HOCHSCHULE OSNABRÜCK
UNIVERSITY OF APPLIED SCIENCES

Richtlinie IT-Sicherheit und Datenschutz der Hochschule Osnabrück

- Veröffentlicht am 27. Mai 2019 -

Inhaltsverzeichnis

1. Inhalt und Ziel dieser Richtlinie

Ziel dieser Richtlinie ist es, das Personal und die Studierenden der Hochschule Osnabrück für die Belange des Datenschutzes und der IT-Sicherheit zu sensibilisieren, um eine störungsfreie, datenschutzkonforme und sichere Nutzung von IT und Daten zu gewährleisten. Das unsachgemäße Verhalten der eigenen IT-Nutzenden ist nachweislich Grundlage eines erheblichen Teils von Sicherheits- und Datenschutzvorfällen. Daher ist die Verbesserung der entsprechenden Kenntnisse und die Erhöhung der Eigenverantwortung jedes IT-Nutzenden eine wirksame Maßnahme zur Verbesserung von IT-Sicherheit und Datenschutz.

Diese Richtlinie ersetzt die bisherige IT-Sicherheitsrichtlinie der Hochschule Osnabrück. Die Umbenennung in Richtlinie zu IT-Sicherheit und Datenschutz liegt darin begründet, dass die Europäische Datenschutzgrundverordnung (EU-DSGVO) auch die nichtautomatisierte und papiergebundene Verarbeitung von Daten betrifft. Die betroffenen Regelungen wurden im Hinblick auf die EU-DSGVO angepasst und ergänzt.

Die vorliegenden Regelungen und Empfehlungen dienen einer sicheren und datenschutzkonformen Nutzung der IT sowie der papiergebundenen Daten der Hochschule Osnabrück. Die Wissenschaftsfreiheit wird von den Regelungen und Empfehlungen nicht eingeschränkt.

Viele der Regelungen sind allgemein gehalten. Bei Fragen zur konkreten Umsetzung der Regelungen wenden Sie sich bitte grundsätzlich an den ServiceDesk.

2. Geltungsbereich und gesetzliche Grundlagen

Diese Richtlinie gilt für jegliche automatisierte und nichtautomatisierte Informationsverarbeitung in der Hochschule Osnabrück (Fakultäten, Labore, Rechnerpools, Institute, zentrale Geschäftsbereiche, zentrale Einrichtungen, etc.). Sie betrifft damit insbesondere den Einsatz von IT. Zudem ist darauf zu achten, die Regelungen und Empfehlungen auch bei der Nutzung privater Geräte im Rahmen der dienstlichen Tätigkeit zu berücksichtigen.

Die Richtlinie basiert auf der EU-DSGVO, dem Bundesdatenschutzgesetz (BDSG), dem Niedersächsischen Landesdatenschutzgesetz (NLDG), den damit in Verbindung stehenden Verordnungen sowie dem Urheberrechtsgesetz in Bezug auf den disziplinierten und sorgfältigen Umgang mit Daten.

Ein vorsätzliches oder grob fahrlässiges Abweichen von den Regelungen und Empfehlungen kann disziplinarische Maßnahmen nach sich ziehen und im Schadensfall Haftungsansprüche auslösen.

3. Vorgaben und Empfehlungen für IT-Nutzende

Die in den folgenden Abschnitten aufgeführten Regelungen, Empfehlungen und Hinweise gelten für sämtliche IT-Nutzenden der Hochschule Osnabrück. Sie bilden die Grundlage für eine sichere und störungsfreie IT-Nutzung und sollen die Hochschule und Mitarbeitenden vor Schäden schützen.

3.1. Generelle Sicherung der Systemintegrität

Wenn ein System nicht manipuliert wurde, spricht man von einem integren System. Durch Schadsoftware infizierte Rechner können beispielsweise folgende Auswirkungen haben:

- Tastaturanschläge werden an den Angreifenden übermittelt (Benutzername, Passwörter, etc.) oder
- der Rechner wird für Straftaten genutzt (der Anfangsverdacht liegt dann beim regulären Nutzenden) oder
- der Rechner wird unbenutzbar langsam, da die Schadsoftware zu viele Ressourcen benötigt.

Nachstehende Grundregeln sind zum Schutz der Systemintegrität einzuhalten:

1. Die Verwendung eines durch die Hochschule freigegebenen Virenscanners ist Pflicht!

Es ist darauf zu achten, dass ein Virenscanner aktiv ist und sich automatisch aktualisiert. Meldungen des Virenscanners, die auf einen Befall oder eine Schädigung des Systems hinweisen, sind umgehend dem ServiceDesk zu melden.

2. Das Ausführen von Schadsoftware ist verboten!

Das Ausführen von Schadsoftware hat negative Folgen und bedingt Schäden für die Hochschule, die vom Zusatzaufwand für Systembereinigungen bis zur Reputationsschädigung reichen können.

3. Eingesetzte Software ist stets auf einem aktuellen Stand zu halten!

Softwareaktualisierungen beheben i.d.R. Schwachstellen und Sicherheitslücken. Halten Sie daher Ihr Betriebssystem und die genutzte Software immer auf einem aktuellen Stand. Viele Programme (Windows, Virenschutz, etc.) bieten eine Autoupdate-Funktion, um Schwachstellen schnell zu beheben. Achten Sie darauf, dass diese aktiviert ist. Bei Software ohne Autoupdate-Funktion, sind Sie für die Software-Aktualisierung und die Beachtung zugehöriger Herstellerangaben verantwortlich.

Generell gilt: Je aktueller der Softwarestand, desto sicherer ist das System.

Sollte ein Hersteller einer Software oder eines Betriebssystems keine Sicherheitsupdates mehr bereitstellen, darf das entsprechende Gerät nicht mehr verwendet werden. Dies gilt in besonderem Maße auch für mobile Geräte.

4. Datenträger unbekannter Herkunft sind nicht einzulesen/ zu verwenden!

Aufgrund automatischer Mechanismen kann das Einstecken eines Datenträgers bereits für eine Infektion ausreichen. Diese Gefahr besteht vor allem bei Datenträgern unbekannter Herkunft. Sollten Sie USB-Sticks oder andere Datenträger finden, geben Sie diese bitte beim ServiceDesk zur Überprüfung ab. So stellen Sie sicher, dass keine Schadsoftware in Umlauf gerät.

5. Sicherheits- und Inventarisierungsclient nicht deaktivieren oder ändern!

Auf den vom ITSC ausgelieferten Geräten wird in der Regel eine Software installiert, welche zum einen die installierten Produkte erfasst und auf Aktualität überprüft und zum anderen die Möglichkeit bietet, zentral vorgegebene Sicherheitseinstellungen zu verteilen.

Hinweis: Diese Software darf nicht deaktiviert oder deinstalliert werden. Sie ist zusätzlich essentieller Bestandteil der Inventarisierung und des Lizenzmanagements der Hochschule.

6. IT-Geräte und Rechner der Hochschule sind vor unzulässigen Zugriffen aus dem Internet zu schützen.

Die Zugriffsmöglichkeit auf das Internet ist eine Standardanforderung für die meisten IT-Geräte. Zudem sind IT-Geräte der Hochschule vor unzulässigen Zugriffen aus dem Internet zu schützen. Diese Anforderung kann durch den Einsatz gängiger Firewalls und bereitgestellter Schutzprogramme erfüllt werden.

