Handreichung zum sicheren Umgang mit IT und Daten

Die heutigen Arbeitsplätze setzen die Nutzung moderner IT-Komponenten voraus. Häufig sind mehrere IT-Geräte parallel im Einsatz, wie z.B. PCs, Notebooks, Tablets, Drucker oder sogar Smartphones. Mittlerweile sind alle diese Geräte vernetzt und häufig ist der Zugriff von mehreren Geräten auf zentrale Daten möglich. Die digitale Kommunikation via E-Mail hat in den meisten Fällen Brief und Fax ersetzt und der Einsatz von mobilen Messengern ist mittlerweile zur Selbstverständlichkeit geworden.

Die digitalen Möglichkeiten der Kommunikation, sowie der Verarbeitung und Speicherung von Daten haben die Arbeitsabläufe beschleunigt und die Effizienz am Arbeitsplatz gesteigert. Die vielfältigen Möglichkeiten bergen allerdings nicht nur Vorteile, sondern auch Risiken und Gefahren. Die einfachen Möglichkeiten Informationen an viele Teilnehmer zu verteilen, erschwert die Kontrolle darüber welche Nutzerkreise Zugriff auf die Informationen haben. Auch steigen von Jahr zu Jahr die Gefahren durch externe Angriffe mittels Schadsoftware.

Um diesen Risiken und Gefahren entgegen zu wirken, wurden alle Landesbehörden verpflichtet ein Informationssicherheitsmanagement nach den Vorgaben des IT-Grundschutzkonzeptes des Bundesamtes für Sicherheit in der Informationstechnik (BSI) einzuführen. Dieses Grundschutzkonzept beschreibt Maßnahmen die helfen sollen die Sicherheit im Umgang mit IT-Systemen zu erhöhen.

Ein weiteres wichtiges Handlungsfeld ist der Umgang mit personenbezogenen Daten. Die neue EU-Datenschutzgrundverordnung (DSGVO) bestätigt in vielen Fällen die gängige Praxis der bisher geltenden Datenschutzgesetze, erweitert diese an einigen Stellen noch, vor allem in Bezug auf die Informationspflichten gegenüber Betroffenen.

Diese Handreichung ist als Hilfestellung für alle Bedienstete der Hochschule gedacht. Sie enthält eine Sammlung von Empfehlungen, die bei dem Umgang mit IT und Daten berücksichtigt werden sollten, mit dem Ziel die Risiken und Gefahren zu minimieren.

Inhaltsverzeichnis

1 Sicherer Umgang mit IT-Systemen

Unter IT-Systemen sind Hardware, Software aber auch Dienste im Internet (Portale, Services, etc.) zu verstehen.

1.1 Allgemeine Vorsichtsmaßnahmen

Arbeitsplatzsysteme sind mit einem automatisiert arbeitenden Virenscanner ausgestattet. Beim Auftreten einer Virenwarnung, die nicht automatisch vom Antivirenprogramm behoben werden kann, sollte der zuständige IT-Administrator informiert werden.

Auf dem Campus der Hochschule werden verschiedene WLANs (Funknetzwerke) betrieben. Um Störungen zu vermeiden, dürfen WLAN-Accesspoints nicht selbstständig ohne Abstimmung mit dem Rechen- und Medienzentrum (RMZ) eingerichtet werden.

1.2 Persönliche Anmeldeinformationen

Die Nutzung der IT-Systeme der Hochschule erfolgt grundsätzlich durch ein persönliches Konto. Das Konto darf ausschließlich persönlich genutzt werden. Müssen Dritte (intern/extern) unter einem nicht ihnen zugewiesenen Konto Tätigkeiten ausüben, so sollten sie nicht unbeaufsichtigt bleiben. Die Verantwortung hierfür trägt der Kontoinhaber des angemeldeten Benutzers.

Achtung: Persönliche Zugangsdaten dürfen in keinem Fall weitergegeben werden!

1.3 Veränderungen von IT-Systemen und Anwendungen

Veränderungen an IT-Systemen sollten nur in Absprache mit dem zuständigen IT-Administrator erfolgen. Dies gilt sowohl für Veränderungen an der Hardware, als auch für Anwendungen und Systemeinstellungen.

1.4 Speicherung von Daten

Es wird empfohlen Geschäftsdaten auf Netzwerkfreigaben/-verzeichnissen abzulegen. Die lokale Datenhaltung sollte vermieden werden. Der Benutzer ist für die Sicherung temporär lokal abgelegter Daten selbst verantwortlich.

Der Benutzer ist auch für die Vertraulichkeit der Daten verantwortlich. Dabei kann eine manuell durchzuführende Verschlüsselung der gespeicherten Daten erforderlich werden.

1.5 Nutzung von Wechseldatenträgern (USB, SD, HD, CD/DVD, ...)

Im Interesse eines vertraulichen Umgangs mit Hochschuldaten ist bei der Nutzung von mobilen Datenträgern Folgendes zu beachten:

(1) Um Datenverluste zu vermeiden, sollten auf mobilen Datenträgern (mobile Plattenlaufwerke, USB-Sticks, Speicherkarten, CDs/DVDs, Smartphones, PDAs, Tablets, etc.) nur Kopien von Hochschuldaten gespeichert werden.

(2) Beim Umgang mit USB-Speichermedien sollten folgende Punkte beachtet werden:

   a. die Dateien auf dem Speichermedium werden automatisch bei Zugriff vom Virenscanner überprüft,
   b. der angemeldete Benutzer am Rechner sollte keine erweiterten Berechtigungen, z.B. Administrationsrechte, besitzen,
   c. generell sollten nur Medien aus vertrauenswürdigen Quellen verwendet werden,
   d. es sollten nur die tatsächlich notwendigen Daten übertragen werden,

e. wenn nach der Verwendung eines fremden USB-Speichermediums Auffälligkeiten bemerkt werden (Rechner reagiert komisch, Dateizugriffe sind nicht mehr möglich, usw.), sollte der Rechner sofort vom Hochschulnetzwerk abgekoppelt werden (LAN Stecker und WLAN ausschalten) und der zuständige IT-Administrator umgehend informiert werden.
f. Wenn möglich, sollten Speichermedien der Hochschule verwendet werden.

(3) Im Sinne des Datenschutzes sollte darauf geachtet werden, dass personenbezogene oder andere vertrauliche Daten nicht unverschlüsselt auf Wechseldatenträgern gespeichert werden.

(4) Mobile Datenträger sollten nicht unbeaufsichtigt sein und zugriffssicher verwahrt werden.

(5) Zum Anschluss an unternehmensfremde Rechner sollten nur mobile Datenträger verwendet werden, die keine personenbezogenen oder sonstigen vertraulichen Daten enthalten.

(6) Nicht mehr benötigte Daten sollten unverzüglich von mobilen Datenträgern gelöscht werden.

1.6 Passwörter – Zugang- und Zugriffsschutz

1.6.1 Sicherer Umgang mit Passwörtern / Speicherung / Ablage

Die folgenden Passwortregeln dienen dem Schutz des eigenen Kontos und des eigenen Profils und sollten deshalb Beachtung finden:

(1) Jeder PC-Benutzer ist verpflichtet, ihm zur Verfügung gestellte bzw. von ihm benutzte Passwörter vertraulich zu behandeln und geheim zu halten, sodass sie Dritten nicht zugänglich sind. Passwörter dürfen nicht an Dritte, nicht an Kolleginnen und Kollegen und auch nicht an IT-Administratoren weitergegeben werden. Passwörter dürfen nicht in Dateien oder Skripten gespeichert und auch nicht am Arbeitsplatz, z. B. auf Zetteln, hinterlegt oder auf Funktionstasten gespeichert werden. Bei Bedarf kann ein verschlüsselter Passwort-Safe, wie z.B. die Software keepass eingesetzt werden. Wenden Sie sich diesbezüglich an den für Sie zuständigen IT-Administrator.

(2) Die Anmeldung darf nicht unter einem fremden Benutzernamen / Passwort erfolgen.

