Dienstanweisung zum Umgang mit Informations- und Kommunikationstechnik

Dienstanweisung - Beschäftigte

der Hochschule Wismar

University of Applied Sciences: Technology, Business and Design

vom 04. November 2024

Präambel

Die Hochschule Wismar erlässt folgende Dienstanweisung.

1. Die Dienstanweisung regelt die Rechte und Pflichten im Umgang mit der Informations- und Kommunikationstechnik an der Hochschule Wismar mit dem Ziel die IT-Sicherheit zu erhöhen und Daten zu schützen. Im Zusammenhang mit der Nutzung von Informations- und Kommunikationstechnik versteht man
   a) alle dienstlichen elektronischen Endgeräte, deren Zubehör (nachfolgend „Dienstgeräte“) und die darauf installierte Software sowie
   b) den Umgang mit dienstlichen Daten und Informationen an sich.

2. Alle Anforderungen leiten sich aus der Informationssicherheitsleitlinie der Hochschule Wismar ab und bilden die Basis für konkrete Vorgaben und Arbeitsanweisungen zur Gewährleistung der Integrität, Vertraulichkeit und Verfügbarkeit von Daten.

§ 1 Geltungsbereich

Diese Dienstanweisung gilt für alle Beschäftigten der Hochschule Wismar.

Die Dienstanweisung wird aufgrund unterschiedlicher Anforderungen zwischen Verwaltung sowie Lehre und Forschung differenziert und orientiert sich am Organigramm der Hochschule:

a) Die Verwaltung umfasst alle dem Rektorat unterstellten Organisationseinheiten inkl. der Verwaltungsbereiche der Fakultäten.
b) Die Lehre umfasst sämtliche Lehr- und Forschungsbereiche der Fakultäten. Dazu zählen auch Werkstätten und Labore in den Fakultäten.

§ 2 Pflichten der Beschäftigten

(1) Jeder Beschäftigte ist verpflichtet, durch sein Verhalten den reibungslosen Ablauf des Geschäftsbetriebs zu gewährleisten und sein Handeln entsprechend dem Schutz der Daten- und der Informationssicherheit auszurichten.
(2) Die Systeme und IT-Dienste der Hochschule stehen den Beschäftigten als Arbeitsmittel im Rahmen der dienstlichen Aufgabenerfüllung zur Verfügung.
(3) Mit hochschuleigenen Geräten ist stets pfleglich und sorgsam umzugehen.
(4) Existierende Lizenzbestimmungen sind zu befolgen und dürfen nicht umgangen werden. Etwaige Fragestellungen sind über die IT-Mitarbeiter zu klären.
(5) Bei geplanten Einführungen von IT-gestützten Systemen sind die zentralen IT-Mitarbeiterinnen und IT-Mitarbeiter (ITSMZ und/oder Fakultäts-IT) vor Eingehen von Verpflichtungen oder Verträgen zwingend zu involvieren

Für die Verwaltung gilt weiterhin:

(6) Das Einbinden von nicht hochschuleigenen Geräten und Speichermedien, wie private Hardware und Software, in die zugehörigen Netzbereiche der Verwaltung ist grundsätzlich untersagt.
(7) Wesentliche Änderungen an Systemeinstellungen (Installation, Deinstallation, Deaktivieren von Diensten oder Schutzmaßnahmen) werden untersagt. Sofern ein

Bedarf besteht, ist dieser in Abstimmung mit dem zuständigen IT-Mitarbeitern vorzunehmen.

Für die Lehre und Forschung gilt:

(8) Das Einbinden von nicht hochschuleigenen Geräten ist nur nach Freigabe durch die zuständigen IT-Mitarbeiter erlaubt (unbedenklich sind öffentliche Netzbereiche wie das hochschulweite WLAN Eduroam oder dafür vorgesehene und speziell abgesicherte Netzbereiche, z.B. in Form von Gäste- oder Labornetzen).