Betriebssystemfirewalls müssen aktiviert sein und sind den Anforderungen entsprechend zu konfigurieren. In der Regel sind die vom ITSC installierten und betreuten Geräte mit geeigneten Schutzmaßnahmen (Betriebssystemfirewall, Virenschutz, usw.) vorkonfiguriert. Diese Sicherheitseinstellungen werden kontinuierlich überprüft und angepasst.

Es ist untersagt, diese Schutzmechanismen zu deaktivieren oder eine eingerichtete Möglichkeit der Fernkonfiguration zu unterbinden.

IT-Geräte, auf die ein Zugriff aus dem Internet oder von zu Hause nicht direkt möglich ist, können mittels einer VPN-Verbindung erreicht werden. Auf diese Weise arbeiten Sie weltweit so, als ob Sie im Hochschulnetz wären.

Bitten wenden Sie bei Fragen hierzu an den ServiceDesk.

3.2. Kennungen und Passwörter

Passwörter in Verbindung mit Kennungen sind der hochschulweit am häufigsten verwendete Schutzmechanismus für den Zugang zu Systemen, Anwendungen und Daten. Die zentrale Hochschulkennung ermöglicht den Zugriff auf

- E-Mails und Kalender,
- Netcase inkl. der Verwaltung der Freigaben und
- den OSCA-Account, damit Teamräumen und i.d.R. personenbezogenen Daten von Studierenden und weiteren Personen.

Daneben ist der Zugang zu anderen IT-Geräten der Hochschule, wie Rechnern, Servern, Poolrechnern, Netzkomponenten oder IoT (Internet of Things) -Geräten i.d.R. auch per Passwort geschützt.

Unsichere oder ausgespähte Passwörter erlauben nicht nur Zugang zu den betreffenden Anwendungen bzw. dem Gerät, sondern dienen Angreifenden auch als Einstiegspunkt, von dem aus sie gezielt weitere Systeme über das Netzwerk angreifen. Daher ist es wichtig, dass durchgängig sichere Passwörter verwendet und diese zudem angemessen geschützt werden. Bereits ein unsicheres Passwort erlaubt Angreifenden den Zugriff auf die Systeme der Hochschule.

Sie gefährden daher die Sicherheit von Systemen und Daten der Hochschule, wenn Sie das Passwort Ihrer Hochschulkennung

- unsicher wählen,
- nicht geheim halten oder unsicher damit umgehen,
- in Internet-Anwendungen Dritter (Shops, Auktionen, etc.) verwenden, oder
- nach einer Offenlegung weiterverwenden).

Das Ermitteln fremder Kennungen und Passwörter wird als Identitätsdiebstahl bezeichnet, da der Angreifende im fremden Namen handeln kann, sobald das Passwort bekannt ist.

Nachfolgende Hinweise und Regeln sind zu beachten:

1. Verwenden Sie sichere Passwörter!

Gerne werden Telefonnummern, Geburtstage, Namen, Tastenfolgen („asdf“) oder Kombinationen dieser als Passwort verwendet. Zur Erhöhung der Sicherheit werden darüber hinaus oft einzelne Zeichen durch Sonderzeichen ersetzt, Zahlen ein- oder angefügt oder Worte rückwärts geschrieben. Solche Passwörter bieten jedoch nur eine begrenzte Sicherheit, da sie durch sogenannte Wörterbuch-Angriffe schnell automatisiert ermittelt werden können.

Sind Passwörter zu kurz, können sie schnell durch automatisiertes Testen aller möglichen Buchstaben- und Zahlenkombinationen ermittelt werden.

Wirklich zufällig gewählte Passwörter bieten einen guten Schutz - sind jedoch schwer zu merken.

Ein mögliches Verfahren, Passwörter zu bilden, die sicherer sind und an die man sich trotzdem recht gut erinnern kann, ist es, die Anfangsbuchstaben der Worte eines frei gewählten Satzes als Passwort zu nutzen.

Beispiel: Als eine Mitarbeitende der Hochschule Osnabrück sollte ich nur sichere Passwörter verwenden. -> Passwort „A1MdHOsinsPv“.

Die Anforderungen an das Passwort, werden zentral vorgegeben und kontinuierlich angepasst. Das heißt, beim Wechsel des Passworts Ihrer Hochschul-Kennung werden grundlegende Komplexitätsanforderungen serverseitig sichergestellt. Dies entbindet Sie aber nicht von der Pflicht ein sicheres Passwort eigenständig auszuwählen und zu prüfen. Achten Sie auf weitere Informationen in der Infothek bzw. im Passwortwechseldialog in OSCA.

Die Hochschule orientiert sich hierbei an den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik.

2. Halten Sie Ihre Passwörter geheim!

Sie dürfen niemals

- Passwörter weitergeben, auch nicht an Kolleg*innen
- Passwörter am Telefon nennen
- Passwörter unsicher verwahren
- Passwörter in E-Mails versenden
- Passwörter auf ungeschützten Internet-Seiten eingeben

Behandeln Sie Passwörter mit der gleichen Sorgfalt wie Ihren Haustürschlüssel oder Ihre Kreditkarte. Wenn jemand anderes Ihr Passwort für missbräuchliche Zwecke einsetzt, sind Sie verantwortlich!

Geben Sie Passwörter nicht weiter, auch nicht am Telefon, auch nicht, wenn der oder die Anrufer*in überzeugende Gründe aufführt, weshalb Ihr Passwort gerade jetzt benötigt wird.

Wenn Sie ein Passwort aufschreiben wollen, verwahren Sie die Abschrift an einem Ort, an dem Sie auch andere wertvolle Dinge aufbewahren, die Sie vor dem Zugriff anderer schützen wollen.

Achten Sie bei der Nutzung von Passwörtern im Internet darauf, dass die Verbindung verschlüsselt ist, bevor Sie ein Passwort eingeben. Die verschlüsselte Verbindung erkennen Sie daran, dass die Internet-Adresse nicht mit „http://“, sondern mit „https://“ beginnt. Falls sie mit „http://“ beginnt, fügen Sie einfach ein „s“ hinter „http“ in die Adresse ein und laden die Seite dann neu. Dies funktioniert in den meisten Fällen. Ihr Browser gibt Ihnen zusätzlich entsprechende Hinweise.

Achtung: In einigen Browsern wird eventuell kein Hinweis auf eine „https://“ Verbindung gegeben. Gegebenenfalls wird eine sichere Verbindung durch entsprechende Symbole in der Adressleiste des Browsers angezeigt.

Melden Sie sich von personalisierten Webseiten immer ab. Ansonsten erleichtern Sie es einem Angreifenden, Ihre Sitzung zu übernehmen.

Das Surfen auf gesicherten Seiten wird generell empfohlen.

3. Nutzen Sie Ihr Hochschul-Passwort niemals bei Dritten im Internet!

Nutzen Sie generell verschiedene Passwörter für verschiedene Einsatzzwecke. Personalisierte Anwendungen im Internet (z.B. Auktionen, Shops, etc.) erfordern eine Anmeldung mit Kennung und Passwort. Kennung und Passwort sind auf dem Server der Internet-Firma (ggf. verschlüsselt) gespeichert. Daher können Sie davon ausgehen, dass die Internet-Firma Ihre Kennung und Ihr Passwort kennt. Oft genug speichern Internet-Firmen Kunden-Passwörter im Klartext. Des Weiteren hängt die Vertraulichkeit Ihres Passworts davon ab, wie gut die Internet-Firma ihre Server (auf denen die Passwörter gespeichert sind) schützt. Oft genug gibt es Einbrüche in Firmen-Server, nach denen Kennungen und Passwörter im Internet veröffentlicht werden.

