



Regelungen zur Informationssicherheit bei der SEH

Inhaltsverzeichnis

1.	Grundlagen der Informationssicherheit	2
2.	Klassifikation von Informationen.....	2
3.	Richtlinien für die elektronische Übermittlung von Daten.....	5
4.	Ansprechpartner*innen Richtlinien für den Zugang und Zutritt	5
5.	Externe Geräte und Software	6

1. Grundlagen der Informationssicherheit (Auszug aus PIMS Informationssicherheitsmanagement)

Unter Informationssicherheit ist nicht nur die klassische IT-Sicherheit zu verstehen. Der Begriff beschreibt vielmehr den ganzheitlichen Schutz von Unternehmenswerten (Assets), zu denen auch Informationen zählen, unter Betrachtung der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit.

2. Klassifikation von Informationen (Klassifikation von Informationen 1.6_68_A02)

Definition von Informationen: Schützenswertes Unternehmensasset, welches in verschiedenen Formen vorliegen kann, z.B. in elektronischer Form als Datei, in physischer Form als Ausdruck, als gesprochenes Wort oder auch als Wissen von Mitarbeitern des Unternehmens.

Informationsklasse	Beschreibung
ÖFFENTLICH	Informationen dürfen uneingeschränkt an jeden, einschließlich Massenmedien, weitergegeben werden. Konsequenz bei Offenlegung: Kein Schaden, da Informationen für die Öffentlichkeit bestimmt sind.
INTERN (Interner Gebrauch nur bei 68)	Informationen dürfen innerhalb der SEH weitergegeben, aber nicht veröffentlicht oder Massenmedien zugänglich gemacht werden. INTERNE Informationen dürfen Dritten, wie z.B. Dienstleistern, zugänglich gemacht werden, solange die SEH in einem Vertragsverhältnis zu diesen steht. Informationen dieser Klassifikationsstufe müssen nicht explizit gekennzeichnet werden. Konsequenz bei Offenlegung: Betroffen ist ein Teil der SEH. Es entsteht geringfügiger finanzieller Schaden und es kann zu rechtlichen Konsequenzen kommen. Imageverlust und eine Verärgerung von Kunden und Lieferanten ist möglich, aber unwahrscheinlich.
VERTRAULICH (Nur ISMS-Geltungsbereich)	Wenn es den Zielen der Arbeitsgruppe dient, dürfen Informationen auch an Kollegen in der eigenen Organisation oder an andere Organisationen (z.B. Berater, Dienstleister) weitergegeben werden („Need-to-know“-Prinzip, „Kenntnis nur, wenn nötig“). VERTRAULICHE Informationen dürfen Dritten nur zugänglich gemacht werden, wenn die Organisation eine Verschwiegenheitsvereinbarung geschlossen hat. Konsequenz bei Offenlegung: Betroffen ist ein Teil der Stadtentwässerung Hannover. Es entsteht finanzieller Schaden oder es kommt zu rechtlichen Konsequenzen kommen. Imageverlust und Verärgerung bei Kunden und Lieferanten ist wahrscheinlich.
STRENG VERTRAULICH (Ausgewählte Mitarbeiter im Geltungsbereich)	Informationen dürfen nur im Kreise der in einer Besprechung anwesenden Personen ausgetauscht werden. Dokumente dürfen vom Empfänger nur nach Genehmigung durch den Absender weitergegeben werden. STRENG VERTRAULICHE Informationen dürfen Dritten nur zugänglich gemacht werden, wenn die Organisation eine Geheimhaltungsvereinbarung geschlossen hat. Konsequenz bei Offenlegung: Betroffen ist die gesamte SEH. Es entsteht ein schwerer Schaden für die Geschäftszwecke und die Ziele der SEH. Es entstehen gravierende rechtliche Konsequenzen und ein erheblicher Verlust von Vertrauen und Ansehen bei Kunden und Lieferanten.

Änderung der Klassifizierung

Eine Information kann verschiedene Stufen an Vertraulichkeit durchlaufen. Eine Änderung der Klassifizierung kann daher nur durch den Verfasser oder den Eigentümer der jeweiligen Information erfolgen.

Angebote, Verträge, Ausschreibungen

Angebote und Verträge zu Geschäften über allgemein angebotene Leistungen zu allgemein bekannten Gegenleistungen ohne besondere Nebenabreden werden mindestens in die Vertraulichkeitsstufe INTERN eingestuft.

Der kaufmännische Teil von Ausschreibungen ist bis zum Zeitpunkt der Vergabe als STRENG VERTRAULICH einzustufen, danach mindestens als INTERN. Der technische Teil einer Ausschreibung ist je nach Inhalt mindestens als VERTRAULICH zu klassifizieren.

