AMTLICHE MITTEILUNGEN

Hochschule Düsseldorf
University of Applied Sciences

Verkündungsblatt
der Hochschule Düsseldorf

HSD NR. 913

Das Verkündungsblatt der Hochschule
Herausgeberin: Die Präsidentin

07.02.2024
Nummer 913

Richtlinie zur Informationssicherheit und Datenschutz am Arbeitsplatz an der Hochschule Düsseldorf

Vom 07.02.2024

Aufgrund der §§ 2 Abs. 4 S. 2, 16 Abs. 1 des Gesetzes über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz - HG) vom 16.09.2014 (GV. NRW. S. 547) in der aktuell gültigen Fassung hat die Hochschule Düsseldorf die folgende Richtlinie erlassen.

Hochschule Düsseldorf
University of Applied Sciences

HSD

Datenschutz- und Informations-
sicherheitsmanagement (DISM)

Infos und Ansprechpartner:
hs-duesseldorf.de/dism

INFORMATIONSSICHERHEIT UND DATENSCHUTZ AM ARBEITSPLATZ

INHALT

1 EINLEITUNG

Die Hochschule Düsseldorf und ihre Mitglieder sind verpflichtet, mit Informationswerten und insbesondere personenbezogenen Daten verantwortungsvoll umzugehen und angemessene technische und organisatorische Maßnahmen gegen den Verlust oder Missbrauch von Daten umzusetzen. Diese Verpflichtung erstreckt sich auch auf die Verarbeitung von Daten an individuellen Arbeitsplätzen und ist unabhängig vom Ort der Verarbeitung. Die Daten können dabei digital oder in Papierform vorliegen.

Die organisatorische Struktur einer Hochschule erschwert die Formulierung allgemeingültiger Regelungen für die informationstechnische Absicherung von Arbeitsplätzen. Während in anderen Organisationen standardisierte Arbeitsplatz-Systeme in der Regel ausschließlich von zentraler Stelle zur Verfügung gestellt und in ein zentrales System-Management eingebunden werden, stellt sich die Situation an Hochschulen mit deren dreigliedrigem Aufbau *Lehre – Forschung – Verwaltung* komplexer dar. Aber auch wenn eine zentral gesteuerte Standardisierung in den Fachbereichen angesichts der Freiheit von Forschung und Lehre nicht ohne Weiteres umsetzbar ist, gelten für Lehrende/Forschende die gesetzlichen Regelungen zum Datenschutz und vertragliche Vereinbarungen (z.B. *non-disclosure agreements* (NDA) mit Kooperationspartnern) zur Informationssicherheit.

Die vorliegende Richtlinie bezieht sich sowohl auf die individuelle Verantwortung aller Beschäftigten für einen verantwortungsvollen Umgang mit Daten als auch auf die Maßnahmen, die Einrichtungen und/oder Beschäftigte umsetzen müssen, wenn sie keine zentral administrierten Arbeitsplatz-Systeme einsetzen. Vorgaben für Beschäftigte (und ggf. dezentrale Einrichtungen) sind im Text hervorgehoben.

Die Gesamtverantwortung des Präsidiums für eine rechtskonforme Datenverarbeitung bleibt davon unberührt.

Diese Richtlinie ist Bestandteil des Datenschutz- und Informationssicherheits-Managements (DISM) der HSD. Die Richtlinie verfolgt die klassischen Schutzziele der Informationssicherheit, nämlich die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen. Sie dient damit auch dem Datenschutz im Sinne der Wahrung der Rechte der von der Verarbeitung personenbezogener Daten Betroffenen. Nicht Gegenstand dieser Richtlinie sind Datenschutz-Prinzipien wie die Datensparsamkeit, die Zweckbindung der Verarbeitung oder der Grundsatz, dass personenbezogene Daten nur auf Grundlage einer Rechtsgrundlage nach Art. 6 und 9 der EU-DSGVO verarbeitet werden dürfen. Diese Prinzipien müssen bereits bei der Gestaltung der Arbeitsprozesse und nicht erst bei der Arbeitsplatzgestaltung berücksichtigt werden.