Aus diesem Grund ist es verboten, dass Sie Ihr Hochschul-Passwort für Internet-Anwendungen Dritter verwenden.

Generell empfiehlt es sich, für unterschiedliche Einsatzzwecke verschiedene Passwörter (und am besten auch verschiedene Kennungen) zu verwenden. Ansonsten können die Betreibenden einer Internet-Anwendung unter falschem Namen ggf. andere Internet-Anwendungen nutzen.

Achten Sie dabei darauf, dass aus dem einen Passwort nicht ein anderes in einfacher Weise ableitbar ist. (z.B. Dkei2Jebay / Dkei3Jamazon / Dkei4Jhsos)

4. Wechseln Sie ihr Passwort bei Verdacht auf Missbrauch!

Wenn die Gefahr besteht oder Sie den Verdacht haben, dass jemand anderes Ihr Passwort kennen könnte, dann wechseln Sie Ihr Passwort umgehend!

Dies ist z.B. dann der Fall, wenn Sie vermuten, dass jemand anderes unter Ihrer Zugangskennung arbeitet (veränderte Daten, Login-Zeiten) oder wenn Sie ein mobiles Gerät (z.B. Smartphone) verloren haben, auf dem Ihr Passwort gespeichert ist.

5. Ändern Sie Default-Passwörter von IT-Geräten!

Einem Angreifenden wird der unbefugte Netzzugriff auf ein IT-Gerät besonders einfach gemacht, wenn entweder kein Zugangsschutz aktiviert ist oder vom Hersteller eingerichtete Standard-Passwörter nicht geändert werden. Richten Sie daher auf allen Geräten einen sicheren Zugangsschutz ein!

3.3. Datenhaltung und -bereitstellung

Die Hochschule möchte fremde Zugriffe auf hochschulinterne Daten verhindern. Daher sind dienstliche Daten generell auf den hierfür vorgesehenen zentral bereitgestellten Systemen (z.B. OSCA, Netzlaufwerke, etc.) zu speichern. Im Vergleich zur lokalen Speicherung der Daten auf Endgeräten hat dies zudem den Vorteil, dass die Daten einer geregelten Sicherung und Archivierung unterliegen. Lokale Daten sind weitestgehend zu vermeiden.

Folgende Regelungen sind zu beachten:

1. Zentrale Datenhaltung

Speichern Sie Ihre dienstlichen Hochschuldaten in den zentral dafür zur Verfügung gestellten Bereichen:

- Netcase: eigene Daten und geteilte Daten,
- OSCA-Lernräume und Teamräume,
- eingerichtete Netzlaufwerke.

2. Bereitstellung von Daten für definierte Benutzergruppen

Sollen Daten für eine Gruppe bereitgestellt werden, bieten sich hierzu verschiedene Möglichkeiten, bei denen sowohl die Bereitstellung (Upload) als auch der Abruf (Download) geschützt sind:

- Abteilung/Bereich: ein zugehöriges Netzlaufwerk
- Studierendengruppe: Bereitstellung im OSCA Lernraum
- Feste Empfänger-/Arbeitsgruppe: Einrichtung eines OSCA Teamraums
- Flexible, selbst gewählte Gruppe: Nutzung von Netcase

E-Mails sollten nur als Kommunikationsmittel verwendet werden. Die Bereitstellung von Daten durch den Versand per E-Mail an eine Empfängergruppe hat den Nachteil, dass die versendeten Daten unverschlüsselt in jedem Postfach liegen. Das Risiko der Offenlegung versendeter Daten vervielfacht sich hierdurch.

3. Keine Nutzung von Cloud-Diensten oder Server Dritter zur Speicherung dienstlicher oder personenbezogener Daten der Hochschule!

Netcase ist der zentrale Cloud-Dienst der Hochschule Osnabrück. Da Hochschuldaten innerhalb der Hochschule verbleiben sollen, ist eine Speicherung dieser auf Servern Dritter grundsätzlich unzulässig. Ausnahmen hiervon erfordern eine schriftliche vertragliche Vereinbarung zwischen der Hochschule und dem oder der Dritten.

Im Fall der Speicherung personenbezogener Daten auf Cloud-Servern Dritter liegt i.d.R. eine Auftragsverarbeitung im Sinne des Datenschutzes vor. Die zugehörigen gesetzlichen Vorgaben sind zu beachten.

4. Speichern Sie sensible oder personenbezogene Daten auf Endgeräten verschlüsselt!

Einen guten Schutz sensibler oder personenbezogener Daten auf Endgeräten bieten funktions- / projektspezifische verschlüsselte Container (verschlüsselte Ordner). Die Container werden nur dann entriegelt / entschlüsselt, wenn die Daten benötigt werden. Z. B.:

- Container für Noten (Klausurergebnisse, etc.)
- Container für Forschungsprojekte
- Container für Pseudonym-Zuordnungs-Listen
- Container für sensible Daten einer Berufungskommission

Hierdurch kann den Datenschutz-Vorgaben der Zweckbindung und der getrennten Verarbeitung genüge getan werden. Bei der Einrichtung der Container unterstützt Sie der ServiceDesk.

Hinweis: Die Basisverschlüsselung (Verschlüsselung des gesamten Speichers) mobiler Endgeräte bietet keinen Schutz vor Datenklau während des Arbeitens mit dem Gerät: Beim Arbeiten ist die Basisverschlüsselung entriegelt und jegliche Software - auch Schadsoftware - hat Zugriff auf die Daten.

3.4. Anbieten von Serverdiensten außerhalb des ITSC

Das ITSC stellt gut gesicherte Serverzentren bereit, in denen verschiedenste Dienste sicher betrieben werden können. Es besteht die Möglichkeit eines Serverhostings im ITSC.

Es gibt innerhalb der Hochschule verschiedene Netzbereiche. Standardmäßig werden Geräte (Clients und Server) so eingerichtet und betrieben, dass ein Zugriff aus dem Internet nicht möglich ist.

Sollten Sie spezifische Dienste im Internet anbieten wollen, ist dies gesondert zu beantragen und mit dem ITSC abzustimmen. Ein Betreiben von Diensten im Internet ohne Absprache bzw. Anmeldung ist untersagt. Systeme, die Dienste im Internet anbieten sind besonders anfällig für Angriffe und bedürfen besonderer Sorgfalt und Wartung.

Nach Möglichkeit sind eigene Internetdienste (z.B. in Forschungsprojekten oder Laborserver) im Serverzentrum und unter der Aufsicht des ITSC zu betreiben.

Hinweis: Dem ITSC muss Zugang zu den dort gehosteten Systemen gewährt werden (Administratorkennung), um in kritischen Situationen die Geräte administrieren zu können. So wird der reibungslose Betrieb der anderen (hochschulweiten) Dienste sichergestellt.

3.5. Internet und E-Mail Nutzung

Fehlende Grenzen und die geschäftliche Nutzung machen das Internet attraktiv für Personen, die versuchen, Systeme mit Schadsoftware zu infizieren und für kriminelle Zwecke zu nutzen. Die Gefährdungen reichen vom Abhören privater Informationen und Passwörtern (Datenklau, Identitätsdiebstahl) bis zur Internet-Blockade ganzer Unternehmen oder Organisationen.

