnahmen.

Insbesondere bei der Kommunikation mit elektronischen Mitteln (z. B. E-Mail, Smartphone, Internet, Social Media) ist besondere Vorsicht geboten. Zum einen ist die elektronische Kommunikation für Vertraulichkeitsverluste besonders anfällig – häufigste Fehlerursache ist die Auswahl falscher Adressen oder Anlagen. Zum anderen kann eine Verbreitung in der Regel nicht rückgängig gemacht werden, eine Schadensbegrenzung ist somit äußerst schwierig bis unmöglich.

Allgemein sind folgende Sicherheitsmaßnahmen zu beachten:

- Schützen Sie dienstliche Informationen, Unterlagen oder Datenträger vor unberechtigtem Zugriff (z. B. durch Nutzung des Verwahrgelasses).
- Sperren Sie bei jedem Verlassen des Arbeitsplatzes den PC gegen unbefugten Zugang.
- Stellen Sie vor dem Versenden die Auswahl der richtigen (E-Mail-)Adresse sowie Anlage sicher.
- Ziehen Sie alternative Kommunikationsformen in Betracht.
- Prüfen Sie kritisch die Erforderlichkeit der Weitergabe (besonders) schutzwürdiger Informationen. Eventuell kann der Informationsbedarf des Empfängers durch die Weitergabe von Auszügen, Zusammenfassungen oder anonymisierten Daten gedeckt werden, die „intern“ oder „öffentlich“ klassifiziert werden können.
- Passen Sie Ihre Sicherheitsmaßnahmen im Einzelfall situationsbedingt an. Beispiele: Vermeiden Sie das Mitlesen/Mithören unberechtigter Personen. Schließen Sie die unberechtigte Kenntnisnahme beim Ausdruck über Flur- bzw. Gemeinschaftsdrucker sicher. Lassen Sie dienstliche Unterlagen nicht unbeaufsichtigt.

Folgende Schutzmaßnahmen werden für den Umgang mit Informationen empfohlen:



Die Tabelle ist nicht abschließend.

Erläuterungen zu den einzelnen Schutzmaßnahmen

- Überprüfung der Richtigkeit der Empfängeradresse
  Adressdaten sind zu überprüfen, falls möglich unter Anwendung des Vier-Augen-Prinzips. Beim E-Mail-Versand bietet sich zusätzlich die Nutzung des elektronischen Adressregisters bzw. vorbereiteter E-Mail-Verteiler an.

- Überprüfung der Inhalte/Anlagen vor Versand
  Schriftstücke, E-Mails und Datenträger sind vor Versand auf Vollständigkeit und Korrektheit der Inhalte und Anlagen zu prüfen. Auf eine empfängerorientierte Informationsauswahl ist bei der Weitergabe zu achten, weitergehende Inhalte sind zu löschen bzw. schwärzen.

- Vier-Augen-Prinzip
  Überprüfung der Kommunikationsinhalte/-anlagen vor Versand durch eine zweite Person (z. B. Vorgesetzter).

- Einsatz von Kennwortschutz und Verschlüsselung
  Beim Austausch (besonders) schutzwürdiger Informationen mittels elektronischer Kommunikation (z. B. E-Mail) sind die Daten mittels Kennwort bzw. Verschlüsselung gegen unbefugte Kenntnisnahme zu sichern. Die Informationen werden hierzu in einer Datei gespeichert, die mit einem Kennwort bzw. Verschlüsselungsprogramm geschützt wird. Die geschützte Datei wird der E-Mail als Anlage beigefügt. Der eigentliche Text der Nachricht bleibt hierbei ungesichert. Voraussetzung ist ein kompatibles Kennwort- bzw. Verschlüsselungsprogramm bei Sender und Empfänger. Das Kennwort bzw. der Schlüssel wird entweder telefonisch oder mit separater E-Mail an den/die Empfänger übertragen.
  Besonders schutzwürdige Informationen sind grundsätzlich mit Kennwort bzw. Verschlüsselung abzuspeichern.

