RICHTLINIE

ZUR IT-NUTZUNG AN DER HMDK STUTTGART

Inhalt

1. VORBEMERKUNG

Der Einsatz von Informations- und Kommunikationstechnik ist für die Arbeit an der HMDK Stuttgart von grundlegender Bedeutung für Lehre, Forschung und Verwaltung. Neben Gefährdungen durch IT-Fehlfunktionen oder Nutzungsfehlern kann die IT-Infrastruktur Ziel von internen und externen Angriffen sein. Um dies zu vermeiden, soll diese Richtlinie verbindliche Vorgaben für Nutzer und Nutzerinnen geben.

Dabei sind IT-Nutzer und -Nutzerinnen sämtliche Personen, die die IT-Infrastruktur der HMDK gebrauchen (z.B. Anwendungen, Zugänge, IT-Systeme etc.).

IT-Bedienstete sind die Beschäftigten der Verwaltung, die mit der Administration, Wartung und Betreuung der IT-Infrastruktur betraut sind.

„Personenbezogene Daten“ meint im Sinne des Art. 4 Nr. 7 Europäische Datenschutzgrundverordnung (DS-GVO) alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, einer Nummer, Standortdaten, einer Online-Kennung identifiziert werden kann.

2. RECHTSGRUNDLAGE

Die geltenden Rechtsvorschriften zu IT-Sicherheit und Datenschutz sind bei der Verarbeitung von Daten durch IT-Nutzer und -Nutzerinnen einzuhalten. Dies gilt ebenso für interne Regelungen und Anweisungen.

Personenbezogene Daten oder sonstige schützenswerte Daten der HMDK dürfen nicht unbefugt oder unrechtmäßig verarbeitet werden. Sie sind daher nur in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der übertragenen Aufgaben erforderlich ist. Die Sicherheit der Verarbeitung der Daten darf weder absichtlich noch unabsichtlich (z.B. durch Vernichtung, Veränderung, unbefugte Offenlegung oder unbefugten Zugang) verletzt werden.

IT-Nutzer und -Nutzerinnen sind angehalten sich bei Unsicherheiten im Umgang mit den vorbezeichneten Regelungen an die IT-Bediensteten sowie ggf. an den Beauftragten für Informationssicherheit und/oder den Datenschutzbeauftragten der HMDK zu wenden. IT-Nutzer und -Nutzerinnen haben pflichtbewusst, umfassend und wahrheitsgemäß mit den IT-Bediensteten zu kooperieren und zu kommunizieren.

3. ALLGEMEINE MAßNAHMEN

3.1. DIENSTLICHE IT

Die zur IT-Nutzung überlassenen dienstlichen Geräte der HMDK sind sorgfältig und schonend zu behandeln. Die vorhandenen Ressourcen und Betriebsmittel – z.B. Arbeitsplätze, Rechner-, Speicher- und Übertragungskapazitäten – sind verantwortungsvoll und wirtschaftlich zu nutzen.

3.2. PRIVATE NUTZUNG DIENSTLICHER IT

Jegliche Form der privaten Nutzung der zur Verfügung gestellten dienstlichen IT ist untersagt.

IT-Nutzer und -Nutzerinnen dürfen insbesondere nicht:

- Laden, Speichern und Bearbeiten privater Dokumente, Bilder, Musikdateien, Videodateien und vergleichbarer Dateiformate,
- Browsern oder sonstiger internetfähiger Software zum Abruf von Information, Daten oder Apps privat nutzen,
- Private Nachrichten, Bildern oder Videos per E-Mail, Chat, Messanger oder sonstiger Kommunikationssoftware versenden oder empfangen,

außer dies ist in dieser Richtlinie ausdrücklich vorgesehen.

Bei Änderungen an Hard- oder Software oder Konfigurationen sind IT-Bedienstete hinzuzuziehen. Eine eigenmächtige Umgehung von Sicherheitseinrichtungen ist untersagt.

Eine dienstlich veranlasste Privatnutzung ist keine Privatnutzung im Sinne dieses Abschnitts. Dies ist etwa der Fall, wenn wegen kurzfristiger dienstlicher Angelegenheiten ein privater Termin abgesagt werden muss.

Die HMDK kann einen angemessenen Kostenersatz erheben, sofern sich die private Nutzung nicht in einem geringfügigen Rahmen hält. Der jeweilige IT-Nutzer oder -Nutzerin haftet für alle Schäden, die der HMDK aus der privaten Nutzung entstehen.