Zum Schutz der Daten der Hochschule Osnabrück sind daher folgende Regelungen bei der E-Mail-Nutzung und dem „Surfen“ im Internet zu beachten:

1. Die Übertragung sensibler Informationen ist nur in verschlüsselter Form zulässig!

Innerhalb der Hochschule, d.h. zwischen Adressen der Form @hs-osnabrueck.de, werden E-Mails verschlüsselt übertragen, jedoch unverschlüsselt in den Postfächern gespeichert. Zudem sind E-Mails leicht fälschbar.

E-Mails sollen möglichst nur als Kommunikationsmittel verwendet werden. Zur Datenbereitstellung sind die weiter oben angegebenen Wege zu bevorzugen.

Durch eine Weiterleitung von E-Mails, z.B. an private E-Mail-Accounts, verlassen die Daten den Bereich der Hochschule. Die automatische Weiterleitung dienstlicher E-Mails an Mail-Accounts außerhalb der Hochschule ist daher generell verboten. Sensible und personenbezogene Daten dürfen ausschließlich zwischen Hochschul-E-Mail-Adressen ausgetauscht werden. Auch in diesem Fall sind eine rechtliche Grundlage und ein legitimer Zweck erforderlich. Es besteht zudem die Möglichkeit der Einrichtung eines E-Mail-Zertifikates zur (automatischen) Signierung und Verschlüsselung von E-Mails. Diese liegen dann auch nicht mehr unverschlüsselt im Postfach des Empfängers, sondern sind entsprechend geschützt. Wenden Sie sich bei Bedarf oder Fragen an den ServiceDesk.

2. Kein Öffnen von E-Mail-Anhängen ohne vorhergehende Plausibilitätsprüfung!

E-Mails sind einer der häufigsten Übertragungswege von Schadsoftware. Daneben können E-Mail-Inhalte und -Absender sehr leicht gefälscht werden. Begegnen Sie deshalb empfangenen E-Mails immer mit gesundem Misstrauen. Prüfen Sie, z.B. anhand der Formulierung, ob es plausibel ist, dass die E-Mail tatsächlich vom angegebenen Absender stammt. Bei Unsicherheiten fragen Sie den ServiceDesk um Rat.

Ganz besondere Vorsicht gilt bei ausführbaren Anhängen. Diese sollten Sie grundsätzlich NICHT öffnen, sondern direkt löschen. Öffnen Sie ausführbare Anhänge nur, nachdem Sie sich zuvor explizit – z.B. durch einen Anruf beim Absender – von deren Vertrauenswürdigkeit überzeugt haben. Eine gültige elektronische Signatur kann auch als vertrauenswürdig angesehen werden. Auch E-Mails von Kolleg*innen können gefälscht sein.

3. Kein Versand ausführbarer Anhänge per E-Mail!

Aufgrund ihrer Gefährlichkeit werden E-Mails mit ausführbaren Anhängen (z.B. *.exe) von vielen Unternehmen direkt gefiltert. Sie erreichen ihren Adressaten erst gar nicht. Falls die E-Mail ihren Adressaten erreicht, sollte dieser sie nicht ungeprüft öffnen.

Verzichten Sie daher auf den Versand ausführbarer Anhänge.

4. Misstrauen Sie Internet-Links in E-Mails

Links in E-Mails werden häufig genutzt, um den oder die Empfänger*in auf nicht vertrauenswürdige Web-Seiten zu führen. Bekanntestes Beispiel ist das Phishing, bei dem man über einen Link auf eine Seite gelangt, die zwar optisch der Originalseite gleicht, sich jedoch auf dem Webserver eines Internet-Kriminellen befindet.

Bereits das Klicken auf den Link in der E-Mail kann ausreichen, um Ihren Rechner mit Schadsoftware zu verseuchen und für den Angreifenden zugänglich zu machen.

Genau wie bei den Anhängen, sollten Sie auch E-Mail-Links nur betätigen, nachdem Sie sich von der Vertrauenswürdigkeit der E-Mail überzeugt haben.

5. Automatisches Nachladen von Inhalten aus dem Internet deaktivieren!

In E-Mails können Links eingebettet sein, die automatisch Daten aus dem Internet nachladen. Bei der HTML-Anzeige einer solchen E-Mail, werden automatisch z.B. Bilder aus dem Internet geladen und mit der E-Mail angezeigt. Diese Funktion ist höchst sicherheitskritisch, da z.B. auch Schadsoftware von nicht integren Servern automatisch ausgeführt werden könnte. In diesem Fall reicht die HTML-Anzeige der E-Mail, um Ihren Rechner zu verseuchen und für den Angreifenden zugänglich zu machen.

Konfigurieren Sie Ihr E-Mail-Programm daher so, dass bei der Anzeige von E-Mails Inhalte aus dem Internet nicht automatisch nachgeladen werden. Der ServiceDesk unterstützt Sie hierbei.

Als weitere Vorsichtmaßnahmen können Sie das Vorschaufenster abschalten, damit E-Mails nicht automatisch geöffnet und angezeigt werden, oder die E-Mail Ansicht auf „Nur Text“ umschalten.

6. Vorsicht beim Download von Software aus dem Internet

Im Internet bereitgestellte Ressourcen, sowohl Software als auch andere Informationen, sind oft nicht vertrauenswürdig. Ihr Einsatz kann schädliche Folgen für die IT und die Hochschule nach sich ziehen.

Falls Sie Software aus dem Internet nutzen wollen, stimmen Sie dies zuvor mit dem ServiceDesk ab, damit die Hochschule einen Überblick über die in der Hochschule eingesetzte Software behält. Des Weiteren kann Ihnen der ServiceDesk bei der Prüfung der Vertrauenswürdigkeit der Quelle helfen.

Lizenzpflichtige Software ist über die definierten Beschaffungsprozesse der Hochschule einzukaufen.

Im Rahmen von Forschungs- und Lehraktivitäten darf Software ohne Einschränkungen und ohne vorherige Abstimmung verwendet werden. Die gesetzlichen Anforderungen sind einzuhalten.

7. Vorsicht beim Surfen im Internet!

Im Internet gibt es zahlreiche Gefahren: Falls Ihre Systemsoftware nicht auf dem neuesten Stand ist, kann bereits der Aufruf von Seiten zu einer Infektion Ihres Rechners führen, die Ihr Virenscanner ggf. nicht erkennt (sog. Drive-by-Downloads). Dies betrifft auch viele Seiten vertrauenswürdiger Anbieter, z. B. aufgrund von manipulierter Werbung. Surfen Sie daher nur auf vertrauenswürdigen Seiten.

Beispiele:

- Manipulierte Bilder können bekannte Sicherheitslücken ausnutzen und so dem Rechner oder der Hochschule schaden
- In vielen Seiten ist zur Steigerung der Funktionalität Software eingebettet, die beim Laden der Seite ausgeführt wird (Java, JavaScript, ActiveX). Diese kann Sicherheitslücken haben und missbräuchlich verwendet werden

Ein jeder kann im Internet Inhalte bereitstellen, anonym und unzensiert. Begegnen Sie daher Informationen mit gesundem Misstrauen.

8. Beachten Sie Warnungen Ihres Browsers!

Aktuelle Browser erkennen bereits teilweise selbständig unsichere Webseiten und warnen den Nutzenden. Klicken Sie entsprechende Warnungen nicht einfach weg. Wenn Sie eine Warnung nicht verstehen, wenden Sie sich zur Klärung bitte an den ServiceDesk.