(3) Bei einem Verdacht auf Verlust der Vertraulichkeit oder Ausspähung ist das Passwort sofort zu ändern. Es muss ein von den bisher genutzten Passwörtern abweichendes Passwort gewählt werden.

(4) Voreingestellte Passwörter (z. B. des Herstellers oder der IT-Administration bei Auslieferung/Installation von Systemen) sind unverzüglich durch individuelle Passwörter zu ersetzen.

(5) Bereits benutzte Passwörter können nach einem Passwortwechsel nicht wiederverwendet werden.

(6) Passwörter sind möglichst verdeckt einzugeben, um eine Kenntnisnahme durch Unbefugte zu verhindern.

(7) Dritte (Studierende/Kollegen/Externe) dürfen nicht unbeaufsichtigt an einem System verbleiben, wenn sie unter einem anderen Benutzerkonto Tätigkeiten durchführen.

(8) Bei Verdacht von Missbrauch ist unverzüglich der zuständige IT-Administrator zu informieren.

(9) Die von einigen Browsern angebotene Funktion „Passwort speichern“ sollte nicht verwendet werden.

(10) Passwörter, welche innerhalb der Hochschule verwendet werden, dürfen nicht in anderen Umgebungen (z. B. im Internet, Kundenportale etc.) sowie im privaten Bereich gleichlautend verwendet werden.

(11) Um im Falle einer Kompromittierung eines Passwortes die Risiken möglichst gering zu halten, müssen sich Passwörter für administrative Berechtigungen von Standard-Passwörtern unterscheiden.

1.6.2 Gestaltung von Passwörtern

Bei der Auswahl von Passwörtern sind nachfolgende Anforderungen zu berücksichtigen. Damit kann gewährleistet werden, dass das Passwort nicht einfach erraten oder durch einfache Algorithmen geknackt werden kann. Generell gilt als

Faustregel je mehr verschiedenartige Zeichen und je länger desto sicherer. Entsprechend ist die Passwortvorgabe unten aufgebaut.

Das Passwort:

(1) muss mindestens 12 Stellen umfassen.

(2) muss Zeichen aus drei der folgenden Kategorien enthalten:

a. Großbuchstaben (A – Z),
b. Kleinbuchstaben (a – z),
c. Zahlen zur Basis 10 (0 bis 9),
d. nichtalphabetische Zeichen (zum Beispiel: !, $, #, %).

(3) muss sich von den letzten sechs benutzten Passwörter unterscheiden.

(4) darf nicht leicht zu erraten sein und darf daher keine Trivialwörter, Zahlenreihen oder Namen, Geburtstage, Kennzeichen, o.ä. enthalten.

(5) Darf nur einmal innerhalb 24 Stunden geändert werden.

(6) Der Benutzername darf nicht Teil des Passworts sein.

Beispiel:

Ich arbeite an der Hochschule Reutlingen an 3 Tagen in der Woche!

Von diesem Satz werden nun für die Passworterstellung die Anfangsbuchstaben aller Wörter sowie die Zahlen und Sonderzeichen verwendet. Das ergibt folgendes Passwort:

IaadHRa3TidW!

1.7 E-Mail-Nutzung

1.7.1 Allgemeine Anforderungen

Die Nutzung von E-Mails birgt Gefahren. Jeder Benutzer ist zur Wachsamkeit im Umgang mit E-Mails aufgerufen:

(1) E-Mails unbekannter Herkunft und mit nicht plausiblen Betreffs oder nicht korrekter Sprache und Anhängen (insbesondere mit ausführbaren Dateien), sollten mit äußerster Vorsicht behandelt werden, ggfs. den zuständigen IT-Administrator einbinden. Im Zweifelsfall E-Mail lieber löschen. Zudem sollte keine Lesebestätigung abgegeben werden.

(2) Sowohl intern als auch extern versendete und empfangene E-Mails sind als verbindliche Nachrichten zu behandeln.

(3) Bei der Erstellung von E-Mails sollte man nachfolgenden Empfehlungen an Form und Gestaltung folgen:

a. Persönliche Ansprache der direkten Empfänger und Grußformel am Ende.
b. Wählen eines kurzen und aussagekräftigen Betreffs.
c. Erwähnen angehängter Dateien.
d. Beschränken des Größenumfangs. Das Versenden größerer E-Mails ist mit dem Empfänger im Vorfeld abzustimmen.
e. Überprüfen, dass der richtige Empfänger angegeben ist.
f. Verschlüsselung vertraulicher Informationen (z.B. passwortgesichertes ZIP-Archiv).

(4) Zu vermeiden ist:

a. der Versand oder die Weiterleitung von Kettenbriefen und von sog. falschen Warnungen,

b. der Versand von E-Mails mit rechtswidrigen, beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, Gewalt verherrlichenden oder pornografischen Äußerungen oder Abbildungen oder sonstigen anstößigen oder dem Ansehen der Hochschule abträglichen Inhalten,
c. die Verbreitung von Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
d. das Verbreiten unbekannter Inhalte aus unsicheren Quellen, insbesondere mit Anhängen und ausführbaren Dateien,
e. die private Verwendung der E-Mail-Adresse der Hochschule in öffentlichen Chat-Räumen oder Foren.

1.7.2 Phishing[1] / Spam[2] / Ransomware[3]

Bei der Nutzung von E-Mail-Diensten gibt es Risiken von Datenverlusten, bzw. bewusstem Abgreifen von Daten (Stichwörter: Phishing, Spam, Ransomware).

Daher ist auf folgende Punkte insbesondere zu achten:

(1) Absendername und E-Mail-Adresse sind in jedem Fall zu prüfen.

(2) Fehlerhafte Rechtschreibung und Satzbau sowie eine unpersönliche Ansprache, teilweise auch die Verwendung von Fremdsprachen sind Indizien für gefälschte E-Mails.

(3) Androhungen, wie Sperrung eines Kontos oder dringendem Handlungsbedarf sollte nicht gefolgt werden.

(4) Direkte Links in E-Mails zu Login-Bereichen sollten nicht verwendet werden – der Login sollte immer über die Original-Website vorgenommen werden.

(5) Links in E-Mails von Unbekannten sowie angebliche Rechnungen, Mahnungen, Zahlungsaufforderungen oder Kontoüberprüfungen sollten grundsätzlich mit äußerster Vorsicht behandelt und im besten Fall direkt gelöscht werden.

(6) Vorsicht bei Dateianhängen, vor allem mit den Endungen .exe, .bat, .com, .vbs, .scr oder .js (häufig tarnen Hacker ihre Malware auch mit doppelten Endungen, zum Beispiel „*.pdf.exe“).

(7) Im Verdachtsfall informieren Sie den zuständigen IT-Administrator!

1.7.3 Versand von E-Mails mit mehreren Empfängern

(1) E-Mail-Adressen von natürlichen Personen sind personenbezogene Daten und unterliegen daher dem Datenschutzrecht. Hier ist besondere Vorsicht im Umgang geboten.

E-Mail-Adressen, die allgemeine öffentliche Kontaktdaten darstellen (z.B. info@...), stellen keine personenbezogenen Daten dar. Diese öffentlichen Kontaktadressen sind daher im Umgang weniger sensibel.

Hinweis: Auch beim Weiterleiten von E-Mails und Konversationen ist darauf zu achten, ob E-Mail-Adressen aus dem aufgezeichneten E-Mail-Verkehr herausgelöscht werden müssen.

(2) Die sichtbare Verwendung einer personenbezogenen E-Mail-Adresse im „AN“- oder „CC“-Feld einer E-Mail, die an mehrere Empfänger gerichtet ist, darf nur mit Einwilligung jedes einzelnen Empfängers oder bei Vorliegen eines gesetzlichen Erlaubnistatbestands erfolgen.

