Hochschule für Musik
Carl Maria von Weber Dresden

Richtlinie zur IT-Nutzung

Inhaltsverzeichnis **Seite**

I. Allgemeines 2

Zielsetzung 2

Begriffsdefinition 2

II. Einhaltung von Rechtsvorschriften **2**

III. Allgemeine Maßnahmen des IT-Grundschutzes für IT-Nutzer*innen

1. Private Nutzung dienstlicher IT 3

2. Umgang mit Nutzerkennungen 3

3. Zugriffsschutz auf dienstlichen Geräten 3

4. Räumlicher Zugangsschutz 3

5. Passwortsicherheit 4

6. Kontrollierter Software- und Anwendungseinsatz 4

7. Einsatz privater Hard- und Software 4

8. Netzzugänge 5

9. Nutzung von E-Mail- und Internetdiensten 5

10. Nutzung externer Clouddienste 5

11. Grundsätze der Informationsweitergabe 5

12. Umgang mit Datenträgern 6

13. Vernichtung von Dokumenten und Hardware gemäß rechtlicher Vorgaben 6

14. Datenschutzanforderungen in der mobilen Arbeit 6

IV. Verhalten bei Weisungen 7

V. Verhalten bei Informationssicherheitsvorfällen 7

Hochschule für Musik
Carl Maria von Weber Dresden

I. Allgemeines

Zielsetzung

Der Einsatz von Informations- und Kommunikationstechnik (im Folgenden jeweils gleichbedeutend IuK und IT) an der Hochschule für Musik Dresden Carl Maria von Weber (HfM) ist von grundlegender Bedeutung für exzellente Forschung und Lehre sowie effiziente Verwaltung. Durch den zunehmenden Einsatz von IuK und daraus resultierende Abhängigkeiten können aber auch Bedrohungen für die HfM entstehen. Neben Gefährdungen durch IT-Fehlfunktionen oder Nutzungsfehler kann die IT-Infrastruktur Ziel von internen und externen Angriffen sein.

Begriffsdefinition

Mit dem Begriff „IT-Personal" werden im Folgenden alle Personen bezeichnet, die mit der Administration, Wartung und Betreuung von IT-Ressourcen betraut sind.

IT-Nutzer*innen meint jede Person, die eine seitens der HfM bereitgestellte Komponente der IT-Infrastruktur (z.B. IT-Systeme, Anwendungen, Nutzerzugänge etc.) in Gebrauch hat.

„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.

Unter „sonstige schützenswerte Daten" sind alle Daten zu verstehen, die einen Informationsgehalt besitzen, unabhängig davon, ob sie analog oder digital gespeichert werden und welcher Personenkreis Zugriff erhält.

II. Einhaltung von Rechtsvorschriften

Bei der Verarbeitung von Daten sind von den IT-Nutzern*innen die geltenden Rechtsvorschriften zu IT-Sicherheit und Datenschutz sowie interne Regelungen und Anweisungen einzuhalten. Es ist untersagt, personenbezogene Daten oder sonstige schützenswerte Daten der HfM unbefugt oder unrechtmäßig zu verarbeiten. 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. Bei Unsicherheiten im Umgang mit den vorbezeichneten Regelungen sind die IT-Nutzer*innen angehalten, sich an das IT-Personal sowie ggf. an den Beauftragten für Informationssicherheit und/oder den Datenschutzbeauftragten der HfM zu wenden. IT-Nutzer*innen haben pflichtbewusst, umfassend und wahrheitsgemäß mit dem IT-Personal zu kooperieren und zu kommunizieren.

III. Allgemeine Maßnahmen des IT-Grundschutzes für IT-Nutzer*innen

In der HfM sind insbesondere – aber nicht abschließend – folgende Maßnahmen der Informationssicherheit bei der Verarbeitung von Daten zu beachten:

Hochschule für Musik
Carl Maria von Weber Dresden

1. Private Nutzung dienstlicher IT

IT-Nutzer*innen ist es untersagt, die zur Verfügung gestellte dienstliche IT in jeglicher Form privat zu nutzen. Dies betrifft insbesondere

- das Laden, Speichern und Bearbeiten privater Dokumente, Bilder, Musikdateien, Videodateien und vergleichbarer Dateiformate,
- die private Nutzung von Browsern oder sonstiger internetfähiger Software zum Abruf von Information, Daten oder Apps,
- Versand und Empfang von privaten Nachrichten, Bildern oder Videos per E-Mail, Chat, Messanger oder sonstiger Kommunikationssoftware.

