Ostfalia
Hochschule für angewandte Wissenschaften

Verkündungsblatt

Ostfalia Hochschule für angewandte Wissenschaften
– Hochschule Braunschweig/Wolfenbüttel

25. Jahrgang | Wolfenbüttel, den 20.05.2022 | Nummer 30

Inhalt

- Informationssicherheitsrichtlinie der Ostfalia Hochschule für angewandte Wissenschaften – Hochschule Braunschweig/Wolfenbüttel

Seite 2

Informationssicherheitsrichtlinie der Ostfalia Hochschule für angewandte Wissenschaften – Hochschule Braunschweig/Wolfenbüttel

Bekanntmachung des Präsidiumsbeschlusses vom 19.05.2022

Inhaltsverzeichnis

1. Zweck, Anwendungsbereich und Anwender 2

2. Referenzdokumente 2

3. Ansprechpartner*in 2

4. Allgemeingültige Vorgaben

4.1 Softwareeinsatz 3
4.2 Cloud-Nutzung 3
4.3 Passwörter 3
4.4 Vorgaben zum Clean Desk und Clear Screen 3
4.5 Mobiles Arbeiten und Umgang mit mobilen IT-Geräten 4
4.6 Private Hard- und Software 4
4.7 Datensicherung 4
4.8 Informationsübertragung 4
4.9 Verhalten bei Social Engineering 4
4.10 Schutz vor Schadsoftware 5
4.11 Entsorgung und Weiterverwendung 5
4.12 Inkrafttreten der Richtline 5

1. Zweck, Anwendungsbereich und Anwender

Der Zweck dieses Dokuments ist sicherzustellen, dass allen Mitgliedern und Angehörigen der Ostfalia Hochschule für angewandte Wissenschaften – Hochschule Braunschweig/Wolfenbüttel (im Weiteren Ostfalia) der verantwortungsvolle Umgang mit den hochschuleigenen IT- und Kommunikationssystemen sowie Informationen vermittelt wird.

Im Rahmen der steigenden Bedrohungslage gewinnt die Bedeutung der Informationssicherheit auch im Hochschulumfeld immer mehr an Bedeutung. Aufgrund des attraktiven Forschungsstandortes in Deutschland, rücken Hochschulen zunehmend in den Fokus von Cyberangriffen. Durch die offene Struktur einer Hochschule stehen diese einer besonderen Herausforderung gegenüber.
Um in diesem schwierigen Umfeld ein angemessenes Sicherheitsniveau gewährleisten zu können, sind technische und organisatorische Maßnahmen zum Schutz der Hochschulwerte umgesetzt.

2. Referenzdokumente

- DIN EN ISO/IEC 27001:2017-06
  Diese Norm ist nicht frei zugänglich.
  Alleinverkauf der Norm durch Beuth Verlag GmbH, 10772 Berlin

- IT-Grundschutz-Profil für Hochschulen
  https://www.zki.de/top-themen/informationssicherheit/

3. Ansprechpartner*in

Datenschutzbeauftragte*r (DSB):

Die Kernaufgabe der/des Datenschutzbeauftragten ist die Überwachung und Analyse des Umgangs mit personenbezogenen Daten innerhalb der Ostfalia.

E-Mail: datenschutz@ostfalia.de

https://www.ostfalia.de/cms/de/service/privacy/

Informationssicherheitsbeauftragte*r (ISB):

Die/der Informationssicherheitsbeauftragte ist für die Entwicklung und laufende Aktualisierung der Informationssicherheitspolitik verantwortlich und steht Hochschulangehörigen bei allen Fragen zu Themen der Informationssicherheit zur Verfügung.

Tel.: +49 5331 939-19990 (Service Desk des Rechenzentrums)

E-Mail: informationssicherheit@ostfalia.de

https://www.ostfalia.de/cms/de/gremien/beauftragte/

4. Allgemeingültige Vorgaben

4.1 Softwareeinsatz

Auf allen IT-Systemen der Ostfalia darf zum Zweck des Schutzes von hochschuleigenen Informationen und der IT-Infrastruktur, nur Software installiert werden, die zur Erfüllung der dienstlichen Aufgaben erforderlich ist.

Das eigenmächtige Einspielen, insbesondere auch das Herunterladen von Software aus dem Internet oder das Starten von per E-Mail erhaltener Software, ist nur gestattet, wenn sichergestellt ist, dass von dieser Software keine Gefährdung für das IT-System ausgeht.

Im Zweifelsfall ist die Zustimmung der Leitung der betreffenden Organisationseinheit und des Rechenzentrums einzuholen.