§ 3 Handhabung am Arbeitsplatz

(1) IT-Systeme sind möglichst so aufzustellen, dass nur die jeweils befugten Mitarbeiter die Bildschirminhalte einsehen können.
(2) Der Arbeitsplatz ist so zu gestalten, dass Unbefugten kein Zugriff auf vertrauliche Informationen inkl. personenbezogene Daten und IT-Systeme möglich wird.
(3) Beim Verlassen des Computerarbeitsplatzes hat die Sperrung der Bildschirminhalte zu erfolgen. Die Entsperrung darf nur durch den jeweiligen Mitarbeiter möglich sein, bspw. über die Eingabe eines Passwortes.
(4) Es ist sicherzustellen, dass bei plötzlicher oder unerwarteter Abwesenheit die Bildschirminhalte spätestens nach 15 Minuten automatisch gesperrt werden. Wo möglich, wird dies durch die IT-Mitarbeiter technisch bereits vorgegeben.
(5) Nach der Aufgabenerfüllung hat sich jeder Mitarbeiter von der entsprechenden Anwendung bzw. vom entsprechenden IT-System abzumelden.
(6) Ist beim Verlassen des Raumes kein weiterer Mitarbeiter mehr anwesend, so ist der Raum zu verschließen.
(7) Die Computerarbeitsplätze sind in Abhängigkeit von der Arbeitsaufgabe, am Ende des Tages und bei längerer Abwesenheit herunterzufahren.

§ 4 Telefon- und Datennutzung bei Dienstgeräten

(1) Dienstliche Gespräche sind zur Sicherstellung der Vertraulichkeit und Integrität nach Möglichkeit über die bereitgestellte zentrale Telefonie der Hochschule zu führen, im Speziellen, wenn sensible Informationen ausgetauscht werden.
(2) Die Nutzung der Diensttelefone für private Gespräche ist grundsätzlich untersagt.
(3) Vertrauliche Inhalte dürfen nicht auf Anrufbeantworter gesprochen werden.

§ 5 Druck- und Kopiersysteme

Die Hochschule Wismar setzt auf eine zentral verwaltete, campusweite Drucklösung, welche neben funktionellen Mehrwerten auch dem Datenschutz und der Datensicherheit gerecht wird. Daraus ergeben sich folgende Regelungen:

(1) Für Druck-, Kopier- und Scan-Anforderungen ist die hochschulweite Campusprint-Lösung zu nutzen.
(2) Der Einsatz lokaler oder nicht zentral verwalteter Drucker oder Multifunktionsgeräte ist zu vermeiden.
(3) Der Einsatz lokaler oder nicht zentral verwalteter Drucker oder Multifunktionsgeräte ist nur im begründeten Ausnahmefall zulässig und hat in Abstimmung mit den IT-Mitarbeitern zu erfolgen.

§ 6 Nutzung mobiler Dienstgeräte

(1) Nutzung mobiler Dienstgeräte

Die Hochschule Wismar stellt ihren Mitarbeitern bei dienstlichem Bedarf mobile Endgeräte zur Verfügung. Zu diesen gehören u.a. Smartphones, Tablets und Laptops. Für deren Einsatz gilt:

a) Die personengebundenen, mobilen Endgeräte der Hochschule Wismar sind stets sicher zu verwahren und nicht an Dritte zu verleihen oder weiterzugeben.
b) Bei Weitergabe oder Verleih nicht-personengebundener IT-Geräte hat dies über die IT-Mitarbeiter zu erfolgen. Hierbei ist sicherzustellen, dass bei einer Weitergabe der Datenschutz- als auch die Datensicherheit gewährleistet ist und keine Kompromittierung des Systems vorliegt.
c) Der geschäftliche Bereich lokaler Datenspeicher bei Laptops, Tablet oder auch Smartphone ist gegen Datenverlust bspw. durch Verlorengehen oder Diebstahl abzusichern. Der Einsatz adäquater (Verschlüsselungs-) Technologien, insbesondere in sensiblen Bereichen, ist mit den IT-Mitarbeitern vom Rechenzentrum und den Fakultäten abzustimmen und umzusetzen.
d) Es ist sicherzustellen, dass auch auf mobilen Endgeräten aktuelle Sicherheitsupdates zeitnah eingespielt werden.
e) Dienstliche SIM-Karten sind nicht in private Geräte zu integrieren.
f) Mobile Geräte müssen mit einer Zugriffssperre, bspw. einer Benutzeranmeldung oder einem Zugriffscode versehen sein. Dieser ist geheim zu halten.