Ausnahmen vom Verbot der Privatnutzung sind nur zulässig, sofern dies im Rahmen dieser Richtlinie ausdrücklich vorgesehen ist. Zudem ist es IT-Nutzer*innen untersagt, eigenmächtige Änderungen an Hard- oder Software oder Konfigurationen vorzunehmen sowie Sicherheitseinrichtungen zu umgehen.

Nicht zur Privatnutzung im Sinne dieses Abschnitts zählt die sogenannte dienstlich veranlasste Privatnutzung, etwa wenn IT-Nutzer*innen wegen kurzfristiger dienstlicher Angelegenheiten einen privaten Termin absagen.

2. Umgang mit Nutzerkennungen

Alle Rechnersysteme der HfM werden durch das IT-Personal in der Form eingerichtet, dass nur berechtigte Nutzer die Möglichkeit haben, mit ihnen zu arbeiten. Ausnahmen hiervon gelten, sofern dies mit dem IT-Personal dokumentiert abgestimmt wurde. Grundsätzlich ist zunächst eine persönliche Anmeldung mit Nutzerkennung und Passwort erforderlich. Die Vergabe von Nutzerkennungen für die Arbeit an IT-Systemen erfolgt in der Regel personenbezogen. Die Arbeit unter der Kennung einer anderen Person ist unzulässig. Den IT-Nutzer*innen ist untersagt, Kennungen und Passwörter weiterzugeben.

3. Zugriffsschutz auf dienstlichen Geräten

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. Der Zugriffsschutz muss so eingestellt sein, dass dieser automatisch nach einer angemessenen Zeit der Nichtnutzung aktiv wird.

Darüber hinaus unterliegen dienstliche Geräte der alleinigen Nutzungsbefugnis der IT-Nutzerin bzw. des IT-Nutzers, der bzw. dem das Endgerät zur Verfügung gestellt wurde. Eine Weitergabe ist – auch unter weiteren IT-Nutzer*innen innerhalb der Hochschulorganisation – nicht gestattet.

4. Räumlicher Zugangsschutz

Der unbefugte Zugang zu Geräten und die Nutzung der Informationstechnik muss verhindert werden. Bei Abwesenheit müssen die Räume der IT-Nutzer*innen mit Informationstechnologie verschlossen gehalten werden. Beim Ausdrucken derartiger Daten muss das Entnehmen der Ausdrucke durch Unbefugte verhindert werden.

Hochschule für Musik
Carl Maria von Weber Dresden

5. Passwortsicherheit

IT-Nutzer*innen sind verpflichtet ihre Passwörter geheim zu halten. Das Passwort sollte nicht notiert werden. Die Nutzung eines Passwort-Safes wird empfohlen. Sofern die technischen Gegebenheiten dies zulassen, sind Passwörter nach den folgenden Regeln zu gestalten:

- das Passwort muss mindestens 8 Stellen lang sein,
- das Passwort sollte mindestens je einen Buchstaben, eine Ziffer und ein Sonderzeichen enthalten,
- das Passwort darf nicht leicht zu erraten sein (keine Namen, Kfz-Kennzeichen, Geburtsdaten, Name von Haustieren, Adressen etc.),
- voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen durch individuelle Passwörter ersetzt werden,
- Passwörter sind bei Verdacht auf Kompromittierung zu wechseln,
- neue Passwörter müssen sich vom alten Passwort, über mehrere Wechselzyklen hinweg, signifikant unterscheiden.

Bei Vergessen des Passwortes bzw. nach mehrfacher fehlerhafter Passworteingabe sind die IT-Nutzer*innen verpflichtet, die IT-Abteilung zu informieren. Die Zahl der erlaubten Fehlversuche wird von der zuständigen Stelle festgelegt. Diese Festlegung soll verhindern, dass der Vorgang als Eindringversuch protokolliert und behandelt wird. In vielen Systemen muss das Zurücksetzen des Passworts durch das IT-Personal veranlasst werden.

Bei Verlust oder Verdacht auf Kompromittierung des Passwortes ist das IT-Personal unverzüglich zu informieren.

6. Kontrollierter Software- und Anwendungseinsatz

Auf Rechnersystemen der HfM dürfen zum Schutz hochschuleigener Hardware und des Hochschulnetzes 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 des IT-Personals 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 dem IT-Personal zu erfolgen.