Ausnahmen hiervon sind:

a. Sämtliche Empfänger der E-Mail sind Angehöriger der Hochschule, bzw. die E-Mail wird an eine Verteilerliste gesendet, die ausschließlich aus Empfängern der Hochschule besteht, oder,

[1] Phishing: Abgreifen von Userdaten – Identitätsdiebstahl (siehe *Wikipedia*)
[2] Spam: Unverlangte, elektronische zugestellte Nachrichten, zumeist Werbung (siehe *Wikipedia*)
[3] Ransomware: Erpressungs-, Krypto-, Verschlüsselungstrojaner (siehe *Wikipedia*)

b. wenn einzelne oder alle Empfänger der E-Mail extern sind, bzw. die E-Mail mittels einer Verteilerliste auch oder nur an externe Empfänger versendet wird und sämtliche externen Empfänger untereinander bereits sichtbare Kommunikationsbeziehungen auf dieser Ebene mit- bzw. untereinander pflegen.

(3) Im Zweifel ist die E-Mail an die externen Empfänger mittels einer Blindkopie (Bcc = blind carbon copy) zu versenden.

(4) Vor Aufnahme eines externen Empfängers in eine Verteilerliste ist dieser über dieses Vorhaben und mögliche Risiken zu informieren. Gibt der Empfänger kein Einverständnis für eine sichtbare Verwendung seiner E-Mail-Adresse, ist zu klären, ob er seine Zustimmung zumindest für den Gebrauch einer vertraulichen Verteilerliste gibt, bei der er E-Mails als Blindkopie erhält. Äußert sich der externe Empfänger nicht, so ist auf die Aufnahme in eine E-Mail-Verteilerliste ganz zu verzichten. E-Mails sind dann ausschließlich per Einzelversand an ihn zu senden.

(5) Bei einer ungewollt offenen Verwendung personenbezogener E-Mail-Adressen sind sowohl die betroffenen Empfänger als auch der Arbeitgeber über diesen Umstand zu informieren. Soweit möglich, sind die Ursache und die Auswirkungen dabei aufzuzeigen. Ferner ist die Angelegenheit unverzüglich dem Datenschutzbeauftragten (DSB) zu melden.

1.7.4 Umgang mit dem Abwesenheitsassistenten

(1) Der Abwesenheitsassistent sollte immer ab dem ersten Tag der Abwesenheit aktiviert sein.

(2) Es ist, sofern möglich, bzw. sinnvoll, eine Vertretung anzugeben. Dies muss mit der Vertretung vorher abgesprochen werden, bzw. die Vertretung muss vorher darüber informiert werden.

(3) Es sollte das Datum angegeben werden, an dem man wieder erreichbar ist.

(4) Falls im Falle längerer Abwesenheiten Weiterleitungen von E-Mails notwendig werden, sollten diese automatisiert nur an dienstliche E-Mail-Adressen weitergeleitet werden.

(5) Wird der Abwesenheitsassistent auch für externe Empfänger eingerichtet, so sollte, sofern möglich, die Option *„Nur meine Kontakte“* aktiviert werden. Dadurch erhalten ausschließlich Absender eine Abwesenheitsnotiz, die im eigenen Outlook-Adressbuch gespeichert sind.

1.7.5 E-Mail als Geschäftsbrief

(1) E-Mails sind grundsätzlich rechtserheblich und stehen dem dienstlichen Schriftverkehr gleich. E-Mails aus der betrieblichen Korrespondenz können als Handels- oder Geschäftsbriefe gelten und müssen bezüglich der Fußleistenpflicht die Vorschriften des Gesetzes über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister (EHUG) erfüllen.

(2) Beim Einsatz von E-Mail empfiehlt es sich sowohl intern, als auch extern eine Signatur zu verwenden. Die Signatur sollte die Kontaktdaten enthalten, z.B.:

Hochschule Reutlingen
Vorname Nachname
Funktion
Alteburgstr. 150
72762 Reutlingen
Tel: +49-7121-271-xxxx
vorname.nachname@reutlingen-university.de

1.8 Internetnutzung

1.8.1 Allgemeine Richtlinien

(1) Dienstliche Beiträge in Internet-Newsgroups, Diskussionsforen und Sozialen Netzen (Facebook, Google+, usw.), unterliegen den gleichen Regelungen wie sonstige öffentliche Meinungsbekundungen und Veröffentlichungen im Namen der Hochschule. Die diesbezüglichen Vorgaben sind zu beachten.

1.8.2 Browsersicherheit

Für die Nutzung des Internets sind folgende Empfehlungen zu beachten:

(1) Da immer wieder Internetseiten gehackt oder Phishing-Seiten eingerichtet werden, sollte nur vertrauenswürdigen Links gefolgt werden.

(2) Software aus dem Internet sollte nur mit entsprechender Expertise oder in Abstimmung mit den zuständigen IT-Administratoren heruntergeladen werden.

(3) Bei einer Nutzung von Internetdiensten sollten keine intern verwendeten Passwörter eingesetzt werden. Ebenso sollen für die Nutzung von mehreren Internetdiensten nicht identische Passwörter eingesetzt werden.

1.8.3 Nutzung von Social Media

Über soziale Medien können Personen und Zusammenhänge ausspioniert werden. Man kann bspw. herausfinden, welche Freundschaften oder Verbindungen mit wem bestehen, wer Arbeitgeber ist, wo eine Person wohnt, welche Fotos sie postet, welche Aktivitäten sie mag, etc.

Alle Daten, die eine Person von sich preisgibt, können aufgenommen und genutzt werden.

Konkrete Risiken:

(1) Private Daten oder Hochschul-Interna, die (mit-)geteilt werden, können für kriminelle Aktivitäten genutzt werden.

(2) Ergaunern von Kontaktdaten und persönlichen Daten von Kontakten (bspw. Verkauf von Adressen).

(3) Verbreiten bzw. Zusenden von Inhalten (Bilder, Dateien, Videos o.ä.) mit Schadsoftware.

(4) Widerrechtliche Nutzung und Veröffentlichung von urhebergeschützten Inhalten wie Bilder, Videos, Texte.

(5) Aussagen und Kommentare bringen interne Themen in die Öffentlichkeit.

(6) Rassistische, ketzerische, beleidigende oder in sonst irgendeiner Weise unangebrachte Aussagen (auch auf privaten Profilen) können, mit dem Unternehmen in Verbindung gebracht, dessen Ruf und Image schädigen.

Folgende Empfehlungen sollten daher beachtet werden:

(1) Das Internet vergisst (fast) nichts. Aussagen, die (teilweise aus der Situation heraus) gemacht werden, könnten noch nach Jahren verfügbar sein.

(2) Negative Aussagen können Konsequenzen für einen persönlich, für die Hochschule oder Bekannte nach sich ziehen.

(3) Persönliche Standpunkte sind klar als eigene Meinung erkennbar darzustellen.

(4) Die Hochschul-E-Mail-Adresse sollte nicht für einen privaten Social-Media-Account verwendet werden.

(5) Es ist nicht darauf zu vertrauen, dass hinter einem Profil tatsächlich ein „Freund“ steckt. Auch Profile von persönlich bekannten Personen könnten von einem Dritten missbraucht werden. Daher ist ein Austausch mittels Social-Media-Angeboten über geheimhaltungsbedürftige Themen nicht geeignet.

(6) Diskreditierende oder peinliche Aussagen oder Bilder, die einen Bezug zur Hochschule haben, müssen auf jeden Fall vermieden werden.

(7) Vertrauliche Informationen sind - auch außerhalb der Hochschule - unbedingt geheim zu halten.

(8) Treue- und Geheimhaltungspflichten bestehen auch nach Beendigung eines Arbeitsverhältnisses.

(9) Private Daten, insbesondere von Dritten, sind zu schützen.

(10) Es dürfen keine unbegründeten Behauptungen zu Funktionen, Leistungen o.ä. aufgestellt werden.

(11) Offizielle Statements der Hochschule dürfen ausschließlich von der autorisierten Stelle veröffentlicht werden.

(12) Auch im Social Web gelten die üblichen Gesetze wie Urheberrecht, Privatsphäre und Datenschutz. Es sind nur Inhalte, Bilder und Videos zu veröffentlichen, für die eine Berechtigung zur Veröffentlichung vorhanden ist.

1.9 Nutzung von Cloud-Diensten

1.9.1 Allgemeine Richtlinien

Die Nutzung anderer als von der Hochschule empfohlenen Cloud-Dienste für die Übertragung von Hochschuldaten sollte vermeiden werden.