(2) Nutzung mobiler Dienstgeräte von unterwegs

a) Die Nutzung von mobilen Endgeräten in der Öffentlichkeit hat entsprechend diskret zu erfolgen. Fremde dürfen keine sensiblen oder vertraulichen Informationen auf den Bildschirmen mitlesen. Eine Blickschutzfolie kann verwendet werden, um den Blickwinkel auf den Bildschirm stark einzuschränken.
b) Vertrauliche Informationen sollten nicht per Telefon in der Öffentlichkeit ausgetauscht werden.
c) Die Nutzung von mobilen Endgeräten in ausländischen Kommunikationsnetzen kann hohe Kosten verursachen und zusätzliche Sicherheitsmaßnahmen erfordern. Deshalb sollte die geplante Nutzung im Ausland frühzeitig mit den internen IT-Mitarbeitern abgestimmt werden.
d) Beim Zugriff mobiler Endgeräte auf das Hochschulnetzwerk ist generell immer eine dem Stand der Technik ausreichend stark verschlüsselte Verbindung zu nutzen.
e) Alle mobilen Endgeräte sind möglichst vor Diebstahl zu sichern (z.B. mit einem Kensington-Schloss, verschlüsselte Festplatte). Auch in Hotelzimmern sollten mobile IT-Systeme nicht ungeschützt ausliegen. In Kraftfahrzeugen sind mobile IT-Systeme so zu verstauen, dass sie von außen nicht sichtbar sind. Generell sollten mobile IT-Systeme möglichst nicht unbeaufsichtigt bleiben.
f) Der Verlust von mobilen Endgeräten ist den IT-Mitarbeitern umgehend zu melden.
g) Sollten auf Reisen Datenträger anfallen, welche entsorgt werden müssen, so sind diese wieder mitzubringen und in der Institution fachgerecht entsorgen zu lassen.

§ 7 Externer Zugriff auf die Netzbereiche der Hochschule

Die Hochschule Wismar ermöglicht ihren Beschäftigten mobile Arbeit. Regelungen und Dienstanweisungen in diesem Zusammenhang sind zu beachten und anzuwenden. Weiterhin gilt:

(1) Der Zugriff auf Dienste und Netzbereiche der Hochschule hat ausschließlich über verschlüsselte Verbindungen zu erfolgen.
(2) Der Zugriff von außen ist beim Vorgesetzten zu beantragen und über diesen den IT-Mitarbeitern zu übermitteln.
(3) Für die Lehre ist der Zugang bei den zuständigen IT-Mitarbeitern der Fakultäten zu beantragen und durch diese umzusetzen.
(4) Die Bereitstellung des Zugangs obliegt ausschließlich den IT-Mitarbeitern. Die eigenständige Einrichtung eines Zugangs über etwaige Lösungen (z.B. TeamViewer o.ä.) ist untersagt.

§ 8 Sonstige Remotezugriffe

(1) Die Nutzung jeglicher Fernsteuerungssoftware (z.B. TeamViewer, Anydesk o.ä.), um auf Geräte innerhalb der Netzbereiche der Hochschule Wismar und/oder dienstliche Computerarbeitsplätze bzw. auf mobile Dienstgeräte zuzugreifen, ist nur in Abstimmung mit den IT-Mitarbeitern gestattet. Entsprechende Softwarelösungen dürfen zudem nur dann zum Einsatz kommen, wenn diese nicht dauerhaft aktiv sind und eine technische Zustimmung vor dem Zugriff erforderlich ist.
(2) Dritten darf kein dauerhafter oder unbeaufsichtigter Remotezugriff auf die Systeme der Hochschule gewährt werden. Ausnahmen sind über autorisierte IT-Mitarbeiter zu beantragen.

§ 9 Nutzung von IT-Systemen und IT-Diensten an der Hochschule Wismar

Nachfolgende Regelungen gelten für alle IT-Systeme und IT-Dienste der Hochschule Wismar.

(1) Alle bereitgestellten Systeme und Dienste werden im Rahmen der Erfüllung der dienstlichen Aufgaben zur Verfügung gestellt.
(2) Eine private Nutzung dienstlicher Systeme ist grundsätzlich untersagt. Dies beinhaltet auch das Speichern privater Daten auf den zentralen Speichermedien der Hochschule Wismar.
(3) Die Nutzung dienstlicher Arbeitsgeräte im Kontext mit einem dienstlichen Verhältnis zur WINGS GmbH wird geduldet.
(4) Die Bereitstellung und der Betrieb von IT-Systemen oder IT-Diensten hat durch oder in Absprache mit zuständigen IT-Mitarbeitern zu erfolgen. Das eigenständige Einbinden privater oder dienstlicher Systeme, Hard- als auch Software, ist grundsätzlich untersagt.