Im Intranet der HSD ist zu dieser Richtlinie eine Online-Version im Intranet verfügbar, die ergänzende Informationen enthält: DISM-Arbeitsplatz-Richtlinie

2 GRUNDSÄTZE

Zur Erfüllung ihres öffentlichen Auftrags ist die HSD auf korrekte Daten und Informationen angewiesen und muss ihre Verfügbarkeit, Integrität und deren Vertraulichkeit gewährleisten. Daraus leitet sich für die HSD die Verpflichtung ab, **geeignete technisch-organisatorische Maßnahmen (TOM) zum Schutz der Daten und Informationen** umzusetzen und die Umsetzung dieser Maßnahmen zu überwachen. Diese Verpflichtung wird durch gesetzliche (hier ist insbesondere die EU-DSGVO zu nennen) oder vertragliche Regelungen (z.B. Geheimhaltungserklärungen in Kooperationen) unterstrichen.

Die zur Absicherung des Arbeitsplatzes eingesetzten Maßnahmen können allerdings nur dann ihre Wirkung entfalten, wenn sie von **verantwortungsbewusstem und kompetentem Verhalten der Nutzer*innen** begleitet werden. Das heißt nicht, dass alle Nutzer*innen Expertenwissen zur Informationssicherheit aufbauen sollen, es geht vielmehr um eine angemessene Sorgfalt und Aufmerksamkeit im Umgang mit Daten, die unter dem Begriff der *Awareness* zusammengefasst werden. Die Hochschule erwartet von ihren Mitgliedern diese *Awareness* und fördert Aufbau und stetige Aktualisierung durch Schulungen, die Aufklärung über aktuelle Sicherheitsereignisse und Bedrohungen sowie die Bereitstellung von ergänzenden Hintergrundinformationen über interne Medien.

Bei der Verarbeitung digitaler Daten am Arbeitsplatz ist auch die **IT-Ordnung** zu beachten, insbesondere §10 *Allgemeine Regelungen*. Zu beachten ist ebenfalls §11 *Informationssicherheit und Datenschutz* der **Dienstvereinbarung zu ortsungebundenem Arbeiten** (DVOUA).

3 DIE ABSICHERUNG DES ARBEITSPLATZES

Die überwiegende Mehrheit der Arbeitsplätze an der HSD ist IT-gestützt und besteht aus den folgenden technischen Komponenten:

- Endgerät (Notebook, PC-Standgerät)
- Peripheriegeräte (lokaler Drucker, Eingabegeräte, externer Monitor etc.)
- Netzanbindung (LAN, WLAN, UMTS, VPN etc.)

Zum Arbeitsplatz gehört auch seine unmittelbare räumliche Umgebung, entweder in den Räumlichkeiten der HSD, im Home-Office oder an beliebigen (zum Teil öffentlichen) Orten (Zug, Hotelzimmer etc.). Sein grundsätzlicher Aufbau bleibt auch während des ortsungebundenen Arbeitens erhalten.
Bestandteil der Arbeits*umgebung* (aber nicht des Arbeitsplatzes i.e.S.) sind die Netzlaufwerke (und andere netzbasierte Systeme) der HSD.

Das sichere Verhalten am Arbeitsplatz

Einfache und für jede*n am Arbeitsplatz realisierbare Maßnahmen leisten bereits einen großen Beitrag zur Verbesserung des Sicherheitsniveaus. Dabei soll primär Unbefugten der Zugriff auf schützenswerte Daten und Informationen (auch in Papierform!) verwehrt werden. Aber auch dem unbeabsichtigten Verlust von Daten soll vorgebeugt werden.

Schutz der Vertraulichkeit

Nicht immer ist es erforderlich, einen technisch komplizierten Weg über Netzwerke und Firewalls zu finden, um unerlaubten Zugriff auf Daten zu erlangen. Manchmal reicht ein Spaziergang über die an der Hochschule offenen Flure hinein in die oft unverschlossenen Büros und Labore.