1.9.2 Übertragung unkritischer Daten

Für die Übertragung unkritischer Daten empfehlen wir den Dienst:

bwSync&Share

welcher auf der Webseite der Hochschule beschrieben ist. bwSync&Share hat folgende Vorteile:

a. Der Dienst wird von einer Partnerhochschule in Baden-Württemberg betrieben (KIT Karlsruhe).
b. Der Zugang zu dem Dienst erfolgt über eigene Netzwerke der Hochschulen in Baden-Württemberg.
c. Die Übertragung wird mittels https verschlüsselt.
d. Die Authentifizierung ist mit den Benutzerdaten der Hochschule möglich.

Mit dem KIT soll ein ADV-Vertrag abgeschlossen werden. Sobald dieser vorliegt, ist bwSync&Share auch für personenbezogenen Daten zulässig.

1.9.3 Übertragung sensibler bzw. schützenswerter Daten

Für die Übertragung sensibler und schützenswerter Daten empfehlen wir ebenfalls bwSync&Share, allerdings sollten die Daten vor dem Hochladen verschlüsselt werden. Die Schlüssel für die Entschlüsselung der Daten müssen dem Partner über andere Kanäle bereitgestellt werden.

1.10 Instant Messaging

Mit Instant-Messaging sind Tools zur digitalen Kommunikation gemeint (z.B. WhatsApp, Hangout, etc.). Bei Hochschul-interner Kommunikation sollte möglichst die intern vorhandene Infrastruktur genutzt werden.

Aktuell ist eine einfache Chat-Möglichkeit innerhalb des BSCWs möglich. Diese Funktion heißt hier Microblog.

Ein mobiler Messenger für die Nutzung innerhalb der Hochschule soll 2019 eingeführt werden.

2 Sicherer Umgang mit mobilen Endgeräten

2.1 Allgemeine Richtlinien zur Nutzung mobiler Endgeräte

Unter mobilen Endgeräten verstehen wir tragbare Rechner, wie z.B. Notebooks, Tablets oder Smartphones.

2.1.1 Zugriffssichere Aufbewahrung / Weitergabe

Während der Nutzung von durch die Hochschule zur Verfügung gestellten mobilen Endgeräten sind diese sicher aufzubewahren und vor dem Zugriff Dritter zu schützen. Hierzu gehören u.a.

(1) die sichere Aufbewahrung zu Hause, auf Dienstreisen und innerhalb der Hochschule,

(2) die Verschließung der mobilen Endgeräte, wenn dies möglich ist. Sie dürfen keinesfalls offen liegen gelassen werden.

(3) Die Geräte nicht an Dritte oder Fremde weiterzugeben, auch nicht vorübergehend.

2.1.2 Informationspflichten der Bediensteten

Die Bediensteten informieren die Hochschule, wenn:

(1) ihr Endgerät gestohlen oder verloren wurde oder in sonstiger Weise abhandengekommen ist. Dies gilt auch, falls der Verlust des Endgeräts aus Sicht der Bediensteten nur vorübergehend sein wird oder das Gerät nach kurzer Zeit wieder aufgefunden wird.

(2) das Gerät beschädigt, zerstört oder die Gebrauchstauglichkeit in anderer Weise beeinträchtigt wurde.

(3) sie vermuten, dass ein unbefugter Zugriff über das mobile Gerät auf Hochschuldaten erfolgt ist.

Vorfälle dieser Art sind dem zuständigen IT-Administrator und ggfs. dem Datenschutzbeauftragten zu melden, falls personenbezogene Daten von dem Vorfall betroffen sind.

2.1.3 Sorgfalt im Umgang mit mobilen Geräten

Folgende Empfehlungen sind zu berücksichtigen:

(1) Je nach Klassifikation der Informationen, muss eine Datenübertragung immer über verschlüsselte Kanäle erfolgen, um ein Ausspähen von Daten zu erschweren.

(2) Dienstliche Daten, bzw. Informationen sollten auf mobilen Endgeräten nur vorübergehend und verschlüsselt gespeichert werden.

(3) Benutzer sollten keine Geräteinhalte (wie etwa Mediendateien) auf Hochschulcomputern sichern oder synchronisieren, sofern dies nicht zu geschäftlichen Zwecken erfolgt.

(4) Für die Kommunikation mit dem Hochschulnetzwerk nutzen Sie am besten verschlüsselte Verbindungen bspw. VPN[4]. Für erhöhte Sicherheit bietet sich an VPN auch beim Abrufen Ihrer E-Mails von unterwegs einzusetzen.

(5) Sämtliche Funk- (WLAN, Bluetooth etc.), Infrarot- und andere Kommunikationsschnittstellen sollten deaktiviert werden, sofern diese nicht in Benutzung sind.

(6) Sämtliche installierte Anwendungen sollten offiziellen, vom Entwickler des jeweiligen Betriebssystems autorisierten Quellen, entstammen.

2.1.4 Rückgabe und Vernichtung

Für die Rückgabe und sichere Entsorgung dienstlicher Geräte bitte die IT-Administratoren anfragen.

[4] VPN: Virtual Private Network (siehe *Wikipedia*)

2.1.5 Öffentliches WLAN

Internetverbindungen, z.B. über WLAN-Verbindungen in Hotels, auf Flughäfen, Bahnhöfen oder in Zügen, können in erforderlichem Umfang genutzt werden, wenn die dafür vorgesehenen Schutzmaßnahmen vorhanden, aktuell und funktionstüchtig sind. Auch hier am besten VPN aktivieren.

2.2 Smartphones

2.2.1 Allgemeine Schutzmaßnahmen

Das Betriebssystem des Smartphones sollte auf dem jeweils aktuellen Stand gehalten werden. Zu diesem Zweck sind alle vom Hersteller verfügbaren Sicherheits-Patches, Updates und Upgrades zu installieren. Hierfür ist die automatische Updatefunktion der Smartphones günstig, die nicht deaktiviert werden sollte.

2.2.2 Sorgfalt im Umgang mit Smartphones

Der ordnungsgemäße Umgang mit dem Smartphone liegt in der Verantwortung der Nutzer. Diese sollten bei der Nutzung von Smartphones Folgendes berücksichtigen:

(1) Die PIN-Nummer sollte geheim gehalten werden, PIN-Nummer am besten 6-stellig.

(2) Sämtliche Funk- (WLAN, Bluetooth etc.), Infrarot- und andere Kommunikationsschnittstellen sowie Ortungsdienste sollten deaktiviert werden, sofern diese nicht benutzt werden. Das spart Akku und ist sicherer.

(3) Insbesondere Fotos, Videos aus dem Hochschulumfeld sollten regelmäßig gelöscht werden.

(4) Der Zugriff von Apps/Applikationen auf Kontakte/Mails/Bilder der Hochschule ist zu verhindern.

(5) Bei der Nutzung von QR-Codes[5] ist auf die Vertrauenswürdigkeit der Anbieter achten.

(6) Für den Zugriff auf Hochschuldaten vom privaten Smartphone aus, empfiehlt sich die Nutzung der vom RMZ empfohlenen App (Sophos Mobile ab September 2018).

2.3 Notebooks / Tablets

2.3.1 Allgemeine Schutzmaßnahmen

Schutzmaßnahmen gegen Viren oder sonstige Schadsoftware bitte regelmäßig durchführen und das Betriebssystem des Notebooks/Tablets o.ä. auf dem jeweils aktuellen Stand halten. Zu diesem Zweck sind alle vom Hersteller verfügbaren Sicherheits-Patches, Updates und Upgrades zu installieren. Darüber hinaus sollte die automatische Updatefunktion des Gerätes aktiviert bleiben. Es sollte die von RMZ empfohlene Sicherheitssoftware aktiviert sein.

2.3.2 Sorgfalt im Umgang mit Notebooks

Folgende Empfehlungen sind zu berücksichtigen:

(1) Zu Notebooks/Tablets der Hochschule sollten Dritte oder nicht autorisierten Personen keinen Zugang haben.