4.2 Cloud-Nutzung

Bei der Nutzung von externen Cloud-Diensten (z. B. Microsoft Teams, Slack, Dropbox, Google Drive etc.) besteht bei der Verarbeitung von Informationen durch unberechtigten Zugriff Dritter und die Verletzung datenschutzrechtlicher Vorgaben ein erhöhtes Risiko.

Diese Risiken bestehen:

- Durch die Bereitstellung der Infrastruktur und bei der Verarbeitung von Informationen an Standorten mit abweichenden gesetzlichen Regelungen hinsichtlich Datenschutz und Informationssicherheit (Drittstaaten); dies gilt für eigene Informationen wie auch für die von Dritten.
- Für die Bereitstellung eigener Softwareprodukte, z. B. im Rahmen der Auslieferung neuer Releases oder Updates.
- Durch Einstellung der Cloud-Services durch den Cloud-Service-Provider ohne kurzfristig verfügbare Alternativen.

Vor der Nutzung eines Cloud-Services müssen immer die oben aufgeführten Risiken berücksichtigt werden. Bei konkreten Fragen oder Bedenken zum Einsatz eines bestimmten Cloud-Services, wenden Sie sich bitte an die/den Informationssicherheits- oder Datenschutzbeauftragte*n der Ostfalia (siehe Ziff. 3).

4.3 Passwörter

Der Zugang und Zugriff auf die IT-Systeme, Anwendungen und Informationen der Ostfalia kann erst nach erfolgreicher Authentisierung erfolgen. Durch die Authentisierung wird die eigene Identität nachgewiesen. Dies erfolgt über die Eingabe eines Passworts, die Verwendung eines Tokens oder eines biometrischen Merkmals.

Um sicherzustellen, dass Passwörter möglichst sicher gewählt werden, sind folgende Regeln im Umgang mit und bei der Vergabe von Passwörtern zu beachten:

- Passwörter dürfen für Dritte nicht einsehbar sein oder mit Dritten geteilt werden,
- müssen selbst gewählt werden,
- es dürfen keine identischen Passwörter für unterschiedliche Authentifizierungsstellen (z.B. Ostfalia-Login, Apple-ID, Google-ID, Office365, …) verwendet werden,
- Initialpasswörter und vom Rechenzentrum zurückgesetzte Passwörter sind schnellstmöglich zu ändern,
- Passwörter dürfen nur in einem „Passwortsafe“ gespeichert werden, nicht in Internetbrowsern, unverschlüsselten Dateien oder in Papierform (ausgenommen davon ist die Ablage in einem verschlossenen Umschlag mit Lagerung in einem Safe),
- bei Verdacht auf Missbrauch muss das Passwort sofort geändert und die IT informiert werden.

Die Sicherheit eines Passwortes ist sehr stark abhängig von dessen Komplexität und Länge. Bei der Wahl des Passwortes sind folgende Regeln zu beachten:

- Das Passwort muss mindestens aus 12 Zeichen bestehen,
- Zeichen aus drei der folgenden vier Kategorien enthalten:
  - Großbuchstaben (A bis Z),
  - Kleinbuchstaben (a bis z),
  - Zahlen (0-9),
  - Sonderzeichen (z. B.: $, #, %, +, -, @, !).

Das Passwort darf nicht leicht zu erraten sein, d.h. es darf **nicht** enthalten:

- Name oder Kontoname der/des Mitarbeitenden,
- Geburtstag oder Kfz-Kennzeichen,
- Aufeinanderfolgende Zeichen- oder Zahlenfolgen auf der Tastatur (z. B. QWERTZ, 23456),
- Jahreszahlen,
- Ganze, gebräuchliche Wörter,
- Begrifflichkeiten, die mit dem Unternehmen in Verbindung stehen,
- Im Wörterbuch enthaltene Wörter.

4.4 Vorgaben zum Clean Desk und Clear Screen

Bei längerer Abwesenheit (z. B. Meetings, Termine außer Haus) oder bei Arbeitsende sind beim Verlassen des Arbeitsplatzes grundsätzlich folgende Prinzipien einzuhalten:

Prinzip des Clean Desk: Alle sensiblen und vertraulichen Dokumente sind vom Schreibtisch zu entfernen und sicher aufzubewahren. Das gilt auch für unverschlüsselte mobile IT-Geräte und Speichermedien (z. B. USB-Sticks und mobile Festplatten). Durch das Rechenzentrum der Ostfalia ausgegebene und verwaltete mobile IT-Geräte sind standardmäßig verschlüsselt.

Sensible Dokumente, unverschlüsselte mobile IT-Geräte und Speichermedien sind verschlossen aufzubewahren und die Schlüssel ebenfalls sicher zu verwahren. Ausgedruckte Dokumente mit vertraulichen Informationen dürfen nicht auf dem Schreibtisch oder in der Ablage von Multifunktionsgeräten verbleiben.

