Hochschule für Technik und Wirtschaft Dresden
University of Applied Sciences

Ordnung zur Organisation, Administration und Nutzung der IT-Infrastruktur der HTW Dresden

IT-Ordnung

der Hochschule für Technik und Wirtschaft Dresden

University of Applied Sciences

Vom

08.05.2023

Auf der Grundlage von § 13 Absatz 5 Satz 1 des Sächsischen Hochschulfreiheitsgesetzes in der Fassung der Bekanntmachung vom 15. Januar 2013 (SächsGVBl. S. 3), das zuletzt durch das Gesetz vom 01. Juni 2022 (SächsGVBl. S. 381) geändert worden ist, hat die Hochschule für Technik und Wirtschaft Dresden (HTW Dresden) nachfolgende Ordnung als Satzung erlassen.

Inhaltsübersicht

Präambel

Die Hochschule für Technik und Wirtschaft Dresden (HTW Dresden) betreibt Informationstechnologien (IT) zur Nutzung in Lehre, Studium, Forschung, Aus- und Weiterbildung, der Hochschulverwaltung und weiteren für den Hochschulbetrieb notwendigen Aufgaben.

Um den hohen Anspruch einer modernen technischen Hochschule an die Qualität der IT-Infrastruktur - z.B. im Hinblick auf Verfügbarkeit, Nutzerfreundlichkeit, Reaktions- und Antwortzeiten sowie die Informationssicherheit zu gewährleisten, regelt die HTW Dresden mit dieser Ordnung die Strukturen zu Aufgaben, Verantwortung und Zusammenarbeit für den Betrieb sowie die Bedingungen für die Nutzung der IT-Infrastruktur an der HTW Dresden.

Alle Nutzerinnen und Nutzer sind zur Einhaltung der vorliegenden IT-Ordnung verpflichtet. Vorgesetzte und Lehrende tragen nach Maßgabe ihrer Möglichkeiten für die Einhaltung durch die Nutzerinnen und Nutzer Sorge. Nutzerinnen und Nutzer sind über die Einhaltung der Regeln zu belehren.

§ 1 Geltungsbereich und Gegenstand der Ordnung

(1) Diese Ordnung gilt für die an der HTW Dresden betriebene IT-Infrastruktur, bestehend aus den informationstechnischen Einrichtungen, Kommunikationsnetzen, Informationsverarbeitungsanlagen, IT-Systemen und den darauf aufbauenden IT-basierten Diensten und Dienstleistungen.

(2) Diese Ordnung ist von allen Mitgliedern und Angehörigen der HTW Dresden sowie von Dritten, die IT-Infrastruktur der Hochschule betreiben oder benutzen, zu beachten.

(3) Diese Ordnung kann durch weitergehende Umsetzungsregelungen konkretisiert werden, sofern dadurch die Bestimmungen der vorliegenden Ordnung nicht verletzt werden.

§ 2 Weiterverpflichtung

Natürliche oder juristische Personen, die die IT-Infrastruktur der HTW Dresden nutzen, oder die über die IT-Infrastruktur der HTW Dresden Teilnehmende des Deutschen Forschungsnetzes des Vereins zur Förderung eines Deutschen Forschungsnetzes e. V. (DFN) sind, sind auf die Einhaltung der Bestimmung dieser Ordnung vertraglich zu verpflichten.

§ 3 Zentrale und dezentrale IT-Organisation

(1) Das Rektorat der HTW Dresden benennt eine für alle zentralen strategischen Entscheidungen zur IT-Infrastruktur der HTW Dresden zuständige Person (Chief Information Officer -CIO). Wenn keine Person benannt ist, übt der Kanzler diese Funktion aus.

(2) Das Zentrum für Informationsdienste und Digitale Transformation (ZID) ist zuständig für den Betrieb der zentralen IT-Infrastruktur sowie die IT-Infrastruktur der Verwaltung und zentralen Einrichtungen der Hochschule.

(3) Die Fakultäten der HTW Dresden können zusätzliche Server, Dienste und fachspezifische Anwendungen zur Nutzung in Lehre und Forschung in eigener Verantwortung betreiben.

(4) Mit vorheriger Zustimmung des Leiters bzw. der Leiterin des ZID ist die Errichtung und der Betrieb von managebaren aktiven Netzkomponenten und WLAN-Technik in dezentraler Zuständigkeit und Verantwortung zulässig. Den Zugang zu Datenverteilerräumen und Serverräumen bestimmt das ZID nach pflichtgemäßem Ermessen.

(5) In begründeten Ausnahmefällen, wie z.B. Personalengpässen und Nichtverfügbarkeiten etc. und unter Berücksichtigung des Schutzbedarfes der zu verarbeitenden Informationen können Dritte mit dem Betrieb oder der Betreuung der IT-Infrastruktur beauftragt werden. Beauftragungen von Dritten erfordern die vorherige Zustimmung der/des Beauftragten für Informationssicherheit.

(6) Die IT-Infrastruktur der Fakultäten, ausgenommen das Netzwerk, wird durch Administratorinnen und Administratoren verwaltet, die durch die Dekanin/den Dekan benannt und durch diese dem ZID mitgeteilt werden.

(7) Administratorinnen und Administratoren der Fakultäten sind grundsätzlich der jeweiligen Fakultät zugeordnet. Eine Zuordnung zum ZID zur Schaffung von Synergien und besseren fachlichen Einbindung verstößt nicht gegen diese Ordnung.