Regel 1: For your eyes only

Bitte beachten Sie, dass Sie

- Räumlichkeiten beim vollständigen Verlassen der Arbeitsplätze verschließen
- Unbeaufsichtigte Endgeräte sperren
- Unbefugten den Einblick auf den Bildschirm verwehren
- Vertrauliche Dokumente in Papierform verschlossen aufbewahren und über die vorgesehenen Container oder Aktenvernichter entsorgen
- Besucher in den HSD-Räumlichkeiten begleiteten, falls sich dort schützenswerte und offen zugängliche Informationen und IT-Geräte befinden

Beim ortsungebundenen Arbeiten beachten Sie zusätzlich, dass

- die Arbeitsmittel an öffentlich zugänglichen Orten und in öffentlichen Verkehrsmitteln kontinuierlich zu beaufsichtigen sind,
- die Arbeitsmittel und Unterlagen beim Transport mit den üblichen Vorsichtsmaßnahmen vor Zugriff und Diebstahl geschützt werden,
- möglichst wenige Daten in Papierform außerhalb der HSD gelagert und nicht in den Hausmüll entsorgt werden.
- §11 (4) der DVOUA zu beachten ist.

Schutz vor Datenverlust

Digitale Daten können absichtlich oder versehentlich gelöscht oder auch überschrieben werden. Auch defekte Festplatten können zu Datenverlust führen. Beim Diebstahl oder Verlust von Laptops und Tablets gehen auch die Daten verloren, die sich darauf befinden.

Regel 2: Ohne Backup fehlt Dir was

- Nutzen Sie nach Möglichkeit die Netz- und Cloudspeicher der HSD mit ihren integrierten Backup-Funktionalitäten.
- Für die Sicherung großer Datenmengen lassen Sie sich von der Campus IT beraten.

Schutz vor Social Engineering

Mit „Social Engineering“ bezeichnet man den Versuch eines Angreifers, das Opfer mit geschickter Manipulation dazu zu bringen, vertrauliche Informationen (z.B. ein Passwort) preiszugeben oder eine dem Angreifer nützliche Aktion auszuführen (z.B. eine Banküberweisung auszuführen oder Schadsoftware zu installieren). Als Medium dient dabei zumeist die elektronische Kommunikation (z.B. beim Phishing per E-Mail oder SMS), aber auch die direkte oder telefonische Ansprache ist möglich. *Awareness* bedeutet, sich dieser Gefahren jederzeit bewusst zu sein und eine entsprechende Vorsicht walten zu lassen.

Regel 3: Die menschliche „Firewall“

Bitte beachten Sie, dass

- die in den E-Mail-Clients angezeigte Absender-Adresse einer E-Mail gefälscht werden kann
- Webseiten täuschend echt gefälscht werden können (auch die HSD-Webseiten!)
- immer dann Vorsicht geboten ist
    - wenn eine E-Mail zum Aufrufen eines Links auffordert, insbesondere dann, wenn dort eine Anmeldemaske Zugangsdaten abfragt
    - wenn eine E-Mail einen unbekannten Datei-Anhang enthält
    - wenn eine E-Mail zum Download einer unbekannten Datei auffordert
    - wenn in einer E-Mail (unüblicher) Druck auf den Empfänger ausgeübt wird und dieser zu schnellem (und damit unüberlegtem) Handeln aufgefordert wird
- im Zweifelsfall direkte Rücksprache mit dem vermeintlichen Absender gehalten wird
- verdächtige E-Mails bei der Campus-IT überprüft werden können und diese bei Bedarf auch andere potentielle Empfänger*innen warnen kann
- man verdächtige E-Mails lieber einmal zu viel als zu wenig ignoriert.

Zum allgemeinen Schutz des HSD-Accounts sind auch die Vorgaben der IT-Ordnung zu beachten (siehe IT-Ordnung, §10 (2) d-f)). In jedem Fall empfiehlt es sich aber, die HSD-Zugangsdaten nur für die Systeme der HSD zu verwenden:

Regel 4: Der HSD-Account ist für die HSD gedacht. Schützen Sie ihn.

Der HSD-Account (Benutzername und Passwort) darf nur für dienstliche Zwecke benutzt werden, nicht jedoch für Anmeldungen bei kommerziellen Diensteanbietern im Internet (z.B. Webshops, Streaming-Dienste, Vergleichsportale etc.). Grundsätzlich sollte jedes Passwort nur für genau einen Zweck/Dienst verwendet werden (Ausnahme: Single Sign-On). Schützen Sie Ihren HSD-Account durch

- Auswahl eines komplexen und minimal 8 Zeichen langen Passworts, das sich in keinem Lexikon oder Wörterbuch findet
- wenn möglich, Nutzung einer Zweifaktor-Anmeldung.
  Zurzeit können Beschäftigte auf freiwilliger Basis eine Zweifaktor-Anmeldung für die Microsoft M365-Dienste in ihren Kontoeinstellungen aktivieren.