Prinzip des Clear Screens: Informationen sind vor dem unberechtigten Einblick oder vor Manipulation von Dritten durch Aktivierung eines Sperrbildschirms zu schützen. Der Sperrbildschirm ist bei jedem, auch kurzfristigem Verlassen des Arbeitsplatzes zu aktivieren.

Am Arbeitsplatz dürfen keine Passwörter oder andere Zugangsinformationen hinterlegt werden.

4.5 Mobiles Arbeiten und Umgang mit mobilen IT-Geräten

Unter mobiler Arbeit wird im Sinne dieser Richtlinie jede auf die Informations- und Kommunikationstechnik gestützte Tätigkeit verstanden, die außerhalb der Geschäftsräume und Gebäude der Ostfalia verrichtet wird.

Beim Einsatz mobiler Geräte entstehen Risiken durch:

- Verlust, Diebstahl oder unsachgemäßem Gebrauch des Geräts,
- Installation nicht lizensierter Software,
- unberechtigten Zugriff auf bzw. Verlust von Informationen bei:
    - Manipulation des Geräts durch bösartige Software/Apps,
    - automatischem Datenabfluss an externe Cloud-Dienste,
    - unzureichendem Patchmanagement für Betriebssystem und Software,
    - Weitergabe oder Entsorgung des Geräts.

Die Einhaltung nachfolgender Regeln soll die oben genannten Risiken minimieren:

- Der Verlust muss umgehend dem Rechenzentrum gemeldet werden.
- Ostfalia eigene Geräte dürfen nicht an Dritte verliehen werden.
- Es liegt in der Verantwortung der anwendenden Person, lokale Daten auf dem persönlichen Netzlaufwerk (Home-Verzeichnis (Laufwerk U:) bzw. im PowerFolder) zu sichern.
- Dritten ist die Nutzung ausschließlich unter Aufsicht der besitzhabenden Person zulässig.
  Die Weitergabe an Dritte ist untersagt.
- Nicht benutzte Schnittstellen (Bluetooth, WLAN) sind zu deaktivieren.

4.6 Private Hard- und Software

Die Benutzung von privater Hard- und Software (Bring Your Own Device, BYOD) ist ausschließlich im W-LAN mit den SSIDs „Ostfalia“, „Eduroam“ und der institutseigenen W-LAN Netze gestattet. Die Leitung der betreffenden Organisationseinheit kann Ausnahmen bei der Leitung des Rechenzentrums beantragen.

Allgemeine Ausnahmen gelten für den Einsatz von privaten Endgeräten für „Mobiles Arbeiten“ im privaten Umfeld.

4.7 Datensicherung

Regelmäßig durchgeführte Datensicherungen sollen vor Verlust durch Fehlbedienung, technische Störungen etc. schützen. Grundsätzlich sind Daten auf zentralen Servern der Ostfalia zu speichern. Ist die Speicherung auf zentralen Servern nicht möglich, sind Sie für die Sicherung Ihrer Daten selbst verantwortlich.

Bei zentraler Datensicherung sollten Sie sich über die in den jeweiligen Bereichen geltenden Regelungen zu Rhythmus und Verfahrensweise für die Datensicherung informieren.

4.8 Informationsübertragung, insbesondere bei dienstlichen Angelegenheiten

Anforderungen an technische und organisatorische Maßnahmen zur Aufrechterhaltung der Vertraulichkeit bei der internen und externen Kommunikation:

- Vor dem Versand von vertraulichen Informationen (z. B. an externe Dienstleister) ist zu prüfen, ob eine Vertraulichkeits- oder Geheimhaltungsvereinbarung abzuschließen ist.
- Keine automatische Weiterleitung von E-Mails an externe E-Mail-Adressen.
- Vor Versand einer E-Mail ist die E-Mail-Adresse der empfangenden Person auf Korrektheit zu prüfen.
- Keine vertraulichen Gespräche in der Öffentlichkeit oder über unsichere Kommunikationskanäle führen.
- Der elektronische Versand vertraulicher Informationen darf ausschließlich verschlüsselt erfolgen.
- Die Nutzung externer öffentlicher Dienste wie Filesharing (z. B. Dropbox, OneDrive und Google Drive etc.) sind für personenbezogene oder vertrauliche Daten auf dienstlichen Geräten untersagt.

4.9 Verhalten bei Social Engineering

Unter „Social Engineering“ versteht man den Versuch, von Personen Informationen zu erhalten, auf die sie kein Anrecht haben. Grundsätzlich sind die Angriffsmethoden und Ziele sehr vielfältig. Prinzipiell nutzen die Angreifer menschliches Verhalten als Schwäche aus. Sie verwenden Autorität und Authentizität, sowie die Hilfsbereitschaft der Opfer.