3.6. Einsatz mobiler Endgeräte / Einsatz privater Endgeräte

Bei mobilen Geräten, insbesondere Smartphones und Tablets, bestehen erhöhte Sicherheitsrisiken. Sensible oder personenbezogene Hochschul-Daten sollten grundsätzlich nicht auf Smartphones und/oder privaten Rechnern gespeichert werden. Generell ist bei privaten Geräten sicherzustellen, dass keine Dritten (z.B. Familienmitglieder) Zugang zu dienstlichen Daten haben.

Folgende Regelungen und Empfehlungen sind zu beachten:

1. Für mobile Endgeräte (Laptops, Smartphones, Tablets, etc.) ist – unabhängig davon, ob es sich um ein privates oder dienstliches Gerät handelt – eine Verschlüsselung des gesamten Speichers Pflicht!

Regemäßig werden Laptops gestohlen und Smartphones geklaut. Auch bei uns an der Hochschule.

Damit Dritte in solchen Fällen nicht auf Daten der Hochschule zugreifen können, ist eine sogenannte Basisverschlüsselung grundsätzlich verpflichtend einzusetzen.

Die Verschlüsselung ist i.d.R. durch ein Passwort geschützt. Die Sicherheit der Verschlüsselung hängt damit direkt vom gewählten Passwort ab. Der ServiceDesk kann Sie bei der Einrichtung unterstützen.

2. Die lokale Datenspeicherung sensibler und personenbezogener Daten ist auf Smartphones, Tablets und artverwandten Geräten der Hochschule zu vermeiden! Für private Geräte mit dienstlicher Nutzung gelten besondere Vorschriften.

Grundsätzlich empfiehlt es sich, so wenig dienstliche Daten wie möglich auf Smartphones, Tablets oder artverwandten Geräten zu speichern. Die Hochschule unterstützt dies durch folgende Maßnahmen:

- Auf IT-Systeme der Hochschule ist soweit verfügbar über Terminal-Dienste (z.B. Fernzugriff auf einen Computer) oder weitergehende virtuelle Umgebungen zuzugreifen. Dabei werden die Daten nicht lokal auf den Endgeräten gespeichert.
- Auf Ihr E-Mail-Postfach und Ihren Kalender haben Sie über die Outlook Web App (https://msx.hs-osnabrueck.de) Zugriff. So können Sie Outlook nutzen, ohne Daten lokal zu speichern.
- In OSCA und Netcase können Sie über im Browser eingebettete Web-Apps pdf- und Office-Dokumente lesen, ohne eine lokale Kopie der Daten zu speichern. Hier ist auch eine Bearbeitung der Dokumente möglich.

Sofern sensible oder personenbezogene Daten auf diesen Geräten erforderlich sind und dort gespeichert bzw. verarbeitet werden gelten nachfolgende Regelungen:

- Alle Hinweise und Regelungen dieser Richtlinie sind zu prüfen und in Ihrer Funktion sicherzustellen. Besonders bei Verwendung privater Geräte.
- Der Abruf von E-Mails muss über Exchange ActiveSync (ein E-Mail-Protokoll mit vielen Komfortfunktionen) eingerichtet werden. Damit wird die Hochschule automatisch als

Geräteadministrator in die Lage versetzt, alle Daten (auch private Daten!) des Telefons zu löschen und sicherheitsrelevante Einstellungen zu tätigen. Dies darf durch den Nutzenden nicht geändert oder umgangen werden. Beachten Sie insbesondere bei der Nutzung von privaten Geräten, dass Sie für die Sicherung Ihrer privaten Daten verantwortlich sind und diese auch im Rahmen der Schadensminimierung durch die Hochschule vollständig gelöscht werden können.

- Speichern Sie Ihre Daten soweit wie möglich nur in den dafür vorgesehenen, hochschulweiten Systemen.
- Bei Verlust – auch von privaten Geräten – ist der ServiceDesk zu verständigen
- Empfehlung: Nutzen Sie auf den Geräten eine Sicherheitssoftware zur schnellstmöglichen Erkennung von Schadsoftware. Eine geeignete Software kann Ihnen der ServiceDesk empfehlen.
- Empfehlung: Richten Sie wenn möglich ein weiteres Benutzerkonto auf den Geräten ein. Damit haben Sie eine explizite Trennung von privat und beruflich erreicht.
- **Tipp**: Durch die Einrichtung von Exchange ActiveSync auf Ihrem Gerät, werden die wichtigsten der nachfolgenden Vorgaben automatisch umgesetzt, so dass Sie sich damit nicht mehr auseinandersetzen müssen.

3. Nutzung privater Geräte auf eigene Verantwortung und eigenes Risiko!

Wenn Sie dienstliche Daten auf privaten Endgeräten speichern, sind Sie selbst für einen angemessenen Schutz dieser Daten verantwortlich. Schützen Sie daher diese privaten Endgeräte gemäß den Regelungen dieser Richtlinie.

Stellen Sie sicher, dass keine Dritten Zugriff auf die Daten haben. Hierzu können Sie z.B. ein verschlüsseltes Laufwerk anlegen, auf das nur Sie persönlich Zugriff haben. Dies gilt auch bei der Verwendung der Geräte durch z.B. Familienmitglieder.

Wenn Sie dienstliche Daten auf Smartphones speichern/verarbeiten oder mit dem Smartphone auf Ihre E-Mails zugreifen, sind folgende Maßnahmen zu berücksichtigen:

4. Passwort / PIN als Zugangsschutz für das Smartphone verwenden!

Nicht jeder, der Ihr Smartphone findet, soll es auch direkt nutzen können. Wischmuster bieten lediglich eine sehr begrenzte Sicherheit und sind daher unzureichend.

5. Deaktivieren oder Umgehen sie nicht systemeigene Sicherheitsmaßnahmen

Dies kann dazu führen, dass Apps unbefugt auf Daten zugreifen und diese versenden.

6. Nutzung mobiler Endgeräte im Ausland

In den meisten Ländern sind das Datenschutzniveau und die Datensicherheit nicht so hoch wie innerhalb der EU. Aus diesem Grund ist bei Auslandsaufenthalten besondere Vorsicht geboten. Die Hochschule orientiert sich in diesem Bereich an den Vorgaben und Empfehlungen der EU.

Je nachdem, welches Land bereist werden soll, sind unterschiedliche Maßnahmen zu treffen, um die Sicherheit der Daten und den Schutz von personenbezogenen Daten zu gewährleisten:

- Innerhalb der EU sind keine weiteren Maßnahmen notwendig. Sie müssen sich an die Vorgaben dieser Richtlinie halten.
- Bei Reisen in sogenannte sichere Drittländer ist das Datenschutzniveau sehr ähnlich zu dem der EU. Es gelten die Regelungen dieser Richtlinie. Begrenzen Sie den Umfang der Daten auf ein absolutes Minimum. Im Zweifelsfall können Daten nachträglich synchronisiert werden. Eine aktuelle Liste der aktuell als sicher geltenden Drittstaaten finden Sie unter https://ec.europa.eu/info/law/law-topic/data-protection_en.
- Bei Reisen in Länder mit Kooperationen der Hochschule (z.B. China) wird zwischen sporadischen (z.B. eine Konferenz) und regelmäßigen Aufenthalten (z.B. im Rahmen einer Lehrtätigkeit) unterschieden. Bei Bedarf von regelmäßigen Reisen in diese Länder wenden Sie sich vor Reiseantritt an den ServiceDesk. Sie erhalten ein Gerät mit besonderen Sicherheitsmechanismen und zusätzliche Informationen. Gegebenenfalls kann Ihr derzeit verwendetes Gerät entsprechend konfiguriert werden. Die Daten auf dem Gerät sind auf ein sinnvolles Maß zu beschränken. Bei sporadischen Besuchen dieser Länder erhalten Sie ein Ersatzgerät über den ServiceDesk. Die Daten auf diesen Geräten sind auf den minimal notwendigen Umfang zu beschränken. Die gespeicherten Daten der Geräte werden nach Wiederkehr gelöscht.
- Bei Reisen in andere Länder, dürfen hochschuleigene Geräte und private Geräte mit dienstlichen Daten nicht verwendet werden. Bei Bedarf besteht die Möglichkeit eines Erlaubnisvorbehalts. Wenden Sie sich hierzu an den ServiceDesk.