§ 10 Passwort Regelungen

Grundsätzlich gilt, dass der Zugriff auf IT-Systeme und Anwendungen durch Einsatz einer Zugriffskontrolle, i.d.R. ein Passwort, abzusichern ist. Hierbei gelten folgende Regelungen:

(1) Passwörter dürfen nicht mehrfach verwendet werden. Für jedes IT-System bzw. jede Anwendung muss ein eigenständiges Passwort verwendet werden, sofern die Anmeldung nicht über die zentralen Authentifizierungsdienste der Hochschule Wismar (z. B. Shibboleth, LDAP, Windows Active Directory) bereits vorgegeben wird.
(2) Passwörter sind so zu wählen, dass diese nicht leicht erraten werden können und müssen mindestens folgender Komplexität entsprechen:

- Minimale Kennwortlänge: 8 Zeichen
- Komplexität: mindestens 3 von 4 Kategorien
    - Großbuchstaben
    - Kleinbuchstaben
    - Zahl
    - Sonderzeichen

(3) Nach Erhalt der zentralen Nutzerkennung der Hochschule Wismar muss das initial vergebene Passwort umgehend geändert werden.
(4) Grundsätzlich müssen initial vergebene Passwörter immer geändert werden.
(5) Passwörter müssen geheim gehalten werden und dürfen nur dem Benutzer persönlich bekannt sein. Dies betrifft auch andere Authentifizierungsmittel (bspw. PIN oder Token). Eine Weitergabe an Dritte ist nicht erlaubt.
Es wird ausdrücklich darauf hingewiesen, dass jegliche Aktivität (auch unzulässige durch Dritte) dem Nutzer zugeschrieben werden kann, dessen Kennung verwendet wurde.
(6) Dienstliche Kennwörter dürfen nicht im privaten Umfeld verwendet werden.
(7) Die Passworteingabe hat unbeobachtet zu erfolgen.
(8) Nutzer dürfen sich nur unter der eigenen Benutzerkennung anmelden und diese für ihre Arbeit an den IT-Systemen verwenden.
(9) Passwörter dürfen nicht auf programmierbaren Funktionstasten von Tastaturen oder Mäusen gespeichert werden.
(10) Ein Passwort darf nur für einen Notfall schriftlich fixiert werden und auch nur, wenn eine sichere Aufbewahrung sichergestellt werden kann.
(11) Ein Passwort muss gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.
(12) Bei der Verwendung von Gruppenpasswörtern, welches einem definierten Personenkreis bekannt ist, ist dieses zu ändern, wenn sich die Personenzugehörigkeit der Gruppe bspw. durch Ausscheiden ändert.
(13) Passwörter dürfen in digitaler Form nicht unverschlüsselt gespeichert werden.
(14) Passwörter dürfen nur dann im Browser gespeichert werden, wenn sichergestellt ist, dass diese dort in einer sicheren Verschlüsselung vorliegen und durch ein Master Passwort der Zugriff auf diese zusätzlich geschützt ist.
(15) Der Einsatz von Passwort Managern wird grundsätzlich empfohlen. Beim Einsatz geeigneter Lösungen sind die IT-Mitarbeiter zu befragen.
(16) Dateien, die der Aufbewahrung von Passwörtern dienen, dürfen nicht über externe Datenträger oder per E-Mail transferiert werden, sofern diese nicht zusätzlich verschlüsselt sind.
(17) Dienstliche Passwörter dürfen auf nicht dienstlichen Geräten nicht gespeichert werden. Das betrifft auch und insbesondere das Speichern von Passwörtern im Browser. Als Ausnahme wird hier ausschließlich die Einrichtung des dienstlichen E-Mail-Zugangs auf einem privaten Smartphone oder Tablet geduldet. Dies wird zwar kritisch bewertet, soll aber die flexible Nutzung, vor allem in Bezug auf die mobile

Arbeit, erhalten. Der Zugriff auf das private Smartphone oder Tablet ist dabei zwingend durch einen zusätzlichen Zugriffsschutz abzusichern.

(18) Bei der dienstlichen Nutzung öffentlicher, nicht durch die Hochschule betriebener oder angebundener (Cloud)-Dienste, darf nicht das zentrale Hochschulkennwort verwendet werden.