Meldung von Sicherheitsereignissen

Der/die Nutzer*in kann die Folgen eines möglicherweise sicherheitsrelevanten Ereignisses oft nicht selbst einschätzen, Informationssicherheitsvorfälle können aber ein rasches Handeln und das Eingreifen von Fachleuten erfordern. Die CIT nimmt daher nach Meldung eine Bewertung/Analyse vor und leitet bei Bedarf weitere Maßnahmen ein. Insbesondere Opfer eines Cyberangriffs sollten keine Scheu haben, dies schnell zu melden. Die Angriffstechniken sind heutzutage so fortgeschritten, dass sich praktisch jeder plötzlich in der Opferrolle wiederfinden kann, und es keinen Grund zu falscher Scham gibt.

Regel 5: Meldung von Sicherheitsereignissen

Mögliche Sicherheitsereignisse sind unverzüglich an den Service Desk der Campus IT zu melden (siehe auch IT-Ordnung, §10 (2) l). Auch der Verlust eines Endgerätes oder eines Datenträgers ist schnellstmöglich zu melden.

Service Desk Campus IT	
Telefon	+49 211 4351 – 9999
E-Mail	servicedesk@hs-duesseldorf.de
Ticket-Tool	https://otrs.cit.hs-duesseldorf.de

Bei Bedarf kann eine Meldung auch vertraulich über die Führungskraft oder die Beauftragten für Informationssicherheit und Datenschutz erfolgen. Folgende Kontaktdaten stehen dazu zur Verfügung:

Chief Information Security Officer	informationssicherheit@hs-duesseldorf.de
Datenschutzbeauftragter	datenschutzbeauftragter@hs-duesseldorf.de

Der HSD-Standard-Arbeitsplatz

Der Standard-Arbeitsplatz befindet sich in den Räumlichkeiten der HSD. Die End- und Peripheriegeräte werden über die Campus IT bezogen, die auch den Netzzugang stellt. Endgeräte und Netzwerk werden von der Campus IT administriert und zentral verwaltet.

Regel 6: Einsatz von Standard-Endgeräten

In den Dezernaten und zentralen Einrichtungen werden ausschließlich zentral administrierte Standard-Endgeräte verwendet. Auch den Fachbereichen wird die Nutzung von Standard-Endgeräten dringend empfohlen.

Diese Vorgabe gilt sowohl für die Arbeit auf dem Campus als auch für das ortsungebundene Arbeiten. Sie leitet sich aus den in Abschnitt 2 dargelegten Grundsätzen ab.

Endgeräte (Notebook und Tablet)

Standard-Endgeräte werden von der Campus IT beschafft, für den Gebrauch vorkonfiguriert und an die Beschäftigten ausgehändigt. Zur Absicherung der Endgeräte werden dabei technisch-organisatorische Maßnahmen gemäß Anhang umgesetzt. Endgeräte in diesem Sinne sind derzeit Notebooks und Tablets, aber nicht die dienstlich bereitgestellten Handys und Smartphones („Diensthandy“), da diese noch keinem zentralen Management unterliegen (siehe auch Regel 9).

Netzanbindung

Am Standard-Arbeitsplatz wird der Netzzugang im LAN oder WLAN von der Campus IT bereitgestellt und mit den im Anhang beschriebenen Maßnahmen abgesichert.

Peripherie-Geräte

Peripherie-Geräte wie Monitor, Dockingstation, Maus, Tastatur, Headset, Drucker, Scanner oder Kabel/Adapter stellen in der Regel kein informationstechnisches Sicherheitsrisiko dar. Gezielte Angriffe mit manipulierten Peripherie-Geräten dieser Art sind technisch möglich, aber selten. Wahrscheinlicher sind dagegen Angriffe über externe Speichermedien (USB-Festplatten oder -Sticks).