Für den Verlustfall gelten nachfolgende Regelungen. Dabei ist es unerheblich, ob Sie ein Smartphone, Tablet oder einen anderen mobilen Rechner verloren haben oder ein Diebstahl vorliegt.

7. Ändern Sie umgehend Ihr Hochschul-Passwort!

Wenn Sie das mobile Endgerät für dienstliche Zwecke verwenden, ist das Passwort Ihrer zentralen Hochschul-Kennung in der Regel auf dem Gerät gespeichert. Dies ist z.B. der Fall, wenn Sie mit dem Gerät auf Ihre E-Mails zugreifen.

8. Melden Sie den Verlust bzw. Diebstahl!

Melden Sie den Verlust/Diebstahl insbesondere hochschuleigener Geräte umgehend dem ServiceDesk. Ansonsten hat die Hochschule keine Möglichkeit, eine Erstattung des Schadens zu beantragen.

Sollten auf dem Gerät personenbezogene oder sensible Daten der Hochschule unverschlüsselt gespeichert gewesen sein, ist dies umgehend zu melden!

9. Aktivieren Sie die Fernlöschung!

Wenn das mobile Gerät über Exchange ActiveSync verbunden ist, kann eine Fernlöschung direkt über https://msx.hs-osnabrueck.de erfolgen. Bitte wenden Sie sich bei Fragen an den ServiceDesk.

3.7. Datenträger und papiergebundenen Daten

Datenträger und Papierdokumente gehen schnell verloren und vervielfältigen in den meisten Fällen den Zugriff auf sensible, geheime oder personenbezogene Daten.

Nachfolgende Regelungen betreffen sowohl papiergebundene Informationen als auch Datenträger (z. B. CD, USB-Stick):

1. Zugriffsschutz für dienstliche Dokumente oder sensible und/oder personenbezogene Dokumente und Datenträger mit entsprechenden Daten

Datenträger und papiergebundene dienstliche Daten sind angemessen gegen den Zugriff durch Unbefugte zu schützen. Beispiele wären ein verschlossener Schrank für Dokumente oder eine Verschlüsselung des gesamten Speichers / einzelner Dateien bei mobilen Datenträgern.

2. Drucken von sensiblen und/oder personenbezogenen Daten

Falls Sie sensible Daten auf Netzwerkdruckern in anderen Räumen oder nicht zutrittsgeschützten Bereichen (z. B. Flur) ausdrucken, verwenden Sie nach Möglichkeit die passwortgeschützte Drucker-Mailbox. Den eigentlichen Ausdruck führen Sie erst dann durch, wenn Sie am Drucker stehen.

Lassen Sie gedruckte sensible oder personenbezogene Daten nicht unbeaufsichtigt liegen. Nehmen Sie Ausdrucke unverzüglich aus dem Ausgabefach.

3. Versand sensibler und/oder personenbezogener papiergebundener Daten

Sensible und personenbezogene papiergebundene Daten sind in verschlossenen Behältnissen (z.B. Umschlägen) zu versenden. Dies betrifft den Postversand wie auch den Versand in der Hauspost.

4. Archivierung sensibler und/oder personenbezogener papiergebundener Daten

Für die Archivierung sensibler und/oder personenbezogener papiergebundener Daten sind die durch die Hochschule angebotenen Archivierungsdienste zu nutzen.

5. Ausmusterung und Vernichtung sensibler Daten

Entsorgen Sie sensible und personenbezogene Dokumente nicht über Ihren Papierkorb im Büro! Die Hochschule hat entsprechende Entsorgungstonnen aufgestellt, über die papiergebundene, dienstliche Daten einer geregelten, vorgabenkonformen Entsorgung zugeführt werden.

Sensible und/oder personenbezogene Daten auf Datenträgern sind nachdem der Zweck erfüllt ist zeitnah sicher zu löschen. Der ServiceDesk nimmt Datenträger (Festplatten, CDs, USB-Sticks, etc.) entgegen und kümmert sich um die sichere Entsorgung von Datenträgern und IT-Geräten.

4. Datenschutz

Beim Datenschutz geht es um den Schutz personenbezogener Daten, um das Recht auf informationelle Selbstbestimmung zu gewährleisten. Jede Person soll selbst über die Preisgabe und Verwendung ihrer Daten bestimmen können.

Die Hochschule verarbeitet eine Vielzahl personenbezogener Daten, wie insbesondere Studierenden- und Mitarbeitenden-Daten, aber auch teils medizinische Daten Dritter im Rahmen von Forschungsprojekten. Diese Daten sind gemäß den Vorgaben des Niedersächsischen Datenschutzgesetztes (NDSG), des Bundesdatenschutzgesetzes (BDSG) und der Europäischen Datenschutzgrundverordnung (EU-DSGVO) zu schützen.

Die nachstehenden Regeln geben wichtige gesetzliche Vorgaben / Grundsätze des Datenschutzes wieder. Die Hochschule ist hinsichtlich der Einhaltung der Datenschutzgrundsätze (EU-DSGVO Art. 1) rechenschaftspflichtig. Achten Sie stets auf eine gute Transparenz beim Umgang mit personenbezogenen Daten.

Folgende Grundsätze des Datenschutzes sind einzuhalten:

1. Personenbezogene Daten nur für Hochschulzwecke erheben

Personenbezogene Daten dürfen erhoben werden, wenn ihre Kenntnis zur Erfüllung der Aufgaben der Hochschule erforderlich ist (Grundsatz der Rechtmäßigkeit). Die Daten sind grundsätzlich bei dem oder der Betroffenen (Person, von der die Daten stammen) zu erheben.

2. Personenbezogene Daten nur zum vorgegebenen Zweck einsetzen!

Personenbezogene Daten unterliegen dem Grundsatz der Zweckbindung. Sie dürfen nur zu dem Zweck verwendet werden, zu dem sie erhoben wurden. Eine Änderung des Verwendungszwecks bedarf der Zustimmung der betroffenen Personen oder einer klaren rechtlichen Grundlage.

3. Personenbezogene Daten nur im erforderlichen Umfang erheben!

Es gilt der Grundsatz der Datenminimierung: Personenbezogene Daten sind am besten geschützt, wenn sie erst gar nicht gespeichert werden.

Personenbezogene Daten sollen nur erhoben werden, wenn dies auch notwendig ist. Dann nur die minimal zur Erfüllung des Zwecks erforderlichen Daten erheben. Der Grundsatz der Datensparsamkeit verlangt auch die Löschung personenbezogener Daten, sobald diese nicht mehr benötigt werden. Aufgrund zahlreicher bekannter Datenschutzvorfälle und der starken Vernetzung ist Datensparsamkeit besonders wichtig.