§ 11 Datennutzung, Datenspeicherung, Datenträger und mobile Datenträger

1. Daten, Datenspeicherung und Datenträger

   a) Die unbefugte Weitergabe von Daten an Dritte ist ausdrücklich untersagt.
   b) Die Verarbeitung personenbezogener Daten ist durch Dritte nur im Rahmen einer Auftragsvereinbarung gestattet.
   c) Dienstliche Inhalte außerhalb der Anwendungen und Fachverfahren sind auf den jeweiligen, zentral zur Verfügung gestellten Speicherbereichen (z.Bsp. Netzlaufwerke, Campus Cloud) der Hochschule Wismar zu speichern.
   d) Auf den lokalen Laufwerken der Computerarbeitsplätze sollten dienstliche Inhalte nur temporär gespeichert werden, da sie lediglich eine unterstützende Funktion haben und nur im Ausnahmefall eine Datensicherung gewährleistet ist.
   e) Die Nutzung von externen oder privaten Cloud-Diensten oder Online-Speichern ist untersagt, sofern diese nicht expliziter Bestandteil einer durch die IT-Mitarbeiter autorisierte Lösung sind. Weiterhin gilt als Ausnahme, dass bei notwendiger, dienstlicher Nutzung externer, nicht durch die Hochschule betriebener oder angebundener (Cloud)-Dienste, das Speichern von Daten (u. a. das Speichern von Daten aus (Verbund-) Forschungsprojekten oder kooperativen Promotionen) gestattet ist, sofern die Arbeitsfähigkeit sonst nicht gegeben ist. Handelt es sich um sensible und/oder besonders schutzbedürftige Daten, müssen diese, nach aktuellem Stand der Technik, verschlüsselt werden.
   f) Das Speichern dienstlicher Inhalte auf privaten Geräten ist untersagt. Dies betrifft insbesondere personenbezogene oder schutzbedürftiger Daten. Das temporäre Speichern nicht schutzbedürftiger Daten auf einem privaten Smartphone wird kritisch bewertet, aber als Ausnahme geduldet. Für die Lehre und Forschung gilt, dass weitere Ausnahmen, z. B. die Nutzung eines privaten Tablets, nur in Abstimmung mit den zuständigen IT-Mitarbeitern gestattet ist.
   g) Die Übertragung von sensiblen, schutzwürdigen und insbesondere von personenbezogenen Daten (z.B. mittels E-Mail) über das Internet ist zur Wahrung der Vertraulichkeit und zur Einhaltung des Datenschutzes ausschließlich in verschlüsselter Form zulässig.
   h) Die fachgerechte Entsorgung physikalischer Datenträger ist über die IT-Mitarbeiter zu organisieren.

2. Mobile Datenträger

   a) Der Einsatz von mobilen dienstlichen Datenträgern (u.a. CD-ROMs, DVDs, USB-Festplatten und auch Flash-Speicher wie z. B. USB-Sticks oder Speicherkarten) ist nach Möglichkeit zu vermeiden.
   b) Die Ein- und Ausgabe von Daten über externe Speichermedien und deren Transport außerhalb der Hochschule Wismar ist nur unter entsprechenden Schutzmaß-nahmen vorzunehmen:

      - Abhängig vom Schutzbedarf der zu transportierenden Informationen ist eine geeignete Versandart festzulegen

- der Transport von Datenträgern mit vertraulichem bzw. personenbezogenem Inhalt hat ausschließlich in verschlüsselter Form zu erfolgen

c) Vor dem Öffnen der Daten eines Speichermediums ist dieses mit einem Antivirenprogramm auf Schadsoftware zu prüfen.

§ 12 Internetzugang und E-Mail-Nutzung

1. Internetzugang

a) Der durch die Hochschule bereitgestellte Internetzugang steht den Beschäftigten als Arbeitsmittel im Rahmen ihrer dienstlichen Aufgabenerfüllung zu dienstlichen Zwecken zur Verfügung.
b) Die private Nutzung des dienstlichen Internetzugangs ist in geringfügigem Umfang außerhalb der Arbeitszeiten gestattet. Es muss in dem Falle bewusst sein, dass auch diese Nutzung der automatischen Protokollierung unterliegt und bei sporadischer Sichtung der Logfiles (z.B. Fehleranalyse) diese Daten sichtbar und ausgewertet werden können.
c) Unzulässig ist jede bewusste Internetnutzung, die geeignet erscheint, den Interessen der Hochschule Wismar oder deren Ansehen in der Öffentlichkeit zu schaden, oder die gegen geltendes Recht verstößt, wie beispielsweise:

- das Abrufen und/oder Anbieten von Inhalten, die gegen datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
- das Abrufen und/oder Anbieten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen oder pornographischen Äußerungen oder Abbildungen oder
- das Abrufen von Internetinformationen bei bekannter Deaktivierung von lokalen Sicherheitsmechanismen (z. B. Firewall oder Virenschutzprogramm).

d) Soziale Medien dürfen ausschließlich zur dienstlichen Aufgabenerfüllung genutzt werden.