3.3. NUTZERKENNUNGEN

Alle Rechnersysteme der HMDK werden durch die IT-Bediensteten in der Form eingerichtet, dass nur berechtigte Nutzer die Möglichkeit haben, mit ihnen zu arbeiten. Grundsätzlich ist zunächst eine persönliche Anmeldung mit Nutzerkennung und Passwort erforderlich. Die Nutzerkennung erfolgt ausschließlich personenbezogen. Es ist untersagt, Kennungen und Passwörter weiterzugeben. Die Nutzungsberechtigung erlischt durch Widerruf der betreibenden Einrichtung oder durch Ausscheiden aus der HMDK, soweit nicht etwas anderes bestimmt ist.

3.4. ZUGRIFFSSCHUTZ DIENSTLICHER GERÄTE

Der Zugriff auf dienstliche Geräte und auf deren Anwendungen muss durch Schutzvorkehrungen wie Passwort, PIN usw. abgesichert werden. Der unbefugte Zugang zu Geräten und die unbefugte Nutzung der Informationstechnik muss verhindert werden. Bei Abwesenheit sind die Geräte zu sperren. Monitore sind so zu platzieren, dass schützenswerte Daten nicht unbefugt eingesehen werden können. Grundsätzlich sind die Systeme nach der Abmeldung auszuschalten, es sei denn, betriebliche Anforderungen sprechen dagegen. Eine Weitergabe der zur alleinigen Nutzung überlassenen dienstlichen Geräte – auch an andere IT-Nutzer und -Nutzerinnen innerhalb der HMDK – ist nicht gestattet.

3.5. RÄUMLICHER ZUGANGSSCHUTZ

Es muss verhindert werden:

- der unbefugte Zugang zu Geräten und die Nutzung der Informationstechnik
- der Zutritt von Räumen mit Informationstechnologie bei Abwesenheit
- das Entnehmen ausgedruckter Daten durch Unbefugte.

3.6. PASSWORTSICHERHEIT

Passwörter sind geheim zu halten und sollten nicht notiert werden. Die Verwendung eines Passwort-Safes (z.B. Keepass) wird empfohlen. Passwörter sind nach den gängigen Sicherheitsstandards zu gestalten.[1]

Bei Vergessen des Passwortes bzw. nach mehrfacher fehlerhafter Passworteingabe, wie auch bei Verlust oder Verdacht auf Kompromittierung des Passwortes sind die IT-Nutzer und -Nutzerinnen verpflichtet, die IT-Bediensteten zu unterrichten.

3.7. SOFTWARE- UND ANWENDUNGSEINSATZ

Auf Rechnersystemen der HMDK dürfen nur Software und Anwendungen installiert werden, die von der zuständigen Stelle dafür freigegeben wurden. Das Einspielen oder das Starten von per E-Mail erhaltener Software ist nur gestattet, wenn eine Erlaubnis der IT-Bediensteten vorliegt. Die Nutzung von Verfahren zur E-Mail-Verschlüsselung und -signatur sowie Verfahren zur Nutzung digitaler Signaturen und vergleichbarer elektronischer Verfahren hat in Abstimmung mit den IT-Bediensteten zu erfolgen.

Bei der Nutzung von Software und Informationsangeboten, Dokumentationen und anderen Daten sind die gesetzlichen Bestimmungen, insbesondere zum Urheberrecht und Markenschutz, einzuhalten und die Lizenz- und Nutzungsbedingungen zu beachten.

---

[1] Derzeit: mind. 8 Stellen lang, mind. je einen Buchstaben, Ziffer und Sonderzeichen, nicht leicht erratbar. Voreingestellte Passwörter sind zu ändern, genauso wie bei Verdacht auf Missbrauch, signifikanter Unterschied zwischen altem und neuem Passwort.

Die private Nutzung der für dienstliche Zwecke erworbenen Software ist generell untersagt.

Das Speichern von Bilderarchiven, Video- und Musikdateien auf den Netzlaufwerken der HMDK kann nach Bedarf und Rücksprache mit den IT-Bediensteten, ggf. auf anderen Speichermedien oder -plätzen, erfolgen.

3.8. EINSATZ PRIVATER SOFT- UND HARDWARE

Der Einsatz von privater Hard- und Software zu dienstlichen Zwecken ist nur im offenen WLAN der HMDK erlaubt. Ausnahmen sind möglich und vom Kanzler oder der Kanzlerin zu genehmigen.