4. Informationspflicht bei der Datenerhebung

EU-DSGVO Art 13. und 14 legen fest, worüber der oder die Betroffene bei der Erhebung zu informieren ist.

Der oder die Betroffene ist bei der Erhebung insbesondere untern anderem über nachfolgende Dinge zu informieren:

- Verarbeitungszweck und Rechtsgrundlage der Verarbeitung
- Speicherdauer oder Kriterien für die Festlegung der Dauer
- Rechte des oder der Betroffenen auf Auskunft, Berichtigung, Widerspruch und Datenübertragbarkeit
- Beschwerderecht bei der Aufsichtsbehörde
- Ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben ist und welche Folgen die Nichtbereitstellung hat.

Für eine vollständige, fallbezogene Aufzählung zur Informationspflicht siehe EU-DSGVO Art. 13 und 14.

5. Gehen Sie mit personenbezogenen Daten vertraulich um!

Mitarbeitende öffentlicher Stellen und ihre Auftragnehmer*innen sind auf das Datengeheimnis verpflichtet, d.h. zum vertraulichen Umgang mit personenbezogenen Daten. Diese Verpflichtung gilt nach Beendigung der Tätigkeit weiter.

6. Anonymisierung der Daten

Daten sollen so gespeichert werden, dass eine Identifizierung der zu den Daten gehörenden Person nur solange, wie für den Zweck benötigt, möglich ist (Speicherbegrenzung). Entsprechend sind personenbezogene Daten zu anonymisieren, wenn der Personenbezug nicht länger benötigt wird.

7. Dokumentationspflicht, Verzeichnis von Verarbeitungstätigkeiten

Die Hochschule ist hinsichtlich der Verarbeitung personenbezogener Daten gegenüber der Aufsichtsbehörde rechenschaftspflichtig (EU-DSGVO Art. 5). Entsprechend schreibt der Gesetzgeber vor, dass Verfahren, in denen personenbezogene Daten verarbeitet werden, zu dokumentieren sind (EU-DSGVO Art. 30).

Die Dokumentation hat u.a. die Verfahrensbezeichnung, die Art der gespeicherten Daten, den Verarbeitungszweck, die Rechtsgrundlage für die Verarbeitung, den Betroffenenkreis, Sperr- und Löschfristen sowie die getroffenen Schutzmaßnahmen zu umfassen.

Eine Dokumentationsvorlage für Verfahrensbeschreibungen finden Sie im Prozessportal.

Zuständig für die Beschreibung der Verfahren sind die jeweiligen Bereiche. Das Verzeichnis von Verarbeitungstätigkeiten ist durch die Hochschule zu führen. Senden Sie die ausgefüllten Dokumente an datenschutz@hs-osnabrueck.de. Unter dieser Adresse erhalten Sie auch Unterstützung in allen anderen Datenschutz- und IT-Sicherheitsfragen.

8. Sicherstellung von Verfügbarkeit, Vertraulichkeit und Integrität

Unter Berücksichtigung des Stands der Technik sind dem jeweiligen Risiko angemessene technische und organisatorische Maßnahmen zu treffen, die geeignet sind,

- unbefugten Zugriff auf personenbezogene Daten,
- ungewollte Änderung oder Manipulation personenbezogener Daten
- sowie ungewollten Verlust von personenbezogenen Daten

zu verhindern. Dabei ist durch datenschutzfreundliche Voreinstellungen sicherzustellen, dass nur die erforderlichen Daten im notwendigen Umfang verarbeitet werden. Diese Verpflichtung gilt auch für die Speicherfrist und Zugänglichkeit.

Die Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung ist regelmäßig zu prüfen und zu bewerten (EU-DSGVO Art.25/32).

Hochschulweit gültige Maßnahmen werden durch diese Richtlinie vorgegeben.

9. Auftragsverarbeitung

Eine Auftragsverarbeitung liegt vor, wenn die Hochschule personenbezogene Daten an Dritte zur Verarbeitung weitergibt. Ein Beispiel ist die Weitergabe von Studierendendaten zum Druck von Abschlusszeugnissen.

Eine Auftragsverarbeitung ist nur unter bestimmten Bedingungen zulässig und bedarf in jedem Fall eines geeigneten Vertrags mit dem Dritten. Auftragsverarbeitungen sind daher mit der Hochschulverwaltung abzustimmen. Wenden Sie sich bei Fragen an datenschutz@hs-osnabrueck.de.

5. Vorgaben für Daten hohen Schutzbedarfs

In manchen Fällen werden an der Hochschule Daten verarbeitet, deren Offenlegung oder Manipulation einen deutlichen Schaden für die Hochschule oder Betroffener zur Folge haben könnte.

Hinsichtlich gesetzlicher Datenschutzvorgaben ist ein entsprechend hoher Schutzbedarf in folgenden Fällen gegeben:

- besondere Arten personenbezogene Daten gemäß EU-DSGVO, Art. 9 (1): rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.
- Ansammlungen anzahlmäßig großer Mengen personenbezogener Daten, z.B.
  - Liste privater E-Mail-Adressen der Studierenden einer Fakultät oder
  - die CampusNet-Datenbank mit Studierendennoten.
- Daten von Forschungsprojekten z.B. in den Bereichen Pflege oder Medizin (z.B. Interview- oder Videoaufzeichnungen von Probanden).
- besondere bewertende personenbezogene Daten, wie z.B. Personalbeurteilungen oder -gutachten.
- Daten einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche,
- ggf. Daten von Forschungsprojekten, in denen strenge Geheimhaltungsvereinbarungen mit Dritten abgeschlossen wurden.

Für die Verarbeitung solcher Daten sind folgende Regelungen zu beachten:

1. Informierung und Aufklärung der beteiligten Mitarbeiter

Die Leitenden des Projektes bzw. Vorgesetzten haben die betroffenen Mitarbeitenden darauf hinzuweisen, dass es sich um sensible, schutzbedürftige Daten handelt, bei deren Verarbeitung (von

der Erhebung, der Speicherung bis hin zur Löschung) besondere Maßnahmen einzuhalten sind. Die Mitarbeitenden sind über die einzuhaltenden Maßnahmen aufzuklären.

2. Datenschutz-Folgenabschätzung vor Verarbeitungsbeginn

Bevor eine Verarbeitung von höchst schutzbedürftigen personenbezogenen Daten erfolgt, deren Offenlegung oder Manipulation einen deutlichen Schaden für die Betroffenen zur Folge haben könnte, ist eine Datenschutz-Folgeabschätzung gesetzlich (EU-DSGVO, Art. 35) vorgeschrieben.

Hierzu bedarf es einer

- genauen Beschreibung des Verarbeitungsverfahrens der Daten inklusive des Managements von Zugriffsberechtigungen,
- einer Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung hinsichtlich des Zwecks,
- einer Bewertung der Risiken für die Betroffenen sowie
- angemessener Maßnahmen zu Bewältigung der Risiken und
- Maßnahmen zum Nachweis, dass die Anforderungen der EU-DSGVO eingehalten werden.

Eine solche Folgenabschätzung ist zeitlich deutlich vor Arbeitsbeginn anzufertigen. Wenden Sie sich bei Fragen an datenschutz@hs-osnabrueck.de.