(2) Nur Geräte, welche nach Abstimmung mit den zuständigen IT-Administratoren installiert wurden, sollten kabelmäßig ans Netzwerk der Hochschule angeschlossen werden.

(3) Blickschutzfolien sind zu empfehlen, wenn eine Einsicht Dritter nicht ausgeschlossen werden kann.

(4) Illegal erworbene Software dürfen nicht auf Hochschulgeräte installiert werden.

[5] QR-Code: zweidimensionaler Code (siehe *Wikipedia*)

(5) Eine automatische passwortgeschützte Sperrung bei Inaktivität (z.B. Bildschirmschoner, Tastensperre) sollte aktiviert werden. Der Zeitraum der Inaktivität bis zur Sperrung sollte nicht mehr als 15 Minuten betragen.

(6) Mobile Geräte sind nach Möglichkeit physisch zu sichern, um einen Gelegenheitsdiebstahl zu vermeiden.

3 Home-Office / Heimarbeitsplätze / Zugriff von außen

3.1 Grundsätzliches

Tele- und Heimarbeitsplätze dürfen nur nach Genehmigung des Vorgesetzten eingerichtet und betrieben werden. Die Vorgaben der Dienstvereinbarung Tele- und Heimarbeit sind einzuhalten.

3.2 Arbeiten in fremder Umgebung

Bei einer Nutzung von Notebooks oder mobilen Datenträgern in fremden Umgebungen sind folgende Risiken zu beachten:

(1) Bei Gesprächen und Besprechungen über vertrauliche Sachverhalte ist darauf zu achten, dass diese Gespräche nicht von unbefugten Personen belauscht werden können.

(2) Das Speichern oder Verarbeiten von internen und vertraulichen Informationen auf fremden Systemen ist zu vermeiden.

(3) Interne und vertrauliche Informationen sollten nur auf Druckern ausgedruckt werden, bei denen die Ausgabe geeignet geschützt ist. Die Ausdrucke sollten umgehend vom Drucker abgeholt werden. Drucker und Kopierer mit umfangreichen Speicherfunktionen sollten für einen Ausdruck von vertraulichen Informationen vermieden werden.

4 Auskunftsanfragen

Vorsicht ist immer geboten, wenn telefonisch oder per E-Mail angefragt und Auskunft, beispielsweise zu einem Mitarbeiter oder Kunden, verlangt wird. Es kann weder nachvollzogen werden, ob der Anfragende tatsächlich derjenige ist, der er vorgibt zu sein, noch besteht die Möglichkeit die Rechtmäßigkeit einer Auskunft zu prüfen.

Beispiele hierfür sind:

- In welcher Abteilung arbeitet denn Person X?
- Wie lange arbeitet diese Person schon da?
- Wie lange dauert denn der Urlaub?
- Für welchen Zeitraum hat Kunde XY denn die Urlaubsunterbrechung beantragt?
- Wie oft hat denn Fa. XY bereits …?

Die Herausgabe solcher vermeintlich belangloseren Informationen kann Schäden verursachen. Verweisen Sie in einem solchen Falle an den Datenschutzbeauftragten. Er wird diese Anfragen prüfen und bearbeiten. Grundsätzlich gilt: Informationen sollten ohne Prüfung und Rechtsgrundlage NICHT an Dritte – auch nicht an Ermittlungsbehörden – herausgegeben werden.

4.1 Anfragen per Telefon

Bei telefonischen Anfragen sind folgende Empfehlungen zu beachten:

Der Anrufer ist freundlich zu bitten, sein Auskunftsbegehren schriftlich zu formulieren.

(1) Es ist ein Schreiben mit den Inhalten anzufordern:

a. Schilderung des Sachverhalts,
b. Beschreibung der begehrten Information,
c. Nennung der Rechtsgrundlage für die Auskunft.

(2) Anfertigen einer Aktennotiz zum Telefonat.

(3) Weiterleiten der Anfrage an den Fachbereichsverantwortlichen, bzw. den Informationseigentümer.

(4) Bei Fragen zu personenbezogenen Daten ist zusätzlich der Datenschutzbeauftragte einzubeziehen.

4.2 Anfragen per E-Mail, Fax oder Schreiben

Was für telefonische Anfragen gilt, ist auch bei schriftlichen Anfragen zu beachten. Es ist ein Leichtes E-Mails usw. zu fälschen und diese so aussehen zu lassen, als stammten sie von einer Behörde.

Bei solchen Anfragen sind folgende Vorgaben zu beachten:

(1) Auf keinen Fall die Anfrage selbst beantworten, bzw. den Eingang bestätigen.

(2) Weiterleiten der Anfrage an den Fachbereichsverantwortlichen, bzw. den Informationseigentümer,

(3) Bei Fragen zu personenbezogenen Daten ist zusätzlich der Datenschutzbeauftragte einzubeziehen.

5 Sichere Kommunikation am Telefon

Wenn der Anrufannehmende das Anliegen des Anrufers nicht selbst bearbeiten kann, sollte sichergestellt werden, dass er an die richtige Stelle weitergeleitet wird.

5.1 Erreichbarkeit

(1) Die telefonische Erreichbarkeit sollte bei Anwesenheit sichergestellt werden.

(2) Wird ein Rückruf gewünscht, ist die entsprechende Taste am Telefon zu betätigen.

(3) Bei längerer Abwesenheit sollten Anrufe auf eine(n) Kollegen/in umgeleitet werden.

(4) Alternativ wird die persönliche Voice Box aktiviert. Dort erfolgt ein Hinweis, an wen sich der Anrufende in dringenden Fällen wenden kann.

5.2 Verbinden von Gesprächen

(1) Es wird beim Verbinden empfohlen abzuwarten, bis der Angerufene das Gespräch annimmt.

Info vor Weiterverbinden: Name und Anliegen des Anrufers.

(2) Bei Nichterreichen: E-Mail an die gewünschte Person mit Namen, Telefonnummer, E-Mail-Adresse und Anliegen des Anrufers oder Herausgabe der Durchwahl/E-Mail-Adresse der/der Kollegin/Kollegen.

5.3 Empfehlungen für das Weiterverbinden

(1) Bedienstete wird namentlich verlangt: direktes Weiterverbinden.

(2) Funktion/Position wird verlangt, z.B. Vertriebsleiter: Nennung des Namens sowie der Durchwahl des Sekretariats/ Assistenz und E-Mailadresse des Fachbereichs.

(3) Angebote an das Unternehmen sind grundsätzlich schriftlich einzureichen: Nennung von Postanschrift/E-Mail-Adresse des Fachbereichs und ggf. Name des Ansprechpartners.

(4) Ist die Zielperson aufgrund von Krankheit oder Urlaub usw. nicht zu erreichen, darf kein Abwesenheitsgrund genannt werden.

5.4 Herausgabe von Kontaktdaten

Kann ein Gespräch nicht durchgestellt werden, so können folgende Kontaktdaten an den Anrufer herausgegeben werden:

(1) die Durchwahl des gewünschten Mitarbeiters,

(2) die Durchwahl des zuständigen Sekretariats,

(3) die E-Mail-Adresse des Fachbereichs.

5.5 Herausgabe personenbezogener Daten am Telefon

Bei Kundenanfragen dürfen ausschließlich Informationen herausgegeben werden, wenn die Identität des Anrufenden sichergestellt ist. Hierzu gelten folgende Vorgaben:

- Prüfung der Identität (telefonisch)
- Name
- Adresse (PLZ / Straße)
- Geburtsdatum
- Matrikelnummer
- Weitere....

Für die Sicherstellung der Identität des Anrufers sollten mindestens 3 korrekte Angaben vom Anrufer gemacht werden! Sollten dennoch Zweifel an der Identität bestehen, ist auf einen persönlichen Besuch zu verweisen.

Ist die Sicherstellung nicht möglich, ist der Anrufende auf einen persönlichen Besuch, einschließlich Ausweispapieren, zu verweisen.