Im internen Verwaltungsnetzwerk ist es untersagt, private Hard- oder Software in Verbindung mit technischen Einrichtungen der HMDK zu verwenden. Die Nutzung privater Endgeräte sowie Peripherie im LAN-Bereich der HMDK (u.a. Laptops, Smartphones, Tablets, USB-Sticks) ist unzulässig.

3.9. NETZZUGÄNGE

Der Anschluss von Systemen an das Datennetz der HMDK hat ausschließlich über die dafür vorgesehene Infrastruktur zu erfolgen. Die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen (Modems, Access-Points o. ä.) ist unzulässig. Auf die IT-Infrastruktur der HMDK soll von außerhalb grundsätzlich mittels VPN erfolgen. Die Zugänge hierfür werden durch die IT-Bediensteten verwaltet.

3.10. NUTZUNG VON E-MAIL-, INTERNET- UND CLOUD-DIENSTEN

Die Nutzung von Internetdiensten darf nur für dienstliche Zwecke erfolgen. Für die dienstliche Kommunikation sowie die Kommunikation im Rahmen des Studiums ist ausschließlich die zugewiesene Hochschul-E-Mail-Adresse zu verwenden. Eine Weiterleitung an eine private E-Mail-Adresse soll nicht erfolgen. Die E-Mail-Adresse wird von der HMDK ausschließlich zu dienstlichen Zwecken bereitgestellt und darf auch nur zu diesen Zwecken genutzt werden. Die private Nutzung der E-Mail-Adresse wird ausdrücklich untersagt.

Anhänge von unbekannten oder unerwünschten E-Mails bzw. von unbekannten Absendern dürfen in keinem Fall geöffnet oder angeklickt werden. Grundsätzlich ist darüber hinaus vor jedem Öffnen einer E-Mail bzw. eines Anhangs zu überprüfen, ob der formulierte Betreff sinnvoll ist und ein Anhang vom Absender erwartet wird, andernfalls dürfen E-Mails und Anhänge nicht geöffnet werden. Im Bedarfsfall ist mit dem Absender telefonisch Rücksprache zu halten. Bei Zweifelsfällen sind die IT-Bediensteten zu informieren.

Die Nutzung externer Clouddienste ist nur oben dargestellten Umfang dieser Richtlinie definierten Vorgaben zulässig. Der Einsatz privater Clouddienste ist stets unzulässig. Falls Cloud-Dienste von externen Providern zum Einsatz gebracht werden sollen, ist zwingend vorherige

Rücksprache mit den IT-Bediensteten erforderlich. Der eigenmächtige Einsatz von Cloud-Diensten ist unzulässig.

3.11. INFORMATIONSWEITERGABE

Die Kommunikation und Weitergabe personenbezogener und sonstiger schützenswerter Daten erfolgt ausschließlich an eindeutig authentifizierte Personen. Stimmen etwa Name und Kontaktdaten der anfragenden Personen mit den in den Systemen der HMDK gespeicherten Daten überein, wird regelmäßig keine Veranlassung bestehen, an der Identität des Anfragenden zu zweifeln. Bei nicht eindeutig identifizierten Kommunikationspartnern (z.B. Abweichung zwischen aktueller und bisheriger Mailadresse) erfolgt nur eine schriftliche Auskunft an die in den Systemen der HMDK hinterlegte Adresse.

Bei nicht authentifizierten Anrufen darf keine Auskunft über personenbezogene und sonstige schützenswerte Daten erteilt werden. IT-Nutzer und -Nutzerinnen müssen die auskunftsbegehrende Person auf die Geltendmachung per Textform (Brief, Fax, E-Mail) verweisen.

3.12. UMGANG MIT DATENTRÄGERN

Dienstliche Mobile Datenträger mit personenbezogenen und sonstigen schützenswerten Daten sind vor unbefugtem Zugriff geschützt (verschlossen) aufzubewahren. Die Daten müssen verschlüsselt werden.

3.13. VERNICHTUNG VON DATEN UND HARDWARE

Papiere mit vertraulichem Inhalt sind mit Hilfe eines Aktenvernichters zu vernichten. Bereitgestellte Sammelbehälter/Container müssen verpflichtend genutzt werden. Datenträger (bspw. USB-Sticks, externe Festplatten, Speicherkarten etc.) mit personenbezogenen oder sonstigen schützenswerten Daten müssen vor einer Weitergabe an nicht autorisierte Personen physisch gelöscht werden. Dasselbe gilt für auszusondernde oder defekte Datenträger.