2. E-Mail-Nutzung

a) Elektronische Post ist als Kommunikationsmittel zur Beschleunigung und Vereinfachung von Vorgängen vorrangig gegenüber der Briefpost zu nutzen, soweit dem keine technischen, rechtlichen oder wirtschaftlichen Gründe entgegenstehen. Auf den parallelen Versand von Papierdokumenten ist zu verzichten.
b) Die Postfächer sind mindestens einmal arbeitstäglich (inklusive Spam-Ordner) zu sichten. Bei Dienstreisen, wo Internetzugang nicht möglich ist oder das Dienstgeschäft es nicht zulässt (Konferenzen, Exkursionen), sollte es dennoch möglich sein nach 3 Tagen das Postfach zu sichten. Beschäftigte werden bei Krankheit oder in der Urlaubszeit von dieser Regelung ausgeschlossen.
c) E-Mails mit sensiblen und schutzwürdigen Informationen dürfen nicht ohne zusätzliche Sicherungsmaßnahmen, z.B. passwortgeschützte ZIP-Datei versandt werden. Das Kennwort ist auf dem zweiten Kommunikationsweg zuzustellen.

d) Der Sender hat vor Absenden der E-Mail die Korrektheit der Empfänger-Adressen zu prüfen um zu verhindern, dass sensible Informationen an falsche Personen versendet werden.
e) Für die dienstliche Kommunikation ist ausschließlich die dienstliche E-Mail-Adresse der Hochschule Wismar zu nutzen. Das Weiterleiten an externe E-Mail-Dienste ist nicht gestattet.
f) Die Nutzung des E-Mail-Dienstes ist grundsätzlich nur für den Dienstgebrauch zugelassen. Zum Umstellen der privaten Kommunikation wird eine Übergangszeit von 6 Monaten gegeben.
g) Die Mitarbeiter wirken, soweit es in deren Einflussbereich liegt, darauf hin, dass die dienstliche E-Mail-Adresse von Dritten nicht für private Kommunikation genutzt wird.
h) Bei einem Empfang rein privater E-Mails auf dem dienstlichen E-Mail-Konto sind diese unverzüglich von dort zu entfernen. Der Beschäftigte hat das Recht, diese privaten E-Mails im Bedarfsfall zuvor auf ein privates E-Mail-Konto weiterzuleiten.
i) Eine Nutzung privater Mail-Dienste ist für dienstliche Zwecke nicht gestattet.
j) Das Speichern dienstlicher E-Mails auf privaten Geräten ist untersagt. Lediglich die unter §11 Absatz 1 Punkt f formulierte Ausnahme wird geduldet.
k) Beim Versand von E-Mails sollte die persönliche digitale zertifikatsbasierte Signatur verwendet werden. Dies ermöglicht dem Empfänger die Herkunft der E-Mail eindeutig festzustellen.
l) Weiterhin gelten die Verhaltensregeln in §14 zum Schutz vor Schadprogrammen.
m) Falsch zugestellte E-Mails sind, wenn die zuständige Empfangsstelle zweifelsfrei erkennbar ist, an diese in geeigneter Form weiterzuleiten. Anschließend sind die E-Mails zu löschen.
n) Die dienstliche E-Mailadresse darf nicht zur Registrierung für privat genutzte Dienste verwendet werden. Sollte dies in der Vergangenheit erfolgt sein und noch Bestand haben, ist dies umgehend aufzulösen.

§ 13 Abwesenheits- und Vertreterregelung

(1) In den Bereichen ist zu organisieren, dass (zeit-) kritische elektronische Post auch bei geplanter oder ungeplanter Abwesenheit zeitnah bearbeitet wird. Das kann bspw. durch Freigaben oder Vertreterregelungen geschehen.
(2) Das Einrichten automatisierter Abwesenheitsnachrichten gegenüber Externen sollte mit Sorgfalt angegeben werden und nur wenn eine entsprechende interne organisatorische Handhabung nicht möglich ist. Diese Meldungen sind so zu gestalten, dass möglichst wenig interne Informationen an Dritte übermittelt werden.
Die interne Nutzung von Abwesenheitsnachrichten wird hingegen als unkritisch eingeschätzt.
(3) Für nicht vorhersehbare Abwesenheit und das Fehlen von benötigten Vertreterregelungen kann in dringenden Fällen durch Vorgesetzte die Einsicht in das Benutzerpostfach über das ITSMZ beantragt und vorgenommen werden. Die Beantragung und Einsichtnahme sind zu protokollieren und müssen durch den zuständigen Personalrat begleitet werden. Nach Rückkehr des Beschäftigten ist dieser unverzüglich über diesen Schritt zu informieren.
(4) Die Einsicht in Funktionspostfächer der Interessenvertretungen (SBV, Gleichstellung, Personalräte) sind grundsätzlich von dieser Regelung ausgenommen. Gegebenenfalls ist der Zugriff nur bei Anwesenheit eines anderen Mitgliedes der entsprechenden Vertretung erlaubt!