Weitergehende Anforderungen (z.B. des Vergaberechts) bleiben unberührt.

Informationen von Dritten

Die Stadtentwässerung Hannover wahrt die Vertraulichkeit von Kunden- und Lieferanteninformationen und trifft dafür entsprechende Vorkehrungen. Die gesetzlichen und vertraglichen Bestimmungen werden beachtet. Grundsätzlich gelten für Informationen, die der Stadtentwässerung Hannover überlassen und mit keiner Informationsklasse gekennzeichnet wurden die gleichen Regelungen wie für interne Informationen der Stadtentwässerung Hannover (INTERN).

Explizite Kennzeichnung

Sind Informationen explizit als VERTRAULICH oder STRENG VERTRAULICH zu kennzeichnen, so ist der Träger der Information (z.B. Papierbogen, DVD, Festplatte, Ordner, Protokoll, etc.) deutlich erkennbar mit der jeweiligen Kennzeichnung zu versehen. Mehrseitige Dokumente in Papier- oder Dateiform sind auf allen Seiten in der Kopfzeile entsprechend zu kennzeichnen; die Gesamtseitenzahl muss erkennbar sein.

Bei STRENG VERTRAULICHEN Informationen ist der Empfängerkreis auf dem Informationsträger zu bezeichnen. Empfänger können Personen, Stellen, Rollen oder Organisationseinheiten sein.

VERTRAULICHE oder STRENG VERTRAULICHE Informationen in Papierform sind bei externem Versand im verschlossenen Kuvert zu versenden und der Empfänger mit dem Zusatz „persönlich“ zu benennen.

Wenn bei VERTRAULICHEN oder STRENG VERTRAULICHEN Informationen das Risiko der Öffnung durch nicht befugte Dritte besteht, sowie grundsätzlich bei allen STRENG VERTRAULICHEN Informationen, sind Kuvertierungen doppelt auszuführen; die innere ist mit der Kennzeichnung der Informationsklasse zu versehen, die äußere darf keinen Hinweis auf die Vertraulichkeit enthalten.

Die explizite Kennzeichnung hat immer Vorrang vor der impliziten Kennzeichnung.

Implizite Kennzeichnung

Die implizite Kennzeichnung stellt innerhalb eines Kernnutzerbereiches eine Erleichterung für die tägliche Arbeit dar. Die Informationen oder Informationsträger werden dabei nicht selbst gekennzeichnet; der Nutzer kennt die Klassifizierung anhand der Art der Information und wurde entsprechend geschult und sensibilisiert.

Die implizite Kennzeichnung ist möglich, solange die damit gekennzeichneten Informationen den Kernnutzerbereich nicht verlassen. Wenn Informationen den Kernnutzerbereich verlassen, so ist generell eine explizite Kennzeichnung mit der Informationsklasse erforderlich.

Dokumente im Entwurfsstadium

Dokumente, die sich noch im Entwurfsstadium befinden sind nicht von der Einstufung des Dokuments in die jeweilige Informationsklasse entbunden.

Ausdrückliche Verpflichtungserklärungen

Jeder externe Dienstleister und Lieferant muss sich zur Verschwiegenheit verpflichten, sofern er potentiell Zugriff auf Daten oder Informationen der Stadtentwässerung Hannover hat. Das kann bereits vor Abschluss eines Vertrags, z.B. im Rahmen von Verhandlungen, der Fall sein. Dann hat er zuvor eine Erklärung zur Verschwiegenheitspflicht (NDA) zu unterschreiben. Daneben ist darauf zu achten, dass ein mit ihm später geschlossener Vertrag ebenfalls eine Verschwiegenheitspflicht enthält. Die Verschwiegenheitspflicht (NDAs) für Lieferanten oder Dienstleister erstellt die Innenrevision und händigt der Einkauf aus. Der jeweilige Auftraggeber ist verantwortlich dafür, mit dem ISK68 den Schutzbedarf der Daten zu klassifizieren und danach die Innenrevision, mit der Ausfertigung des NDAs zu beauftragen.

Beispiele und Regeln zum Umgang mit Informationen

Die Regeln zum Umgang mit Informationen werden in folgender Tabelle -Umgang mit klassifizierten Informationen- zusammengefasst.