Regel 7: Keine Nutzung von privaten Speichermedien

In den Dezernaten und zentralen Einrichtungen dürfen privat beschaffte oder fremde externe Speichermedien nicht genutzt werden. Dazu gehört auch das spontane Lesen geringer Datenmengen von solchen Medien. Dienstlich beschaffte und ausschließlich dienstlich genutzte Speichermedien dürfen genutzt werden. Wegen der erhöhten Verlustgefahr sind Daten darauf möglichst zu verschlüsseln.

Wo zum Datenaustausch im Rahmen von Lehre und Forschung, z.B. bei der Abgabe von Prüfungsleistungen, andere als von der HSD dienstlich beschaffte Speichermedien genutzt werden, müssen Beschäftigte Vorsichtsmaßnahmen (wie z.B. einen Virenscan) vor der Nutzung des betreffenden Speichermediums durchführen.

Cloud-Speicher-Dienste

Die HSD stellt verschiedene cloudbasierte Dienste zur Speicherung von Daten zur Verfügung, die für dienstliche Zwecke insbesondere im Office-Bereich geeignet sind (siehe https://cit.hs-duesseldorf.de/services/online-speicher). Die Nutzung weiterer externer Cloud-Speicher birgt zusätzliche technologische und rechtliche Risiken.

Regel 8: Beschränkung auf von der HSD lizenzierte Cloud-Dienste

Vertrauliche und personenbezogene Daten oder Daten der Verwaltung dürfen nicht zu hochschulfremden Cloud-Diensten (Dropbox, Google Drive, iCloud etc.) kopiert werden.

Ort und Räumlichkeiten

Schutzmaßnahmen in Bezug auf die Räumlichkeiten, die u.a. der Informationssicherheit und dem Datenschutz dienen, werden vom Gebäude-Management (D4) vorgegeben und umgesetzt:

- Elektronisches Schließsystem mit differenzierter Rechteverwaltung und Protokollierung
- Brandmeldeanlage
- Alarmierungssystem für allgemeine Notfälle
- Zentraler Empfang und Wachdienst auf dem Campus-Gelände

Ortsungebundenes Arbeiten

Im ortsungebundenen Arbeiten verlagern sich die vier Basiskomponenten des IT-Arbeitsplatzes in den privaten oder öffentlichen Raum. Dabei verlieren am Campus eingesetzte Schutzmaßnahmen (Netzanbindung, Räumlichkeiten etc.) an Wirksamkeit oder gehen gänzlich verloren, wodurch das Risiko einer Beeinträchtigung von Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen steigt. Es muss versucht werden, dieses Risiko so weit wie möglich zu reduzieren. Dabei kann es erforderlich sein, auf bestimmte Formen des ortsungebundenen Arbeitens zu verzichten.