§ 14 Schutz vor Schadprogrammen

Die Benutzer tragen dafür Verantwortung, die IT-Systeme so zu nutzen, dass eine Infektion mit Schadprogrammen vermieden wird. Dies heißt im Einzelnen:

(1) Verdächtige Dateien dürfen nicht selbstständig geöffnet werden. In Zweifelsfällen sind die IT-Mitarbeiter zu konsultieren.
(2) IT-Systeme sollten sorgfältig hinsichtlich möglicher Gefahren beobachtet werden.
(3) Eingehende und ausgehende Dateien sind im Falle eines Datenträgeraustauschs durch eine Antivirensoftware zu prüfen.
(4) E-Mails und insbesondere E-Mails mit Anhängen sind vor dem Öffnen letzterer auf ihre Plausibilität zu prüfen.
(5) Durch die IT-Mitarbeiter installierten Virenschutzprogramme dürfen nicht deaktiviert, deinstalliert oder in ihrer Konfiguration verändert werden.
(6) Es dürfen nur IT-Systeme betrieben werden, für die aktuelle Sicherheitsupdates bereitgestellt werden. Zudem ist sicherzustellen, dass diese Updates, je nach Kritikalität, sehr zeitnah eingespielt werden. Dies betrifft auch mobile Endgeräte. Etwaige Ausnahmen sind zwingend mit den IT-Mitarbeitern abzustimmen.
(7) Jeder Verdacht auf einen Befall mit Schadsoftware muss sofort den IT-Mitarbeitern gemeldet werden.

Für die Verwaltung gilt weiterhin:

(8) Das selbstständige Einbringen von nicht durch die IT-Mitarbeiter freigegebene Software in zugehörige Netzwerkbereiche ist untersagt.

Bei Anzeichen eines Befalls mit Schadsoftware muss das betroffene IT-System umgehend vom Netzwerk (LAN/WLAN) getrennt werden. Dies vermindert das Risiko einer Ausbreitung auf benachbarte Systeme im Netzwerk.
Das System ist in unverändertem Zustand zu belassen und zur weiteren Analyse umgehend dem zuständigen IT-Mitarbeiter zu melden.

Anzeichen für einen Befall mit Schadsoftware können sein:

- häufige Programmabstürze
- Programmdateien werden größer
- unerklärliches Systemverhalten
- unerklärliche System-Fehlermeldungen
- Nutzung unbekannter Dienste
- nicht auffindbare Dateien
- veränderte Dateiinhalte
- ständige Verringerung des freien Speicherplatzes, ohne dass etwas abgespeichert wurde.

§ 15 Meldepflichten

(1) Neben der Feststellung oder des Verdachts auf einen Befall von Schadsoftware sind nachfolgende Vorfälle zwingend und schnellstmöglich gegenüber den IT-Mitarbeitern anzuzeigen:
   a) Relevante Ereignisse, wie z. B. ungewöhnliches Systemverhalten, jeglicher Verlust von Daten oder Programmen, Verdacht auf Viren und nicht autorisierte Zugriffe
   b) Der Verlust von IT-Komponenten, Speichermedien, mobilen Endgeräten oder ähnlichem.
   c) Der Verlust eines Mobiltelefons bzw. einer SIM-Karte ist zusätzlich sofort dem Netzbetreiber zu melden, um eine Kartensperre zu veranlassen.