  - Kennwortschutz mittels Microsoft Office
    Aufgrund der weiten Verbreitung und einfachen Handhabung von Microsoft Office eignet sich der Kennwortschutz für die interne und externe E-Mail-Kommunikation. (Register Datei => Informationen => Dokument/Präsentation/Arbeitsmappe schützen)

  - Verschlüsselung mittels Osborn Advanced File Security (AFS)
    Die Anwendung AFS steht im Polizeinetz zur Verfügung und bietet einen hohen Verschlüsselungsstandard. Beim Versand von Anlagen an LPP-externe Empfänger ist auf die Programmkompatibilität (AFS Version 3.0) zu achten. (Windows Start => Alle Programme => Osborn Software)

- Ankündigung bzw. Bestätigung der Kommunikation
  Die Maßnahme sieht die Ankündigung des Informationsaustauschs vor Absendung bzw. die Bestätigung des Eingangs der Nachricht vor. Die Verwendung vorhandener Nachrichtenoptionen (z. B. elektronische Übermittlungs- und Lesebestätigungen bei E-Mail und Telefax) wird empfohlen, setzt jedoch die Kompatibilität der benutzten Systeme voraus. Im Bereich der E-Mail-Kommunikation wird eine unverzügliche schriftliche oder fernmündliche Bestätigung des Eingangs angeregt.

- Strikte Begrenzung der Information
  Die Begrenzung kann auf Mitarbeiter von Organisationseinheiten oder auf bestimmte namentlich ausgewählte Personen erfolgen. Die Empfänger sind auf die Vertraulichkeit der Information hinzuweisen. Eine Informationsübermittlung an Dritte steht unter dem Entscheidungsvorbehalt der verantwortlichen Stelle. Die Datenträger bzw. Schriftstücke sind verschlossen aufzubewahren. Elektronisch gespeicherte Daten sind nur falls erforderlich auszudrucken.

- Speicherung mit Kennwortschutz bzw. Verschlüsselung
  Die Datei wird mit Kennwort bzw. verschlüsselt gespeichert. Eine unbefugte Kenntnisnahme kann hierdurch gänzlich ausgeschlossen werden. Auf die Ausführungen zu Kennwortschutz und Verschlüsselung wird hingewiesen.

Für Fragen stehen Ihnen folgende Ansprechpartner zur Verfügung

- Softwareanwendungen (Microsoft Office, AFS)
  Die System- und Anwendungsbetreuer (LPP 4.3.2), Telefon 7-63-4399

- Behandlung von Verschlusssachen
  Der Geheimschutzbeauftragte
  Herr KHK Markus Burckhardt (LPP/PS 1), Telefon 7-63-8013

- Schutz personenbezogener/datenschutzrelevanter Daten
  Der behördliche Datenschutzbeauftragte
  Herr KHK Marko Groß (LPP/PS 1), Telefon 7-63-8018

- Informationssicherheit und IT-Geheimschutz
  Der operative Informationssicherheitsbeauftragte und IT-Geheimschutzbeauftragte
  Herr POK Volker Schwindling (LPP 4.0), Telefon 7-63-4023

Weitergehende Informationen

- Polizeidienstvorschrift 810.1 Formelle elektronische Kommunikation (Elektronische Post).
- Ministerium für Inneres und Europaangelegenheiten, Erlass zu IT-Sicherheit und Datenschutz bei der Vollzugspolizei des Saarlandes, Az. 98.00 D1/IT-Sicherheit, vom 01.01.2009.
- Ministerium für Inneres und Europaangelegenheiten, Verschlusssachenanweisung für das Saarland (VSA Saarland), Az. 58.10, vom 16.03.2010.
- Ministerium für Inneres und Europaangelegenheiten, Dienstanweisung zur Nutzung der Dienste elektronische Post (nicht formelle Kommunikation) und Internet bei der Vollzugspolizei des Saarlandes, Az. 98.00-1556/2010, vom 20.05.2010.
- Ministerium für Inneres und Europaangelegenheiten, Rahmendienstanweisung über die Sicherheitsanforderungen im Netz der Vollzugspolizei des Saarlandes, Az. D1-98.00, vom 11.08.2010.
- Landespolizeipräsidium, Geschäftsordnung des Landespolizeipräsidiums der Vollzugspolizei des Saarlandes, Az. PS1-17.06-452/2013, vom 01.12.2014.