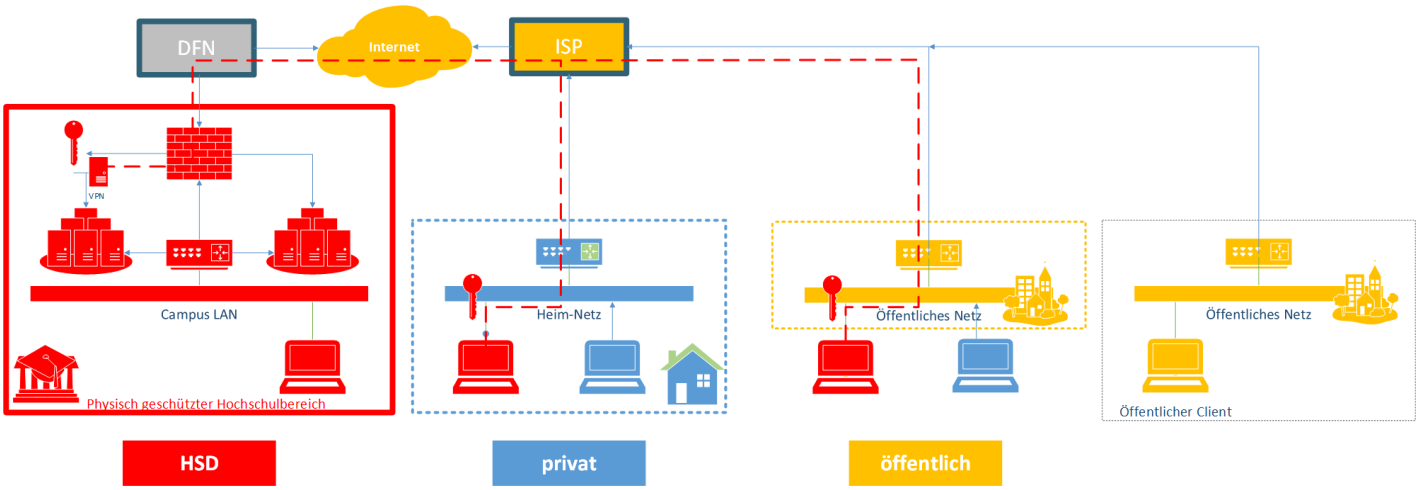

Abbildung 1 Verlagerung des IT-Arbeitsplatzes in den öffentlichen Raum. Der Schlüssel symbolisiert die Absicherung des Netzwerkverkehrs mit einem VPN-Tunnel.

Ort und Räumlichkeiten

Heimische Räumlichkeiten werden als für das ortsungebundene Arbeiten hinreichend sicher betrachtet. Dabei wird erwartet, dass die Beschäftigten den Arbeitsplatz so wählen, dass die Geräte und Unterlagen vor typischen Gefahren im Haushalt (weniger geeignet zum ortsungebundenen Arbeiten sind z.B. Küche und Badezimmer) und in vernünftigem Umfang vor dem Zugriff Unbefugter geschützt werden.

Endgeräte (Notebook und Tablet)

Transportable Endgeräte nach HSD-Standard (Notebook und Tablet) sind auch im ortsungebundenen Arbeiten einsetzbar. Auf privaten Notebooks und Tablets kann die Hochschule geeignete TOM weder

durchsetzen noch kontrollieren**.** Auch ein von den dienstlichen Gepflogenheiten abweichendes Nutzerverhalten (z.B. Aufruf und Nutzung maliziöser Webseiten, Öffnen von infizierten Mail-Anhängen, Installation von Software aus unseriösen Quellen) kann auf privaten Geräten nicht technisch unterbunden werden.

Regel 9: Nutzung von Standard-Endgeräten auch im ortsungebundenen Arbeiten

Auch beim ortsungebundenen Arbeiten sind durch die Beschäftigten in den Dezernaten und zentralen Einrichtungen Endgeräte nach HSD-Standard einzusetzen. Den Beschäftigten in den Fachbereichen wird die Nutzung solcher Endgeräte dringend empfohlen. Die Verwendung privater Endgeräte ist für dienstliche Zwecke nicht gestattet.

Abweichend von Regel 9 ist die geringfügige Nutzung privater Endgeräte, die sich im Besitz der Beschäftigten befinden, gestattet für Online-Zugriffe auf HSD-Dienste wie das Zeiterfassungs-Portal (Dienstgänge, Ausbuchen etc.) oder das Abrufen von E-Mails im Webmaildienst, falls die Nutzung eines Standard-Endgerätes temporär nicht möglich ist (z.B. zur Krankmeldung). Dabei ist die Nutzung auf die Webbrowser-Software zu beschränken, um die aktive Speicherung dienstlicher Daten (z.B. E-Mail-Anhänge) auf dem privaten Gerät zu vermeiden. Gestattet ist die Nutzung eines privaten Smartphones für die Mehrfaktorauthentifizierung.

Smartphones

Dienstliche Smartphones werden derzeit technisch nicht zentral verwaltet, so dass die Durchsetzung und Kontrolle von technischen-organisatorischen Maßnahmen auf diesen Geräten nicht möglich ist. In diesem Sinne besteht kein (technischer) Unterschied zwischen dienstlichen und privaten Smartphones. Dienstliche Smartphones sind daher kein Ersatz für standardisierte Notebooks und Tablets, ihr Einsatz ist – insbesondere in der Verwaltung – auf das erforderliche Minimum zu beschränken. Darüber hinaus wird den Beschäftigten dringend empfohlen, die Geräte ausschließlich für dienstliche Zwecke zu nutzen und so die Risiken weiter zu reduzieren.

Für die Verwendung privater Smartphones für dienstliche Zwecke gelten dieselben Einschränkungen wie für andere private Endgeräte.

Öffentliche Endgeräte

Auf öffentlich zugänglichen Endgeräten (Internet-Café, Hotel-Lobby…) stellt bereits die bloße Eingabe von HSD-Anmeldedaten ein hohes Risiko dar, da diese durch einfache Manipulation des Gerätes mitgeschnitten werden können.