6 Datenschutzrechtliche Vorgaben (EU-DSGVO)

6.1 Betrieblicher Datenschutzbeauftragter (DSB) nach Art. 39 EU-DSGVO

Der betriebliche Datenschutzbeauftragter hat folgenden Aufgaben:

(1) die ordnungsgemäße Anwendung der Datenverarbeitung zu überwachen,

(2) die Mitarbeiter/innen durch geeignete Maßnahmen mit den Vorschriften des Datenschutzes vertraut zu machen,

(3) bei besonderen Verfahren die Vorabkontrolle durchzuführen und

(4) die Datenschutzdokumentation, insbesondere das interne und externe Verfahrensverzeichnis, zu führen.

Im Rahmen dieser gesetzlich normierten Pflichten bzw. Aufgaben ergeben sich folgende Detailaufgaben:

(1) Durchführung von Prüfungen/Analysen über den Stand von Datenschutz und Datensicherung,

(2) Beratung im Zusammenhang mit datenschutzrechtlich relevanten Verträgen und Vereinbarungen, z.B. bei Datenverarbeitung im Auftrag, Wartungsverträgen, Betriebsvereinbarungen u.a.,

(3) Beratungsaufgaben für die Verfahrensentwickler/innen, Anwender/innen, Benutzer und Betroffene,

(4) Prüfung und Dokumentation der Zulässigkeit von EDV-Verfahren und Festlegung von Auskunfts- und Benachrichtigungspflichten,

(5) Sicherstellung der Rechte von Betroffenen, d.h. Recht auf Auskunft, Recht auf Berichtigung, Sperrung oder Löschung von Daten,

(6) Beratung bezüglich Hinweis- und Unterrichtungspflichten gegenüber Betroffenen, z.B. im Zusammenhang mit Werbung, Markt- und Meinungsforschung oder Übermittlung von Daten,

(7) Erarbeitung von Datenschutzregelungen und Verfahrensanweisungen zu den technischen und organisatorischen Maßnahmen des Datenschutzes und Kontrolle ihrer Einhaltung.

6.2 Grundsätze des Datenschutzes (EU-DSGVO)

Wer personenbezogene Daten verwenden möchte, muss die Grundprinzipien des Datenschutzrechts einhalten:

(1) **Verbot mit Erlaubnisvorbehalt**: Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist grundsätzlich verboten. Eine Ausnahme besteht nur dann, wenn es eine ausdrückliche gesetzliche Regelung dafür gibt oder die Betroffenen in die Verarbeitung Ihrer Daten eingewilligt haben.

(2) **Direkterhebung**: Eine Datenerhebung, also das Beschaffen von Daten, ist nur beim Betroffenen unmittelbar selbst zulässig. Das bedeutet, dass das Beschaffen von Daten nur unter Mitwirkung des Betroffenen zulässig ist.

(3) **Datensparsamkeit**: Daten sollen nicht für unbegrenzte Zeit aufbewahrt werden, sondern es soll mit ihnen sparsam umgegangen werden. Das bedeutet, dass sie zu löschen sind, wenn sie nicht mehr gebraucht werden. Dabei gibt es für unterschiedliche Datenkategorien unterschiedlich lange Aufbewahrungsfristen.

(4) **Datenvermeidung**: Bereits bei der Entwicklung und Auswahl von Datenverarbeitungssystemen und bei der Ausgestaltung der konkreten Datenverarbeitungsprozesse ist darauf hinzuwirken, dass möglichst wenig personenbezogene Daten verarbeitet werden.

(5) **Zweckbindung**: Jeder Datenverarbeitung muss ein bestimmter Zweck zugrunde liegen. Dieser ist vor der Verarbeitung festzulegen und zu dokumentieren. Nur zu diesem zuvor ursprünglich festgelegten, nicht jedoch zu einem anderen Zweck darf eine Verarbeitung und Nutzung erfolgen. Eine Ausnahme bildet wieder die vorher erteilte freiwillige Einwilligung des Betroffenen.

(6) **Transparenz**: Der Betroffene muss über die Verarbeitung seiner personenbezogenen Daten von der verarbeitenden Stelle informiert werden. Das Transparenzgebot wird gewährleistet durch Hinweispflichten über die personenbezogenen Daten, Unterrichtungspflichten über Profilbildungen und über die Möglichkeit anonymer und pseudonymer Nutzung, Informationspflichten über die Identität der verantwortlichen Stelle und über die Auskunftsansprüche der Betroffenen.

(7) **Erforderlichkeit**: Die Einhaltung des Erforderlichkeitsgrundsatzes im Einzelfall ist bereits in der Konzeptions- und Planungsphase von Anwendungen und bei der Systemauswahl zu berücksichtigen. Insofern korrespondiert die Vorgabe mit den Geboten zur Datenvermeidung und Datensparsamkeit. Das Gebot der Erforderlichkeit gilt für alle Phasen der Verarbeitung, also nicht nur für die Erhebung, sondern auch für den gesamten anschließenden Verarbeitungsprozess.

6.3 Verzeichnis von Verarbeitungstätigkeiten

Werden personenbezogene Daten durch automatisierte Verfahren verarbeitet, ist eine Gesamtübersicht über die im Einsatz befindlichen Verarbeitungsverfahren zu erstellen. Zweck dieses Verfahrensverzeichnisses ist die Überprüfbarkeit der Zulässigkeit des Umgangs mit personenbezogenen Daten.

Für jedes neue Verfahren oder Änderung an einem bestehenden Verfahren ist die Verfahrensbeschreibung zu erstellen oder anzupassen.

6.4 Beteiligung des DSB

Der DSB ist ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen, Planungen oder Verfahren einzubinden und zu beteiligen.

6.5 Prüfpflichten des Datenschutzbeauftragten

Datenschutz-Folgenabschätzung Art. 35 DSGVO

Eine Datenschutz-Folgenabschätzung ist durch den Datenschutzbeauftragten (DSB) bei automatisierten Verfahren durchzuführen, wenn besondere Risiken für die Rechte und Freiheit der Betroffenen nicht ausgeschlossen werden können.

Die Datenschutz-Folgenabschätzung hat nach dem Erhalt / der Erstellung der Verfahrensbeschreibung und vor Beginn / Inbetriebnahme der Verarbeitung zu erfolgen und ist schriftlich zu dokumentieren.

6.6 Rechte der Betroffenen

6.6.1 Das Auskunftsrecht

Betroffenen steht gemäß Art. 15 DSGVO ein Auskunftsrecht zu. Das Unternehmen hat in diesem Rahmen Auskunft über die gespeicherten Daten des Betroffenen zu geben. Dies betrifft die zu seiner Person gespeicherten Daten, die Herkunft der Daten, sowie die Empfänger bzw. die Empfängerkategorien.

Im Falle eines Auskunftsersuchens ist der Datenschutzbeauftrage, bzw. der Datenschutzkoordinator umgehend zu informieren.

6.6.2 Der Widerspruch

Einzelfallbezogen kann dem Betroffenen ein Widerspruchsrecht zustehen, wenn er aufgrund bestimmter Umstände besonders schutzbedürftig ist. Aufgrund der besonderen Umstände bei der Markt-, Meinungsforschung und der Werbung sieht hier Art. 21 DSGVO ein Widerspruchsrecht vor, welches keiner Begründung bedarf. Für diese Zwecke dürfen erhobene und/oder erhaltene personenbezogene Daten nur mit vorheriger ausdrücklicher Einwilligung verarbeitet werden. Der Betroffene ist in diesen Fällen sowohl bei erstmaliger Erhebung auf das jederzeitige Widerspruchrecht hinzuweisen, als auch gesondert bei jeder werblichen Ansprache.

Sofern von der Möglichkeit des Widerspruchs Gebrauch gemacht wird, ist umgehend der Datenschutzbeauftragte, bzw. der Datenschutzkoordinator zu kontaktieren.

6.6.3 Anspruch auf Berichtigung, Löschung und Sperrung der Daten

Ein Anspruch auf **Berichtigung** besteht dann, wenn die gespeicherten Daten fehlerhaft, veraltet oder sonst wie unrichtig sind.