3. Kein Internet-Zugang

Ein Internet-Zugang zu diesen Daten ist grundsätzlich zu unterbinden. Falls ein Internet-Zugang eingerichtet wird, bedarf dies der detaillierten Begründung der Notwendigkeit unter Bewertung der damit verbundenen Risiken sowie der Dokumentation und Umsetzung geeigneter Sicherheitsmaßnahmen. Falls ein Internet-Zugang notwendig ist, bietet unter anderem eine 2-Faktor Authentifizierung einen geeigneten Zugangsschutz.

4. Berechtigungskonzept

Bei aggregierten Daten (z.B. CampusNet Datenbank) kann durch ein geeignetes Berechtigungsmanagement sichergestellt werden, dass nur auf eine begrenzte Menge der Daten zugegriffen werden kann. Das Berechtigungskonzept ist zu dokumentieren.

5. Grundsätzlich verschlüsselte Speicherung

Zur Speicherung solcher Daten auf Endgeräten, ist ein projektspezifischer verschlüsselter Container (verschlüsselter Ordner für das jeweilige Projekt) zu verwenden. Bei der Einrichtung unterstützt Sie der ServiceDesk.

Falls eine Verschlüsselung bei Endgeräten nicht möglich ist (z.B. Kameras), ist der Zugriff auf die Geräte, auf denen die Daten gespeichert sind, zu kontrollieren und zu protokollieren. Die Anbindung solcher der Geräte an das Hochschulnetz oder das Internet ist nicht zulässig. Die Daten sind umgehend auf andere Geräte zu übertragen und anschließend zu löschen.

6. Verwahrung papiergebundene Daten und Datenträger

Bei papiergebundenen Daten und Datenträgern ist eine besonders geschützte Verwahrung notwendig, die mehr Sicherheit bietet als die Verwahrung in einem abgeschlossenen Büroschrank. Nutzen Sie für die Entsorgung die bereitgestellten Container.

7. Grundsätzlich kein Versand per E-Mail!

Der Versand solcher Daten per E-Mail setzt eine sichere Ende-zu-Ende Verschlüsselung voraus. Diese ist im Regelfall nicht gegeben. Somit sollte auf den Versand solcher Daten verzichtet werden oder es muss die passende Infrastruktur eingerichtet werden.

6. Organisatorische Regelungen

Nachstehend werden für bestimmte Personengruppen der HS Osnabrück grundlegende Verantwortlichkeiten mit IT-Bezug aufgeführt.

6.1. Vorgesetzte

Vorgesetzte sind dafür verantwortlich, ihre Mitarbeitenden auf diese Richtlinie hinzuweisen und sie für Belange der IT-Sicherheit und des Datenschutzes zu sensibilisieren. Weisen Sie Ihre Mitarbeitenden auf die Erforderlichkeit der datenschutzrelevanten Dokumentation hin.

6.2. Administrator*innen

Administrator*innen sind für die IT-Sicherheit der von ihnen betreuten IT-Systeme verantwortlich. Umgesetzte Sicherheitsmaßnahmen sind zu dokumentieren. Für IT-Systeme, die personenbezogene Daten speichern/verarbeiten, ist eine Verfahrensbeschreibung zu erstellen.

6.3. Der/ Die Datenschutzbeauftragte

Die Aufgaben der/des Datenschutzbeauftragten sind in EU-DSGVO, Art. 39, festgelegt. Sie umfassen die

- Unterrichtung des Verantwortlichen und Beschäftigten hinsichtlich der aus den gesetzlichen Vorgaben resultierenden Pflichten und
- die Überwachung der Einhaltung der gesetzlichen Vorgaben.

6.4. Datenschutzmanagement

Die Hochschule verfügt über ein Datenschutzmanagement. Aufgabe ist dabei die Anforderungen des Datenschutzes in Einklang mit den Bedingungen des Betriebes zu bringen. Das Ziel ist die stetige Verbesserung der Prozesse innerhalb der Hochschule und im Kontakt mit Externen.

Das Datenschutzmanagement der Hochschule ist zu informieren

- bei der Einführung neuer Programme, die personenbezogene Daten verarbeiten,
- beim Austausch personenbezogener Daten mit Dritten,
- bei der Verarbeitung personenbezogener Daten durch Dritte,
- sowie Datenschutzvorfällen

6.5. Weitere organisatorische Regelungen

Es gelten nachfolgende grundsätzliche Regelungen:

1. Eigenverantwortlicher sicherer und datenschutzkonformer Umgang mit Informationen

Egal ob Studierende, Lehrende oder Mitarbeitende: Tragen Sie zu einem sicheren und datenschutzgerechten Umgang mit Informationen bei!

Informationssicherheit kann nur begrenzt „top down“ sichergestellt werden - trotz zentraler Konzepte und Analysen. Es hängt entscheidend davon ab, ob Sie mitmachen! Fallen Ihnen Schwachstellen, organisatorische Mängel, unklare oder schwierige Prozesse, Gefährdungen oder unangemessene Schutzmaßnahmen auf, dann teilen Sie es bitte durch eine Nachricht an datenschutz@hs-osnabrueck.de mit.

2. Meldung von Sicherheitsvorfällen

Es besteht die gesetzliche Verpflichtung, IT-Sicherheits- und Datenschutzvorfälle zentral zu erfassen. Schwerwiegende Fälle müssen zudem innerhalb von 72 Stunden von der Hochschule an die Datenschutz-Aufsichtsbehörde gemeldet werden. Die Bewertung, wie schwerwiegend ein Vorfall ist, wird zentral durchgeführt.

Sämtliche Datenschutz- und IT-Sicherheitsvorfälle sind daher umgehend dem ServiceDesk zu melden.

Beispiele:

- Verlust oder Diebstahl mobiler Geräte / Datenträger
- Befall mit Schadsoftware
- erkannte unbefugte Zugriffe

Der ServiceDesk leitet die Meldung umgehend an die zuständigen Stellen weiter.

3. Sperrung von Geräten mit schädlicher Netzaktivität

Immer wieder kommt es vor, dass Rechner oder IT-Geräte der Hochschule Angriffsaktivitäten aufweisen.

In diesem Fall wird der oder die Eigentümer*in des Gerätes informiert. Da Angriffsaktivitäten zu einem Schaden für die Hochschule führen können, wird zudem umgehend zentral der Netzzugang für das Gerät gesperrt. Eine Entsperrung erfolgt erst nach Behebung des Problems.

4. Nutzung von Dienstgeräten/ Administratorrechte

Dienstliche Endgeräte werden i.d.R. durch das ITSC beschafft, installiert und administriert. Dadurch wird ein sicherer und lizenzkonformer Betrieb gewährleistet, für den auch entsprechender Support geleistet werden kann.

Für die Nutzung der Endgeräte sind in der Regel keine Administratorrechte notwendig, da die Geräte durch das ITSC betreut werden. In begründeten Fällen können dem oder der Benutzer*in Administratorrechte erteilt werden.

In diesem Fall ist der oder die Nutzer*in ausschließlich selbst für die Einhaltung der Regelungen dieser Richtlinie verantwortlich. Schutzmechanismen, Verwaltungstools usw. dürfen nicht deaktiviert/deinstalliert werden.

5. Ausscheiden aus der Hochschule

Dienstgeräte verbleiben nach dem Ausscheiden in der Hochschule und werden im Rahmen des Client LifeCycle Prozess vor einer Weiternutzung durch das ITSC datenschutzkonform gelöscht.