Regel 10: Keine öffentlichen Endgeräte für dienstliche Zwecke

Die Verwendung von Diensten, die eine Anmeldung mit dem HSD-Anmeldedaten erfordern, ist auf öffentlichen Endgeräten nicht gestattet.

Netzanbindung

Beim ortsungebundenen Arbeiten ist die Verwendung

- lokaler privater Netze (heimisches LAN oder WLAN)

- öffentlicher Netze (mobile Datenverbindungen, Hotspot, LAN oder WLAN in Hotels und Gaststätten etc.)
- darüber erreichbare Internet-Zugänge beim jeweiligen Provider

unvermeidbar. Es ist zu beachten, dass die Campus IT bei der Nutzung dieser Netze lediglich Remote-Support bei der Konfiguration des Standard-Endgerätes leisten kann, nicht aber bei privaten oder öffentlichen Routern oder anderen Netzwerk-Geräten.

Der Zugriff auf sicher konfigurierte HSD-Ressourcen (z.B. Netzlaufwerke, Web-Portale, Server) erfolgt in der Regel mit Transportverschlüsselung und auf Standard-Endgeräten **über einen automatisch aktivierten VPN-Tunnel**. Bei Nicht-Standard-Geräten sollte nach Möglichkeit ebenfalls eine VPN-Verbindung hergestellt werden. Bei den verwendeten lokalen Netzen sollte **ergänzend darauf geachtet werden:**

a) Nutzung des dienstlichen Gerätes im heimischen Netzwerk
   - Nutzen Sie im WLAN WPA2-Verschlüsselung mit starkem Passwort
   - Geben Sie das WLAN-Passwort nur einem begrenzten Nutzerkreis bekannt.
   - Überprüfen Sie regelmäßig, ob unbekannte Geräte Zugang zu Ihrem WLAN haben.
   - Geben Sie Admin-Passwort des Routers so wenig Nutzer*innen wie möglich bekannt, ändern Sie auf jeden Fall das Default-Passwort!

b) Nutzung des dienstlichen Gerätes in einem öffentlichen Netzwerk
   - Benutzen Sie möglichst verschlüsselte öffentliche Netze. Falls Sie keinen Standard-PC nutzen, aktivieren Sie immer unmittelbar nach der Verbindung mit dem öffentlichen Netz eine VPN-Verbindung mit der HSD.
   - Aktivieren Sie keine Datei- und Verzeichnisfreigaben (Einstellung als öffentliches Netzwerk).
   - Deaktivieren Sie das automatische Verbinden mit offenen WLAN-Netzen

Peripherie-Geräte

Der Einsatz von privaten Peripherie-Geräten, die kein erhöhtes Sicherheitsrisiko darstellen (Monitor, Dockingstation, Maus, Tastatur, Headset, Drucker, Scanner oder Kabel/Adapter), ist im ortsungebundenen Arbeiten gestattet.

Dienstreisen ins Ausland

Die Ein- und Ausfuhr von elektronischen Geräten und Datenträgern sowie deren Nutzung kann strengen Regelungen des Reiselandes unterliegen. Auch die Ausfuhr von Software, Daten und Informationen in bestimmte Länder kann durch deutsches oder europäisches Recht eingeschränkt sein.

Regel 11: Beachten Sie die Regelungen des Reiselandes!

Informieren Sie sich bei Dienstreisen, welche Regelungen im Reiseland zu beachten sind (z.B. auf den Webseiten des Auswärtigen Amtes) und verzichten Sie im Zweifelsfall auf die Mitnahme von elektronischen Geräten und Datenträgern. Möglicherweise sind auch Regelungen zur Ausfuhrkontrolle zu beachten. Informationen dazu (insbesondere auch für Wissenschaft und Forschung) finden Sie auf den Webseiten des Bundesamtes für Wirtschaft und Ausfuhrkontrolle (BAFA).