Ein Anspruch auf **Löschung** besteht, wenn die Speicherung der personenbezogenen Daten unzulässig ist, die Richtigkeit besondere Arten personenbezogener Daten von der verantwortlichen Stelle nicht nachgewiesen werden kann, der Zweck der Verarbeitung erfüllt und eine Speicherung daher nicht mehr erforderlich ist oder bei zum Zwecke der Übermittlung gespeicherten Daten eine längere Speicherung nicht mehr erforderlich ist.

Kommt eine Löschung aufgrund bestimmter Umstände nicht in Betracht, so sind die betreffenden personenbezogenen Daten stattdessen zu **sperren** (bspw., wenn dem gesetzliche Aufbewahrungsfristen entgegenstehen).

Wird von dem Anspruch auf Berichtigung, Löschung und Sperrung von Daten Gebrauch gemacht, ist der Datenschutzbeauftragte, bzw. der Datenschutzkoordinator umgehend in Kenntnis zu setzen.

6.7 Meldepflichten

6.7.1 Meldepflichten gegenüber Behörden

Eine Informationspflicht gegenüber der Aufsichtsbehörde besteht, wenn

- die verantwortliche Stelle feststellt, dass Dritte von besonders sensiblen Daten unrechtmäßig Kenntnis erlangt haben,
- die „Datenpanne“ besonders sensible Daten betrifft,
- eine schwerwiegende Beeinträchtigung für die Betroffenen droht (hohes Gefahrenpotential).

Es ist umgehend der Datenschutzbeauftragte, bzw. der Datenschutzkoordinator zu kontaktieren. Erst nach Klärung der Sachlage und der Ermittlung der weiteren Vorgehensweise ist die Aufsichtsbehörde zu verständigen.

6.7.2 Meldepflichten gegenüber Betroffenen

Eine Informationspflicht gegenüber den Betroffenen besteht, wenn

- die verantwortliche Stelle feststellt, dass Dritte von besonders sensiblen Daten unrechtmäßig Kenntnis erlangt haben,
- die „Datenpanne“ besonders sensible Daten betrifft,
- eine schwerwiegende Beeinträchtigung für die Betroffenen droht (hohes Gefahrenpotential).

Vor der Kontaktaufnahme des Betroffenen ist umgehend der Datenschutzbeauftragte, bzw. der Datenschutzkoordinator zu kontaktieren.

6.8 Datensicherheitsbewusstsein, Ausbildung und Schulung

Alle Bediensteten der Hochschule sowie gegebenenfalls Auftragnehmer sollten in geeigneter Weise aufgeklärt und geschult werden und regelmäßige Ergänzungen zu organisatorischen Leitlinien und Verfahren erhalten, die für ihre berufliche Funktion maßgebend sind.

Die jeweiligen Sensibilisierungs- und Awareness-Schulungen werden von DSB und ISB erarbeitet und sind im DSMS-Handbuch definiert.

Spezielle Anforderungen und Bedarfe sind mit DSB und ISB abzustimmen und können als Sondermaßnahmen umgesetzt werden.

7 Klassifikation von Informationen

7.1 Grundlagen

Die an der Hochschule vorhandenen Informationen sollten nach ihrer Vertraulichkeit klassifiziert werden. Die Vertraulichkeit ist abhängig von ihrer Bedeutung für die internen Prozesse oder dem potenziellen Schaden bei falschem Umgang mit ihnen.

Informationen sollten in folgende Vertraulichkeitsklassen eingestuft:

- Öffentlich
- Intern
- Vertraulich
- Streng vertraulich

7.2 Schadensgrößen

Für die korrekte Einstufung von Informationen in die jeweiligen Vertraulichkeitsklasse ist das Wissen um den potenziellen Schaden bei unerwünschter Offenlegung oder Weitergabe an Dritte unerlässlich.

Schadensgröße	Schaden für die Hochschule	Vertraulichkeitsklasse	Beispiele
Keiner	- Kein Schaden, da Information für Öffentlichkeit bestimmt	**Öffentlich**	- Freigegebene Flyer - Beschreibung von öffentlichen Projekten, …
Gering	- Keine weitreichenden Konsequenzen	**Intern**	- Organigramme
Mittel	- Betroffen ist ein Hochschulbereich - Erheblicher finanzieller Schaden - Rechtliche Konsequenzen bis hin zu Ordnungswidrigkeiten und Geldstrafen - Imageverlust - Personenbezogene Daten gemäß Landesdatenschutzgesetz	**Vertraulich**	- Informationen, die im Rahmen von Vertraulichkeitsvereinbarungen erlangt wurden - Kontaktdaten von Geschäftspartner - Kalkulationen - Arbeitsverträge - Mitarbeiterbeurteilungen - Bewertungen von Prüfungen
Groß bis existenzgefährdend	- Betroffen ist die gesamte Hochschule - Sehr schwerer Schaden für die Geschäftszwecke und Ziele - Gravierende rechtliche Konsequenzen bis hin zu Haftstrafen - Erheblicher Verlust von Ansehen und Vertrauen	**Streng vertraulich**	- Strategieunterlagen - Daten von gravierenden Störfällen - Ergebnisse Technik-Benchmark - Passwörter - Brief an Kooperationspartner bzgl. Vertraulichen Forschungsprojekten

Tabelle 1 - Schadensgrößen

Es wird empfohlen die Vertraulichkeitsklasse in die Fußzeile eines jeden Dokumentes einzufügen.

Unberührt von dieser Richtlinie bleiben die Sonderfälle der Geheimhaltungsbedürftigkeit gemäß § 79 BetrVG, § 96 SGB IX (Bekanntgabe von Betriebs- und Geschäftsgeheimnissen gegenüber BR, JAV und Schwerbehindertenvertretung).

7.2.1 Klassifizierung von Angeboten und Verträgen

Angebote und Verträge zu Geschäften über allgemein angebotene Leistungen zu allgemein bekannten Gegenleistungen ohne besondere Nebenabreden werden in die Vertraulichkeitsklasse „*intern*“ eingestuft. Andere Angebote und Verträge sind je nach Inhalt als „*vertraulich*“ oder „*streng vertraulich*“ einzustufen.

Weitergehende Anforderungen, z.B. des Vergaberechts, bleiben unberührt.

7.2.2 Klassifizierung Informationen Dritter

Grundsätzlich gelten für Informationen, die uns überlassen und mit einer Vertraulichkeitsklasse gekennzeichnet wurden, die gleichen Regelungen wie für interne Informationen.

8 Umgang mit Störungen und Sicherheitsvorfällen

8.1 Definition Störung

Störungen sind Vorfälle ohne Gefährdung von Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität und Revisionsfähigkeit der Daten oder in Verbindung mit einer vorübergehenden Gefährdung der Verfügbarkeit von Daten, von Hard- oder Software oder der Funktionsfähigkeit von Datenverarbeitungsverfahren.

Störungen verletzen nicht unsere Sicherheitsziele.

Beispiele:

- Arbeitsplatzrechner startet nicht,
- iPhone / iPad ist defekt,
- Drucker funktioniert nicht,
- U.v.m.

Störungen werden vom Service Desk entgegengenommen, dokumentiert und durch die zuständigen IT-Administratoren behandelt.

8.2 Definition Sicherheitsvorfälle

Ein Sicherheitsvorfall ist ein Ereignis oder eine festgestellte Situation, bei der unsere Sicherheitsziele in Bezug auf:

- Vertraulichkeit,
- Integrität und
- Verfügbarkeit

verletzt, bzw. gefährdet wurden oder der Versuch unternommen wurde, diese zu verletzen.

Sicherheitsvorfälle sind nicht zwingend ereignisbezogen. Auch Situationen, die bereits länger bestehen, deren Entdeckung aber den Schluss zulässt, dass ein unangemessenes Risiko für die Informationssicherheit des Unternehmens besteht, werden als Sicherheitsvorfälle behandelt.

Beispiele:

- E-Mails mit Schadcode, z.B. Verschlüsselungstrojaner,
- Anrufe mit dem Versuch vertrauliche Informationen zu erhalten,
- Ungewöhnliches Verhalten des Arbeitsplatzrechners,
- Verlust oder Diebstahl des iPhones/iPads,
- U.v.m.