	ÖFFENTLICH	INTERN	VERTRAULICH	STRENG VERTRAULICH
Beschreibung	- Alle Personen - Auch außerhalb der Organisation - Landeshauptstadt Hannover	- Jeder Mitarbeiter der Organisation - Dritte nur bei Vertragsverhältnis	- Geltungsbereich des ISM6 - Dritte nur mit Geheimhaltungspflicht	- Ausgewählte Mitarbeiter der SEH - Nur der Dokumentverantwortliche kann weitere Personen aufnehmen - Dritte nur mit gültiger Geheimhaltungsverpflichtung
Beispiele	- Produktbroschüren, Flyer, Werbematerial - Im öffentlichen Umfeld verfügbare Informationen - Firmenwebseite - Newsletter zur externen Verteilung - Organigramme ohne Namen	- Unterliche Informationen aus dem Fachbereich IS - Standardbotschaftswerkzeuge der Organisation - Organigramme mit Namen - Interne Telefonlisten und Mailadressen - PIMS-Handbuch - Ständert IT-Sicherheitsrichtlinien - Noch nicht klassifizierte Dokumente	- Geltungsbereich des ISM6 - Standardbotschaftswerkzeuge im Geltungsbereich - IT-Sicherheitsrichtlinien des Geltungsbereichs	- Passwörterlisten, Gruppenpasswörter - Sinkbox-, Schutzrechte- und Risikoanalysen - Ausfall-, Wiederanlauf-, Notfallpläne, etc. - Vertrauliche Dokumentationen
E-Mail		- Intern: Alle - Extern: Nur bei Vertragsverhältnis	- Nur Mitteilung der Informationen bewahren (Versenden von Links). Kein Versenden der Informationen über E-Mail. Intern: Nur Geltungsbereich. Extern: nur wenn nötig. Austausch der Informationen nur über gemeinsame Mailboxen. - Extern: Nur mit Geheimhaltungspflicht. Austausch der Informationen nur über Daten-austauschplattform	- Kein Versenden der Informationen nur Benachrichtigung der Informationen verfügbar sind. Intern: Nur Benachrichtigung der Informationen bewahren (Verteilung auf gemeinsame zugriffsspezifisches Austausch). - Extern: Nur mit gültiger Geheimhaltungspflicht. Nur Informationen des Daten zur einer Daten-austauschplattform bewahren.
Datenspeicherung / Datenbearbeitung		- Auf jedem PC / Notebook - Speichern nur auf Netzlaufwerken (SEH) - Zugriffsrechte für alle Mitarbeiter	- Bearbeiten auf jedem PC / Notebook der SEH - Speichern nur auf Netzlaufwerken (SEH) - Zugriffsrechte für Mitarbeiter der Arbeitsgruppe oder Arbeitsgruppe	- Nur auf geeigneten, verschlüsselten PCs / Notebooks der SEH - Speichern nur auf Netzlaufwerken (SEH) - Zugriffsrechte nur für befugte Personen, weiterzugeben durch Dokumentenverantwortlichen
Externe Medien: USB, Datenträger, CDs, DVDs	Keine Versand	Nur auf dienstlich geneigten Medien	- Nur auf dienstlich geneigten Medien - Nur in verschlüsselter Form	- Nur auf dienstlich geneigten Medien - Nur in verschlüsselter Form
Papier		Darf gedruckt werden	- Darf gedruckt werden (nur Vertraulicher Druckvorgang) - Sichere Aufbewahrung nach Verwendung empfohlen	- Darf gedruckt werden (nur Vertraulicher Druckvorgang) - Sichere Aufbewahrung nach Verwendung vorgeschrieben - Sofortige Zerstörung sobald nicht mehr benötigt
Postversand		- Intern: Gibermappe - Extern: Verschlussener Umschlag	- Intern: Verschluss Gibermappe - Extern: Verschlussener Umschlag	- Verschlussener Umschlag, doppelt konvertiert - Extern: Kastenmaterial mit Abgabe- und Empfangsprotokoll
Entsorgung		- Entsorgungsfähigkeit - Zerkleinern / Durchbohren / Thermische Verwertung		- Sofortige Entsorgung durch Schredder / Aktenvernichter - Schreddermaterial entsorgen durch Entsorgungsdienstleister

Bild ist Beispielhaft: Revision 1 (1.6_68_A02 Handout Umgang mit klassifizierten Informationen)

3. Richtlinien für die elektronische Übermittlung von Daten (ISMS Sicherheitsrichtlinie Mobile Datenträger & 1.7_68_A01 Sicherheitsrichtlinie Kryptographie und PKI-Betrieb)

Datenträger nicht unbeaufsichtigt herumliegen zu lassen.