Dezentral administrierte Arbeitsplätze

In den Fachbereichen und Instituten können bei Bedarf und mit entsprechender Begründung vom HSD-Standard-Arbeitsplatz abweichende Arbeitsplätze genutzt werden. Dadurch spielt der verantwortungsvolle Umgang der Beschäftigten mit Daten und Informationen dort noch eine größere Rolle. Es empfiehlt sich, den in dieser Richtlinie formulierten Regeln zur technologischen Gestaltung des Arbeitsplatzes und seines sicheren Gebrauches Folge zu leisten, insbesondere dann, wenn personenbezogene Daten verarbeitet werden oder in Projekten und Förderverfahren die Beachtung von Datenschutz- und Informationssicherheit vertraglich vereinbart oder verlangt wird.

Bei Projektanträgen und dem Abschluss von Geheimhaltungsvereinbarungen ist es in der Regel von Vorteil, auf eine gemäß dieser Richtlinie standardisierte IT-Ausstattung verweisen zu können.

Regel 12: Selbstverwaltung heißt Eigenverantwortung

Bei der Nutzung dezentral verwalteter Arbeitsplätze sind die*der Nutzer*in oder die für die Administration zuständige Einrichtung gehalten, technisch-organisatorische Maßnahmen umzusetzen, um ein dem HSD-Standardarbeitsplatz vergleichbares Schutzniveau (vgl. Anhang) zu gewährleisten.
Darüber hinaus sollte die Kompatibilität alternativer Geräte mit den zentralen IT-Diensten berücksichtigt werden.

In-Kraft-Treten

Diese Richtlinie tritt am Tage nach ihrer Veröffentlichung im Verkündungsblatt der Hochschule Düsseldorf in Kraft.

Ausgefertigt aufgrund des Beschlusses des Präsidiums der Hochschule Düsseldorf vom 10.01.2024. Düsseldorf,

den 07.02.2024

gez.
Die Präsidentin
der Hochschule Düsseldorf
Prof. Dr. Edeltraud Vomberg

4 ANHANG

Endgeräte

Die von der Campus IT beschafften und an die Beschäftigten ausgehändigten Endgeräte werden durch die folgenden technisch-organisatorischen Maßnahmen über ihren Lebenszyklus abgesichert:

- Auswahl der Hardware und des Betriebssystems nach funktionalen, organisatorischen und wirtschaftlichen Aspekten
- Definition und initiale Installation von standardisierten System-Images einschließlich
- Initial-Konfiguration des Betriebssystems
- Anti-Virus-Lösung (auch als Bestandteil des Betriebssystems)
- Netzwerk-Konfiguration und VPN-Client
- Datenträger-Verschlüsselung auf Betriebssystem-Ebene
- Standard-Software
- Einbettung des Gerätes in ein zentrales System-Management zur
    - Benutzerauthentifizierung und Rechtevergabe gegen das zentrale Identitäten-Management
    - lokalen System-Konfiguration gemäß einer zentralen Richtlinie
    - Steuerung der Funktions- und Security-Updates des Betriebssystems
    - Steuerung des Updates der Antivirus-Signaturen
    - Weiterleitung sicherheitsrelevanter lokaler Systemmeldungen in eine zentrale Management-Konsole (z.B. Malware-Funde)
    - Netzwerk-Installation und -aktualisierung von Standard-Software
    - Zertifikats- und Schlüsselverwaltung
    - Fernwartung durch CIT
    - Begrenzung der Telemetriedaten auf support- und sicherheitsrelevante Information
- Support bei Sicherheits-Ereignissen durch Service Desk der CIT
- Allgemeiner Support des Gerätes durch CIT
- Rücknahme des Gerätes, fachgerechte Entsorgung oder Wiederverwendung der Hardware und Löschung von Daten
- Aufklärung der Beschäftigten über diese Richtlinie bei Ausgabe des Gerätes

Bei der Auswahl und Umsetzung dieser Maßnahmen orientiert sich die HSD an Anforderungen, die in den relevanten Bausteinen des BSI-Grundschutzes formuliert werden (insbesondere Baustein *SYS.2.1 Allgemeiner Client*, *SYS.3.1 Laptops* und *OPS.1.2.4 Telearbeit*)

Netzanbindung

Der Netzzugang eines Standard-Arbeitsplatzes wird von der Campus IT mit

- 802.1x-Authentifizierung im Campus-LAN und WLAN
- WLAN-Verschlüsselung per WPA2 Enterprise
- VPN

abgesichert.