Elektronische Kommunikation

Die digitale Informationsverarbeitung verlangt eine besondere Achtsamkeit beim Umgang mit den eigenen und fremden Daten. Insbesondere bei der elektronischen Kommunikation, z. B. mittels E-Mail, Smartphone, Internetchat oder bei der Nutzung sozialer Netzwerke, ist besondere Vorsicht geboten.

Die häufigste Ursache für den Vertraulichkeitsverlust von Informationen ist Unachtsamkeit, wie beispielsweise die Auswahl falscher Adressen oder Anlagen beim Versenden von E-Mails.

Eine solche Weitergabe von Informationen ist in der Regel nicht rückgängig zu machen. Die Schadensbegrenzung ist äußerst schwierig bis unmöglich !

Speichern Sie deshalb (besonders) schutzwürdige Informationen in gesonderten Dateien und fügen diese der elektronischen Kommunikation (z. B. E-Mail) als geschützte bzw. verschlüsselte Anlage bei. Beachten Sie, dass der eigentliche Nachrichtentext hierbei ungeschützt bzw. unverschlüsselt bleibt !

Kennwortschutz von Office-Dokumenten

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 mit Advanced File Security (AFS)

Die Anwendung AFS steht im Polizeinetz zur Verfügung. Beim Versand von Anlagen an LPP-externe Empfänger ist auf die Programmkompatibilität (AFS Version 3.0) zu achten. (Windows Start => Alle Programme => Osborne Software)

Weitere Informationen

ⓘ 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/ IT-Geheimschutzbeauftragte
Herr POK Volker Schwindling (LPP 4.0)
Telefon 7-63-4023

ⓘ Intranet: Wissen/Vorschriften

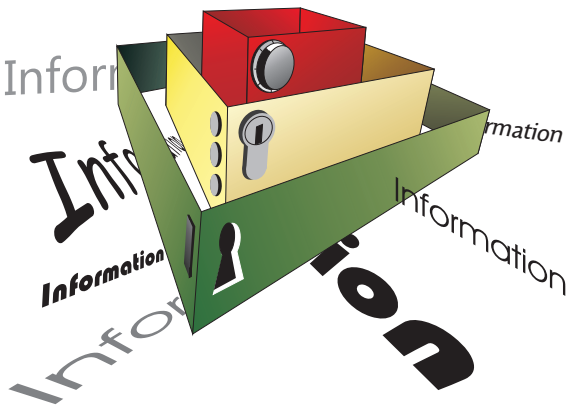
Landespolizeipräsidium
Präsidialstab
Mainzer Str. 134 - 136
66121 Saarbrücken
E-Mail: LPP-PS@polizei.slpol.de

Telefon: 0681-962-8003
Telefax: 0681-962-8005

Stand: 07/2015

Informationsschutz

Eine Handlungsempfehlung.



Polizei

SAARLAND

Ziel

Diese Handlungsempfehlung soll zu einem sicheren Umgang mit Informationen beitragen.

Einordnung von Informationen

Treffen Sie Maßnahmen zum Schutz einer Information nach Ihrer persönlichen Einordnung der Wertigkeit:

<u>Öffentlich</u>
Die Information ist öffentlich verwendbar und allgemein zugänglich.

<u>Intern</u>
Die Information steht allen Mitarbeiterinnen und Mitarbeitern des LPP bzw. benachbarten/vorgesetzten Behörden und Organisationen (z. B. Staatsanwaltschaft, andere Polizeien) zur Verfügung und ist zum internen Gebrauch bestimmt. Das „Öffentlichmachen" der Information kann zu einer Beeinträchtigung der polizeilichen Aufgabenerledigung führen.

<u>Schutzwürdig</u>
Die Offenlegung der Information kann negative Konsequenzen für die polizeiliche Aufgabenerledigung nach sich ziehen und zu einem Schaden für das LPP führen.

<u>Besonders schutzwürdig</u>
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.

Maßnahmen zum Schutz von Informationen

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

Allgemeine Schutzmaßnahmen

- 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.
- Passen Sie Ihre Sicherheitsmaßnahmen im Einzelfall situationsbedingt an.

Beispiele für Schutzmaßnahmen

Einordnung	öffentlich	intern	schutzwürdig	besonders schutzwürdig
Schutzmaßnahmen	■ keine.	Überprüfung der: ■ Richtigkeit der Empfängeradresse, ■ Inhalte und Anlagen vor Versand.	+ ■ 4-Augen-Prinzip, ■ Kennwortschutz von E-Mail-Anlagen.	+ ■ Verschlüsselung von E-Mail-Anlagen, ■ Kenntnisnahme vor Abgang durch den Vorgesetzten, ■ Ankündigung bzw. Bestätigung der Kommunikation, ■ strikte Begrenzung der Information, ■ Speicherung mit Kennwortschutz bzw. Verschlüsselung.
Beispiele	Veröffentlichte Pressemitteilungen, Broschüren, Statistiken.	Telefonverzeichnis des LPP, Organigramme mit personenbezogenen Daten, Mitarbeiterbriefe, Bekanntmachungen im Intranet, Dienstanweisungen.	Erkenntnisse aus polizeilichen Dateien/ Ermittlungen (z.B. Polis), Personaldaten, POLADIS-Rapporte, Bewerbertableaus, Personalstärken, taktische Konzepte, Einsatzbefehle.	PKS vor Veröffentlichung, Vergabeverfahren für Dienst-Kfz, Kennzahlen mit Personenbezug, Personal- und Krankheitsakten, geschützter POLADIS-Vorgang, verdeckte Ermittlungen.

Die Tabelle ist nicht abschließend.