Das Vorgehen beim Social Engineering kann hier nur beispielhaft geschildert werden, da derartige Angriffe auf alle Bereiche und Abläufe des Alltags gerichtet sein können.

- Sie erhalten eine E-Mail eines unbekannten Absenders.

  Öffnen Sie in keinem Fall den ***Anhang oder Link einer E-Mail***, deren Absender/-in Sie nicht kennen oder dessen Inhalt nicht plausibel erscheint. Hierdurch könnte eine Schadsoftware ausgeführt werden, die z. B. zur Verschlüsselung ihrer Daten lokal und auf Netzwerklaufwerken führen kann. Sofern die Absenderadresse unbekannt ist, löschen Sie diese E-Mail. Falls die Absenderadresse bekannt ist, die E-Mail aber verdächtig erscheint, öffnen Sie bitte keine Anhänge, sondern fragen Sie bei der absendenden Person nach und informieren ggf. den Service Desk.

Sie sollten sich immer bewusst sein, dass es gefährlich ist, geschützte Informationen preiszugeben und sollten sich sofort an die/den Datenschutzbeauftragte*n oder die/den Informationssicherheitsbeauftragte*n wenden, wenn der Eindruck entsteht, dass ein Versuch unternommen wird, auf solche Informationen unberechtigten Zugriff zu erhalten. Alle Informationen sollten deshalb nach dem „Need-to-know“-Prinzip geteilt werden. Es gilt also immer zu berücksichtigen, ob die Person diese Information wirklich benötigt und besitzen darf.

4.10 Schutz vor Schadsoftware

Auf allen dienstlichen Windows-PCs der Ostfalia sind Viren-Schutzprogramme installiert, die durch die IT-Administration installiert und überwacht werden. Diese sollten durch die Anwender*innen grundsätzlich nicht deaktiviert werden. Auf IT-Systemen, welche sich mit dem Ostfalia Netz verbinden, muss eine Viren-Schutzsoftware installiert sein.

Folgende Situationen können im Zusammenhang mit einer möglichen Infektion stehen:

- Häufige Programmabstürze, unerklärliches Systemverhalten oder Fehlermeldungen (insb. Betriebssystem, Office-Anwendungen, etc.).
- Unerklärliche Veränderungen von Icons oder Dateiinhalten.
- Ständige Verringerung des freien Speicherplatzes.
- Versand von E-Mails ohne Aktion durch die Anwender*innen.
- Nicht auffindbare oder verschlüsselte Dateien.
- Kein Zugriff auf Laufwerke oder Datenträger.
- Probleme beim Starten des IT-Systems.
- Probleme beim Verändern oder Abspeichern von Dateien.

Die beschriebenen Effekte können allerdings auch andere Ursachen haben, daher gilt in jedem Fall:

- **Ruhe bewahren!**
- IT-System vom Netz trennen (Netzwerkkabel ziehen oder WLAN-Verbindung trennen) und nicht mehr am System weiterarbeiten!

Meldung an zentrale Meldestelle und auf weitere Anweisungen warten!

- Der Service Desk ist als erste Anlaufstelle über jegliche Art von ungewöhnlichem Verhalten von IT-Geräten zu informieren.

4.11 Entsorgung und Weiterverwendung

Informationen der Ostfalia werden auf Ausdrucken, Betriebsmitteln und Datenträgern gespeichert. Diese Informationen sind vor Weitergabe, Austausch oder Reparaturen der Betriebsmittel und Datenträger zu sichern und zu löschen.

In diesem Rahmen müssen folgende Regeln von allen Mitarbeiter*innen beachtet werden:

Entsorgung von Ausdrucken

- Nicht vertrauliche Dokumente können über ungeschützte Papiersammelbehälter entsorgt werden.
- Ausdrucke mit vertraulichen Inhalten sind über aufgestellte Aktenvernichter zu entsorgen oder bis zur Vernichtung in verschlossenen Einrichtungen (z. B. Datenschutztonne) zu sichern.

Rückgabe, Weiterverwendung oder Entsorgung von Betriebsmitteln

- Bei Rückgabe von Betriebsmitteln, geplanter Weiterverwendung funktionsfähiger oder Entsorgung defekter Betriebsmittel sind diese dem Rechenzentrum zu übergeben.
- Eine Weitergabe oder Entsorgung darf nur durch das Rechenzentrum und erst nach Löschung der darauf gespeicherten Informationen erfolgen.

4.12 Inkrafttreten der Richtline

Die Informationssicherheitsrichtlinie der Ostfalia Hochschule für angewandte Wissenschaften – Hochschule Braunschweig/Wolfenbüttel tritt nach ihrer Bekanntmachung im Verkündungsblatt der Hochschule zum 01.06.2022 in Kraft.