Die private Nutzung der für dienstliche Zwecke erworbenen Software ist generell untersagt. Ausnahmen sind nur zulässig, sofern diese Nutzungsform den Lizenzbestimmungen nicht widerspricht und seitens der HfM Dresden die Privatnutzung erlaubt wurde.

Für die dienstliche Nutzung ist das Speichern von Dokumenten und aktuell verwendeten Bilddateien zulässig. Nicht aktuell verwendete Bilddateien sind in sog. Bildarchive zu ordnen. Das Speichern von Video- und Musikdateien auf den Netzlaufwerken der HfM ist untersagt, weil sonst wichtige Funktionen (z.B. gelöschte Dateien wiederherstellen) im Netzwerk aufgrund von Speicherplatzengpässen beeinträchtigt sind. Das Speichern von Bilderarchiven, Video- und Musikdateien kann nach Bedarf und Rücksprache mit dem IT-Personal auf anderen Speichermedien oder -plätzen erfolgen.

7. Einsatz privater Hard- und Software

Der Einsatz von privater Hard- und Software ist nur im WLAN erlaubt. Im internen Verwaltungsnetzwerk ist es dagegen explizit untersagt, private Hard- oder Software in Verbindung mit technischen Einrichtungen der HfM zu betreiben. Die Nutzung privater Endgeräte sowie Peripherie im LAN-Bereich der HfM (u.a. Laptops, Smartphones, Tablets, USB-Sticks) ist unzulässig.

Hochschule für Musik
Carl Maria von Weber Dresden

In besonders geschützten Bereichen und im Umgang mit personenbezogenen und sonstigen schützenswerten Daten ist die Benutzung von privater Hard- und Software in Verbindung mit technischen Einrichtungen der Hochschule und deren Netzen stets unzulässig.

8. Netzzugänge

Der Anschluss von Systemen an das Datennetz der HfM hat ausschließlich über die dafür vorgesehene Infrastruktur zu erfolgen. Die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen (Modems, Access-Points o. ä.) ist unzulässig. Ausnahmen dürfen nur durch das IT-Personal mit dem Beauftragten für Informationssicherheit und ggf. mit dem Datenschutzbeauftragten eingerichtet werden. Ein Zugriff von außerhalb auf die HfM IT-Infrastruktur soll grundsätzlich mittels VPN erfolgen. Die Zugänge hierfür werden durch das IT-Personal verwaltet.

9. Nutzung von E-Mail- und Internetdiensten

Soweit nicht ausdrücklich die Zustimmung der HfM erfolgt ist, darf die Nutzung von Internetdiensten 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 ist für IT-Nutzer*innen (hier Mitarbeiter, Professor*innen und Lehrbeauftragte) untersagt. Dies gilt auch für studentische/wissenschaftliche Hilfskräfte und sonstige Beschäftigte der HfM Dresden. Die E-Mail-Adresse wird von der HfM 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. Alle anderen E-Mails und Anhänge dürfen von IT-Nutzer*innen nicht geöffnet werden. Im Bedarfsfall ist mit dem Absender telefonisch Rücksprache zu halten. Bei Zweifelsfällen ist das IT-Personal zu informieren.

10. Nutzung externer Clouddienste

Die Nutzung externer Clouddienste ist nur im Umfang der durch die Ziffern 5 bis 8 dieser Richtlinie definierten Vorgaben zulässig. Der Einsatz privater Clouddienste ist stets unzulässig. Hierzu zählt insbesondere der Einsatz von Diensten wie Dropbox, WeTransfer, Google Drive/Google Fotos, Amazon Drive/Amazon Photos o.ä.

Falls Cloud-Dienste von externen Providern zum Einsatz gebracht werden sollen, ist zwingend vorherige Rücksprache mit der IT-Abteilung erforderlich. Der eigenmächtige Einsatz von Cloud-Diensten ist unzulässig.

11. Grundsätze der 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 HfM gespeicherten Daten überein, wird regelmäßig keine Veranlassung bestehen, an der Identität des Anfragenden zu zweifeln. Bei nicht eindeutig

Hochschule für Musik
Carl Maria von Weber Dresden

identifizierten Kommunikationspartnern (z.B. Abweichung zwischen aktueller und bisheriger Mailadresse) erfolgt nur eine schriftliche Auskunft an die in den Systemen der HfM hinterlegte Adresse.