- Alle Medien die portabel (z.B. DVD, USB-Stick, SD-Card) sind, gehören in den Fokus.
- Es sind nur Dienstliche Datenträger erlaubt.
- Die Datenträger müssen verschlüsselt werden.
- Die Verschlüsselung ist getrennt vom Datenträger aufzubewahren.
- Bei Weitergabe ist die Verschwiegenheitserklärung zu kontrollieren
- Das Verschlüsselungsprogramm Bit Locker ist anzuwenden.
- Die Weitergabe des Schlüssels zum entsperren erfolgt über SMS oder fernmündlich
- Die Verwendung der folgenden Hashalgorithmen ist aufgrund der mangelnden Kollisionsresistenz im KRITIS-Geltungsbereich der SEH verboten:
 - DES / Triple-DES
 - MD5 / HMAC-MD5
 - SHA1 / HMAC-SHA1
- Ausnahmen, beispielsweise aufgrund der Verwendung von Altsystemen, sind explizit durch den AGKo zu genehmigen.
- Mitarbeiter der SEH sind dazu verpflichtet, betriebsfremde Dateien und Datenträger mit einem Intranet PC ohne aktive Netzwerkverbindung mit aktueller Virendefinition zu scannen. Bei Verdacht auf Infektion mit Schadsoftware ist der Rechner vom Netzwerk getrennt zu halten und ein Sicherheitsvorfall zu melden.

4. Ansprechpartner*innen Richtlinien für den Zugang und Zutritt (1.7_68_A02 Sicherheitsrichtlinie Zugangs- und Zutrittsschutzkonzeption)

Zur Sicherung der Informationen gilt auch ein eingeschränkter Zugang/Zutritt zu den Bereichen der Stadtentwässerung Hannover. Es wird hierbei zwischen allgemeinem Sicherheitsbereich und Hochsicherheitsbereich unterschieden. Die Zuteilung zu welchem (Sicherheits- bzw. Hochsicherheits-) Bereich der von der Fremdfirma betretene Bereich liegt, wird in der Arbeitsbeschreibung, bzw. -erlaubnis beschrieben.

Grundsätzliche Vorschriften in Sicherheitsbereichen

Das Mitführen eines Lichtbild-Ausweises (Personal-/Dienstausweis oder gleichwertig) ist zwingend vorgeschrieben und auf Verlangen vorzuzeigen.

Folgende Tätigkeiten sind in Hochsicherheitsbereichen strengstens untersagt:

- Unautorisiertes anschließen von Geräten
 - Sämtliche Arten von Aufzeichnungen wie z.B. Video, Tonband oder Fotos die nicht für das Ausüben der Tätigkeit notwendig sind
 - Essen, Trinken und Rauchen
 - Mitführen von schnell entflammaren Materialien, außer den für die Tätigkeit notwendigen
- Verstöße sind als Sicherheitsvorfall zu dokumentieren und gemäß der Meldung von Vorfällen zu melden

Hochsicherheitsbereich

In den Hochsicherheitsbereichen gelten zusätzlich zu den grundsätzlichen Vorschriften folgende Vorschriften:

- Betriebsfremde haben sich vor Beginn ihrer Tätigkeiten bei den zuständigen Aufsichtspersonen der SEH anzumelden und auszuweisen.
- Die Bewegungsfreiheit innerhalb der Hochsicherheitsbereiche beschränkt sich ausschließlich auf den direkten Tätigkeitsbereich.

Sämtliche Aktivitäten und Besuche im Hochsicherheitsbereichen müssen von der zuständigen Aufsichtsperson vermerkt werden.

Zutrittsvorschriften für Elektrische Betriebsstätten

Elektrische Betriebsstätten müssen stets verschlossen gehalten werden. Sie dürfen nur von Elektrofachkräften oder anderweitig elektrotechnisch unterwiesenen Personen bzw. von anderen Personen nur unter Aufsicht von Elektrofachkräften oder in den Betrieb elektrischer Anlagen unterwiesenen Personen betreten werden (nach DIN VDE).

Verschließen nach Beendigung der Arbeit

Jegliche Netzwerk- und Fernwirktechnik ist stets unter Verschluss und vor Fremdzugriff geschützt zu halten. Nach Beendigung der Arbeit haben die Mitarbeitenden dafür Sorge zu tragen, dass alle geöffneten Schließungen wieder verschlossen werden.

5. Externe Geräte und Software

Die Nutzung externer Systeme (z.B. Parametrier- oder Service-Systeme) durch IT-Dienstleister innerhalb von Netzwerken des Anwendungsbereichs des ISMS der Stadtentwässerung Hannover ist untersagt. Systeme, welche für die Durchführung von Service-Dienstleistungen innerhalb kritischer Netzwerke notwendig sind, werden von der SEH gestellt. Benötigte Software wird mit ausreichend Vorlaufzeit (mindestens zwei Wochen) ebenfalls nach Bedarf auf eigenen Systemen zur Verfügung gestellt.

Ausnahmen hiervon bedürfen der Genehmigung durch den ISK der Stadtentwässerung Hannover.