8.3 Zielsetzung Sicherheitsvorfallbehandlung

Durch eine effiziente Sicherheitsvorfallbehandlung soll sichergestellt werden, dass Sicherheitsvorfälle ausgewertet und Erkenntnisse für die langfristige Weiterentwicklung und Verbesserung des Sicherheitsprozesses und -konzeptes gewonnen werden.

8.4 Verhalten bei Sicherheitsvorfällen

Die Benutzer sollten alle sicherheitsrelevanten Störungen oder beim Verdacht auf sicherheitsrelevante von IT-Systemen, sowie sonstige Vorfälle in Bezug auf die Sicherheit der Daten der Hochschule melden.

Beim Auftreten von Sicherheitsvorfällen oder bei einem entsprechenden Verdacht und bei sonstigen, nicht zuzuordnenden Störungen ist folgendermaßen zu verfahren:

(1) Bedienstete sollen nicht versuchen den Vorfall selbst aufzuklären oder etwas gegen den Verursacher zu unternehmen.

(2) Laufende Programme sind zu beenden.

(3) Neue Programme dürfen nicht mehr gestartet werden.

(4) Es dürfen keine Daten oder E-Mails mehr versandt werden.

(5) Systemhinweise und Systemmeldungen sind festzuhalten.

(6) Der Service Desk oder die zuständigen IT-Administratoren sind umgehend zu informieren.

9 Zutrittsschutz / Physische Sicherheit

Ein unverzichtbarer Beitrag zur Sicherheit der Hochschule sind vorbeugende Maßnahmen, die die Entstehung von Gefahrensituationen verhindern sollen. Zu diesem Zweck sind die folgenden Vorgaben zu beachten.

9.1 Umgang mit Zutrittsmitteln (Hochschulausweis, Schlüsseln, etc.)

Der Schlüssel/Chip ist ausschließlich zur persönlichen Verwendung vorgesehen. Er muss sicher aufbewahrt werden. Eine Weitergabe an Dritte ist nicht vorgesehen.

Der Verlust des Schließmittels ist unmittelbar der verantwortlichen Stelle mitzuteilen.

9.2 Umgang mit Besuchern

Besucher können, wenn sie unbegleitet oder nicht über die Maßnahmen/Vorgaben der Hochschule informiert sind, Zugriff oder Einsicht in Unterlagen, Datenträger oder Geräte haben, diese beschädigen oder unbefugt Kenntnis von schützenswerten Informationen erlangen. Externe Mitarbeiter können zudem bei ungesicherten Verbindungen bzw. der Nutzung von externen Speichermedien (USB, Festplatte, Disc etc.) versehentlich oder willentlich Schadsoftware auf das Firmennetzwerk übertragen. Gleiches gilt für die unsachgemäße Handhabung von IT-Geräten.

9.2.1 Grundsätzliches

Die wichtigste Voraussetzung für den Schutz der Hochschule, aber auch des Besuchers, ist dessen Begleitung innerhalb des Gebäudes durch einen Bediensteten, insbesondere in Laboren und Büros.

Ist es nicht möglich, Fremdpersonen (z. B. Reinigungspersonal) ständig zu begleiten oder zu beaufsichtigen, sollte zumindest der persönliche Arbeitsbereich abgeschlossen werden: Schreibtisch, Schrank und PC (Zugriffssperre aktiviert).

Für den häuslichen Arbeitsplatz gilt, dass Familienmitglieder und Besucher sich nur dann alleine im Arbeitsbereich aufhalten sollten, wenn alle Arbeitsunterlagen verschlossen aufbewahrt sind und die verwendeten IT-Systeme über einen aktivierten Zugriffsschutz gesichert sind.

9.2.2 Allgemeine Vorgaben

Folgende Punkte betreffen v.a. die zutrittsgeschützten Bereiche der Hochschule und sollten von allen Mitarbeitern berücksichtigt werden:

(1) Der Zugang zu den zutrittsgeschützten Sicherheitsbereichen der Hochschule ist berechtigten Mitarbeitern und Personen vorbehalten.

(2) Besucher sind möglichst vorab anzukündigen.

(3) Hinweis an die Besucher, sich nicht in bestimmten Bereichen (Serverräumen, Laboren etc.) aufzuhalten.

(4) Werden von Besuchern Dienstleistungen in besonderen Betriebsräumen, z.B. Rechenzentrum, etc., erbracht, so muss der Besucher auf die einzuhaltenden Regeln und besondere Gegebenheiten der Örtlichkeiten hingewiesen werden.

(5) Es sollte darauf geachtet werden, dass Besucher keine externen Geräte an das Firmennetzwerk anschließen, da hierdurch Schadsoftware übertragen werden kann. Die Anbindung kann an dafür vorgesehenen Gästenetze (Gast-WLAN) erfolgen.

9.3 Schließen der Türen und Fenster

Zur Vorbeugung von Diebstahl und Einbrüchen sind Büroräume und Türen zutrittsgesicherter Sicherheitsbereiche bei Abwesenheit geschlossen zu halten.

Um Schäden durch Gewitter und Unwetter zu vermeiden und um Diebstahl und Einbrüchen vorzubeugen, sind Fenster beim Verlassen eines Raumes zu schließen.

10 Verlassen des Arbeitsplatzes

10.1 Clean Desk

In Räumen mit Publikumsverkehr sind IT-Arbeitsplätze so anzuordnen, dass betriebsfremde Personen keinen unmittelbaren Einblick auf die Bildschirme haben, ggf. sind die Monitore mit Sichtschutzfolien gegen unbefugte Einsichtnahme zu schützen. Ebenso dürfen Drucker nur so aufgestellt werden (z. B. in Sicherheitszonen), dass unbefugte Personen keinen Zugang zu den Druckerzeugnissen besitzen. Ausdrucke sind nach Veranlassung des Druckprozesses unverzüglich vom Drucker abzuholen. Nach Möglichkeit, insbesondere für vertrauliche Vorgänge, sind vertrauliche Druckfunktionen zu benutzen.

Dokumente sind nicht frei und offen am Arbeitsplatz liegen zu lassen. Falschausdrucke und Duplikate sind nach Möglichkeit umgehend zu vernichten, um die Einsichtnahme Dritter zu verhindern. Gerade bei Arbeitsplätzen mit Publikumsverkehr ist auf das Einrichten eines automatischen Bildschirmschoners zu achten, der nach kurzer Dauer (unter fünf Minuten) ohne Benutzereingabe wirksam wird.

Weiterhin sollten die Monitore an sensiblen Arbeitsplätzen über einen Sichtschutz (Folie) verfügen.

10.2 Längere Abwesenheit / nach der Arbeit

Folgende Maßnahmen müssen beim Verlassen des Arbeitsplatzes durchgeführt werden:

(1) Abmeldung des Benutzers vom System oder die Aktivierung der Bildschirmsperre (passwortgeschützter Bildschirmschoner). Unabhängig davon muss diese automatisch nach einer Zeitspanne von fünf bis zehn Minuten ohne Benutzereingabe wirksam werden.

(2) Bei längerem Verlassen des Arbeitsplatzes (länger als 30 bis 45 Minuten) sind alle offenen Anwendungen zu schließen und noch benötigten Daten abzuspeichern, um einen Datenverlust zu vermeiden.

(3) Datenträger, Ausdrucke oder sonstige Unterlagen mit vertraulichem/streng vertraulichem Inhalt sind grundsätzlich bei Verlassen des Arbeitsplatzes unter Verschluss zu halten.

Folgende Maßnahmen müssen zusätzlich bei Arbeitsende durchgeführt werden:

(1) Endgeräte wie PCs, Monitore oder Drucker sind auszuschalten.

(2) Offene Anwendungen sind zu schließen und noch benötigte Daten abzuspeichern, um einen Datenverlust zu vermeiden.

(3) In nicht abgeschlossen Räumen sind Notebooks, die nicht durch ein Kabelschloss gesichert sind, einzuschließen.

(4) Soweit keine anderweitigen Regelungen entgegenstehen, sind abschließbare Einzelbüros beim Verlassen abzuschließen.