§ 16 Filter, Protokollierung und Kontrolle

(1) Jeder Datenverkehr zwischen den lokalen Netzen der Hochschule sowie dem Internet unterliegt einer automatischen Protokollierung.
(2) Die Hochschule ist berechtigt den dienstlich bereitgestellten E-Mail- und Internetzugang durch Einsatz von Filtersystemen zu beschränken (z.B. Sperren bestimmter Adressen oder Dateitypen, Domains, URLs, Dienste / Protokolle, Filesharing, Streaming, Ports) sowie Spam- und Virenfiltern einzusetzen.
(3) Die Nutzung des E-Mail- und Internetzugangs wird aus Gründen der Daten- und Systemsicherheit und zur Fehleridentifikation ebenfalls protokolliert und gespeichert.
   (a) Eine Unterscheidung zwischen privater und dienstlicher Nutzung ist aus technischen Gründen nicht möglich. Die Protokollierung erfolgt insbesondere mit Datum / Uhrzeit, genutztem Dienst (z.B. E-Mail, HTTP), Daten von Absender und Empfänger (z.B. IP-Adressen, Namen der Rechner, E-Mail-Adressen), gegebenenfalls Benutzerdaten (z.B. Benutzername mit E-Mail-Versand oder bei Einsatz eines Proxy-Servers), gegebenenfalls URLs der aufgerufenen Websites, technischer Statuscodes und übertragener Datenmenge.
   (b) Die Protokolle werden entsprechend der jeweiligen Löschkonzepte (spätestens nach 12 Monaten) gelöscht, soweit nicht eine längere Speicherung im Einzelfall aus Gründen der Daten- und Systemsicherheit oder zur Fehleridentifikation und -behebung erforderlich ist.
   (c) Die Protokolle werden durch die IT-Abteilung regelmäßig stichprobenhaft gesichtet und ausschließlich zu Zwecken der Gewährleistung / Wiederherstellung der Systemsicherheit, Analyse und Korrektur technischer Fehler und Störungen, Kapazitätsplanung und Lastverteilung sowie Optimierung der IT-Infrastruktur, statistischer Feststellung des Nutzungsumfangs, Missbrauchskontrolle und -verfolgung sowie bei Verdacht einer Straftat verwendet. Bei Bedarf werden die Protokolldaten an den Datenschutzbeauftragten und die Hochschulleitung weitergegeben.
(4) Der Zugriff auf die Protokolldateien zum Zwecke der Erstellung der Übersicht und der jeweiligen Auswertung ist auf einen dienstlich beauftragten Personenkreis beschränkt.

Jedwede Überwachung zu Verhaltens- und Leistungskontrolle der Beschäftigten ist unzulässig.

§ 17 Regelung bei Missbrauch und Verstößen

Eine generelle personenbezogene Überwachung der Nutzung dienstlicher Endgeräte, einschließlich der Telefon- und Datennutzung (E-Mail und Internet) findet nicht statt.

(1) Ergibt sich aus der Auswertung von Protokolldaten Anzeichen für einen Verstoß bzw. einen Missbrauch, so sind die verantwortlichen IT-Mitarbeiter autorisiert dem nachzugehen und ggf. auch technisch entgegenzuwirken.
(2) Bei Sicherheits- und Datenschutzvorfällen ist entsprechend dem Schweregrad die Hochschulleitung sowie der/die Datenschutzbeauftragte durch das ITSMZ zu beteiligen.
(3) Ein nachweislich grober Missbrauch bzw. eine grobe Fahrlässigkeit im Sinne dieser Vereinbarung, kann neben arbeits- auch strafrechtliche Folgen haben. In solchen Fällen ist der Personalrat einzubinden.

§ 18 Haftung

(1) Im Falle des Verlustes oder der Beschädigung der dienstlichen Hard- und Software sowie Daten, die nachweislich nicht grob fahrlässige oder vorsätzliche Handlungen des Beschäftigten erleiden, haftet der Arbeitgeber nach den gesetzlichen Bestimmungen.
(2) Im Falle des Verlustes oder der Beschädigung der dienstlichen Hard- und Software sowie Daten, die durch vorsätzliche oder grob fahrlässige Handlungen des Beschäftigten selbst verursacht werden (auch soweit durch mangelnde Pflege oder Wartung sowie durch unterlassene Reparaturen entstehen), haftet der Beschäftigte ebenso selbst, wie im Zusammenhang mit der reinen privaten Nutzung.

§ 19 Rechte und Beteiligung der Personalvertretung

(1) Die Unterrichtungs- und ggf. Zustimmungspflicht bezieht sich insbesondere auf
a) die organisatorischen und personellen Auswirkungen,
b) die vorgesehenen Maßnahmen zu Datenschutz und Datensicherheit.

(2) Der Personalrat kann sich von der Einhaltung der Dienstanweisung - auch stichprobenweise - überzeugen.

§ 20 Schlussbestimmungen

(1) Verantwortlich für das in Kraft treten dieser Dienstanweisung und deren Einhaltung ist die Hochschulleitung.
(2) Die Dienstanweisung tritt mit Unterzeichnung in Kraft und läuft auf unbegrenzte Zeit.

Wismar, den 05.12.2024

Rektorat
der Hochschule Wismar
University of Applied Sciences: Technology, Business and Design