3.14. DATENSCHUTZ IN DER MOBILEN ARBEIT

Die DS-GVO und das LDSG BW sowie alle weiteren einschlägigen datenschutzrechtlichen Regelungen für den Datenschutz am Arbeitsplatz in der jeweils aktuellen Fassung gelten auch für Mobile Arbeit. Personenbezogene und sonstige schützenswerte Daten in jeder Form sind auch am Mobilen Arbeitsplatz vor dem unberechtigten Zugriff Dritter zu schützen und vertraulich zu verwahren.

Es ist dabei insbesondere verboten

- Dritten Passwörter oder sonstige Zugangsmöglichkeiten zur dienstlichen EDV mitzuteilen
- Dritten (z.B. Familienmitgliedern, sonstigen Mitbewohnern, Besuchern) Zugriff auf dienstliche IT und/oder dienstliche Unterlagen zu gewähren;

- den Mobilen Arbeitsplatz unbeaufsichtigt zu lassen;
- dienstliche Daten auf privaten Speichermedien zu speichern;
- die bereitgestellten dienstlichen Endgeräte bzw. Nutzerkennungen privat zu nutzen;
- Sicherheitsmaßnahmen zu deaktivieren oder zu umgehen oder sonstige technische Veränderungen an den zur Verfügung gestellten Geräten vorzunehmen. Software darf nur durch die IT-Abteilung installiert werden;

Ausdrucke mit personenbezogenen oder sonstigen schützenswerten Daten müssen sicher vernichtet werden, wenn sie nicht mehr benötigt werden.

Im Übrigen wird auf die Dienstvereinbarung Mobile Arbeit in der jeweils geltenden Fassung verwiesen.

4. VERHALTEN BEI WEISUNGEN, HAFTUNG

IT-Nutzer und -Nutzerinnen sind verpflichtet, den Weisungen der IT-Bediensteten hinsichtlich der technischen Umsetzungen dieser Richtlinie Folge zu leisten. Bei Zweifeln über die Sinnhaftigkeit kann der Teamleiter oder Kanzler eingebunden werden.

Die HMDK kann die Nutzung der IT durch den IT-Nutzer und -Nutzerin ein- und beschränken oder entziehen, wenn gegen die in dieser Richtlinie genannten Pflichten verstoßen wurde.

Der jeweilige IT-Nutzer und -Nutzerin haftet für alle Schäden, die der HMDK durch missbräuchliche oder rechtswidrige Verwendung der IT entstehen oder dadurch entstehen, dass er oder sie schuldhaft ihren oder seinen Pflichten aus dieser Richtlinie nicht nachkommt. Der jeweilige IT-Nutzer und -Nutzerin hat die HMDK von allen Ansprüchen freizustellen, wenn Dritte die HMDK wegen eines missbräuchlichen oder rechtswidrigen Verhaltens von ihm oder ihr auf Schadensersatz, Unterlassung oder in sonstiger Weise in Anspruch nehmen.

5. SICHERHEITSVORFÄLLE

Ein Sicherheitsvorfall als Ereignis, das tatsächlich nachteilige Auswirkungen auf die Informationssicherheit hat, kann absichtlich oder unabsichtlich eintreten, indem versucht wird die Vertraulichkeit, Integrität oder Verfügbarkeit zu verletzen:

- Missbrauch von Nutzer-Credentials (Passwörter, Zugangsdaten),
- (Distributed) Denial of Service (herbeigeführte Überlastung eines Systems zur Lahmlegung),
- nichtautorisierte Nutzung von Diensten oder Systemen,

- Versenden von Malware per E-Mail,
- Verbreitung illegaler Inhalte (z.B. Filme, Fotos),
- Sabotage,
- Datenabfluss durch Malware, Hacking oder Social Engineering,
- Manipulation von Daten, Hard- oder Software,
- Installation von Malware auf Server oder Clients,
- Unsachgemäße Entsorgung von IT-Systemen,
- Diebstahl oder Verlust von IT-Systemen oder mobilen Geräten/Datenträgern,
- Offenlegung dienstlicher Informationen.

Wird ein Informationssicherheitsvorfall festgestellt oder vermutet, so ist der Vorfall unverzüglich an die IT-Bediensteten und dem Kanzler zu melden.

6. ANSPRECHPARTNER IT

it@hmdk-stuttgart.de

7. INKRAFTTRETEN

Diese Richtlinie tritt zum 15.11.2025 in Kraft und löst alle bisherigen Regelungen zum Themenbereich IT ab.

Stuttgart, den 10.11.2025

gez. Martin Renz
Kanzler