Das zentrale Merkmal von Angriffen in diesem Bereich besteht in der Täuschung über Identität und Absicht des Täters. So gibt sich dieser beispielsweise als Techniker*in oder Mitarbeiter*in eines Unternehmens wie PayPal, Facebook oder eines Telekommunikationsunternehmens aus, um Anmelde- oder Kontoinformationen zu erhalten. Ein klassisches Beispiel ist der vorgebliche Systemadministrator, der Mitarbeiter*innen anruft und angeblich zur Behebung eines Systemfehlers oder Sicherheitsproblems das Passwort der Nutzer*innen benötigt.

Eine Möglichkeit der Informationsabfrage durch unberechtigte Dritte sind Abfragen via Telefon oder E-Mail. Hier wird den Kommunikationspartner*innen suggeriert, dass besondere Umstände vorlägen, eine vertrauliche Kommunikation zu führen und keine Einbeziehung weiterer Personen erfolgen dürfe. Bei ungewöhnlichen Anweisungen durch Vorgesetzte sind diese auf einem zweiten Kommunikationsweg auf Echtheit zu überprüfen. Übt die anfragende Person Druck zur Herausgabe von Daten auf IT-Nutzer*innen aus, ist im Zweifelsfall das IT-Personal zu informieren.

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

12. Umgang mit Datenträgern

Dienstliche Mobile Datenträger (Laptop, Notebook, USB-Stick, CD/DVD, externe Festplatten und Speicherkarten etc.) mit personenbezogenen und sonstigen schützenswerten Daten sind vor unbefugtem Zugriff geschützt (verschlossen) aufzubewahren. Die Daten müssen verschlüsselt werden.

***Darüber hinaus ist es untersagt dienstlich nicht zugelassene Peripheriegeräte (z.B. Ladegeräte, private Headsets sowie andere, über USB angeschlossene, technische Geräte) an die IT-Systeme der HfM anzuschließen.

13. Vernichtung von Dokumenten und Hardware gemäß rechtlicher Vorgaben

Papiere mit vertraulichem Inhalt sind mit Hilfe eines Aktenvernichters zu vernichten. Soweit die HfM Sammelbehälter/Container bereitstellt, müssen diese 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.

14. Datenschutzanforderungen in der mobilen Arbeit

Die DS-GVO und das Sächsische Datenschutzdurchführungsgesetz (SächsDSDG) 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. Insbesondere

- ist es verboten, Dritten Passwörter oder sonstige Zugangsmöglichkeiten zur dienstlichen EDV

Hochschule für Musik
Carl Maria von Weber Dresden

mitzuteilen;
- ist es verboten, Dritten (z.B. Familienmitgliedern, sonstigen Mitbewohnern, Besuchern) Zugriff auf dienstliche IT und/oder dienstliche Unterlagen zu gewähren;
- ist es verboten, den Mobilen Arbeitsplatz unbeaufsichtigt zu lassen;
- ist es verboten, dienstliche Daten auf privaten Speichermedien zu speichern;
- ist es verboten, die bereitgestellten dienstlichen Endgeräte bzw. Nutzerkennungen privat zu nutzen;
- ist es verboten, 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;
- müssen eventuelle Ausdrucke mit personenbezogenen oder sonstigen schützenswerten Daten sicher vernichtet werden, wenn sie nicht mehr benötigt werden.

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

IV. Verhalten bei Weisungen

Die IT-Nutzer*innen sind verpflichtet, den Weisungen des IT-Personals hinsichtlich der technischen Umsetzungen dieser Richtlinie Folge zu leisten. Sofern Zweifel an der Richtigkeit oder der Sinnhaftigkeit von Weisungen des IT-Personals bestehen, kann die Leitung des Dezernats IV Organisation/Liegenschaften/IT eingebunden werden.

V. Verhalten bei Informationssicherheitsvorfällen

Informationssicherheitsvorfälle können sogenannte Sicherheitsereignisse oder Sicherheitsvorfälle sein. Bei einem Sicherheitsvorfall handelt es sich um ein Ereignis, dass tatsächlich nachteilige Auswirkungen auf die Informationssicherheit hat. Hierbei ist es grundsätzlich unerheblich, ob ein Sicherheitsvorfall unbeabsichtigt oder vorsätzlich eingetreten ist. Ein Sicherheitsereignis ist ein Versuch, eines der Schutzziele (Vertraulichkeit, Integrität und Verfügbarkeit) zu verletzen.

Sicherheitsereignisse oder -vorfälle können insbesondere – aber nicht abschließend – sein:
- 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.

Stellen IT-Nutzer*innen einen Informationssicherheitsvorfall fest oder vermuten einen solchen Umstand, so ist der Vorfall unverzüglich an das IT-Personal zu melden.