(8) Das Rektorat der HTW Dresden kann ein beratendes Gremium (IT-Rektoratskommission) einsetzen, dass den CIO im Rahmen ihrer/seiner Aufgaben beratend unterstützt.

§ 4 Nutzungszwecke

(1) Die Errichtung und der Betrieb der IT-Infrastruktur sowie die Zulassung zur Nutzung der IT-Infrastruktur erfolgt zum Zwecke der Erfüllung der Aufgaben der HTW Dresden, insbesondere in Lehre, Studium, Forschung, Aus- und Weiterbildung und der Hochschulverwaltung sowie weitere für den Hochschulbetrieb notwendige Aufgaben.

(2) Die Nutzung der IT-Infrastruktur für andere als im Absatz 1 genannten Zwecke ist zulässig, wenn sie geringfügig ist, die anderen Nutzerinnen und Nutzer nicht behindert oder stört, die dienstliche Aufgabenerfüllung nicht beeinträchtigt, kein strafbares Verhalten darstellt und sonstige Bestimmungen/Regelungen nicht entgegenstehen.

(3) Die IT-Infrastruktur darf nicht zur individuellen Leistungs- und Verhaltenskontrolle der Mitglieder und Angehörigen der HTW Dresden genutzt werden.

§ 5 Berechtigung zur Nutzung und Nutzerverwaltung

(1) Zur Nutzung der IT-Infrastruktur sind grundsätzlich nur Mitglieder und Angehörige der HTW Dresden (geschlossene Nutzergruppe) berechtigt.

(2) Gäste, d.h. sonstige natürliche Personen, können zeitlich begrenzt als Mitglied der geschlossenen Nutzergruppe aufgenommen werden, wenn sich diese auf die Einhaltung der Pflichten für Nutzerinnen und Nutzer verpflichtet haben.

(3) Für Nutzerinnen und Nutzer wird durch das ZID ein zentrales Benutzerkonto in elektronischer Form gebildet und verwaltet. Für Gäste, die über den WLAN-Internetzugang hinausgehende Funktionen nutzen sollen, ist die Bereitstellung eines Benutzerkontos möglich. Dies erfordert die Benennung einer Ansprechperson, die Mitglied oder Angehörige/Angehöriger der HTW Dresden ist, gegenüber dem ZID. Das Benutzerkonto umfasst insbesondere HTW-Login, Passwort und E-Mail-Adresse. HTW-Login und Passwort bilden die sogenannte Benutzerkennung.

(4) Scheidet eine Nutzerin/ein Nutzer aus, wird deren/dessen zentrales Benutzerkonto durch das ZID gesperrt und nach 6 Monaten gelöscht, soweit keine Rückkehr an die HTW Dresden zu erwarten ist. Von der Löschung sind auch die mit dem Konto verbundenen Daten betroffen. Weitere gespeicherte Daten unterliegen den Datenschutz- und Löschanforderungen des jeweiligen Zwecks bzw. speziellen Rechtsgrundlagen.

(5) Die Nutzung der IT-Infrastruktur kann vorübergehend eingeschränkt werden, z.B. durch Sperrung der Benutzerkennungen, soweit dies zur Störungsbeseitigung, zur Systemadministration und -erweiterung oder aus Gründen der Systemsicherheit, zum Schutz der nutzereigenen oder anderer Daten sowie zur Aufklärung und Unterbindung einer unzulässigen oder pflichtwidrigen Nutzung der IT-Infrastruktur erforderlich ist.

§ 6 Namenskonventionen für Endgeräte und E-Mails

(1) Alle dauerhaft an das Datennetz der HTW Dresden angeschlossenen Endgeräte erhalten einen eindeutigen Namen (Hostnamen) unterhalb der Domain „htw-dresden.de“. Das ZID verwaltet diese Domain sowie deren Subdomains.

(2) Eindeutige Hostnamen werden nach dem Schema „Hostname.Substruktur.htw-dresden.de“ gebildet. Für den Teil „Substruktur“ kann die Abkürzung der Fakultät, der Verwaltung, der Zentralen Einrichtung oder für spezifische Dienste des ZID eine passende andere Bezeichnung verwendet werden. Der Teil „Hostname“ wird nach den Schemavorgaben der HTW Dresden festgelegt. Eine weitere Unterteilung in Untereinheiten ist möglich.

(3) Für die E-Mail-Kommunikation aus der Domaine @htw-dresden.de sind E-Mail-Adressen zu verwenden, die grundsätzlich folgenden Namenskonventionen entsprechen:

a) für Beschäftigte der HTW Dresden (Beamtinnen und Beamte, Arbeitnehmerinnen und Arbeitnehmer, Auszubildende): vorname.nachname[y]@htw-dresden.de und

b) für die Studierenden: vorname.nachname[y]@stud.htw-dresden.de.

Studentische Hilfskräfte zählen zur Gruppe der Studierenden (Primärrolle). Die Verwendung von Funktions-E-Mail-Adressen ist zulässig. Die Nutzung bereits bestehender dezentraler E-Mail-Adressen ist bis zum Erlass einer anderslautenden Regelung weiterhin zulässig.

§ 7 Besondere Bestimmungen für die E-Mail-Nutzung

(1) Abzusendende E-Mails aus der Domäne @htw-dresden.de sind grundsätzlich mit einer elektronischen vom DFN-Verein organisierten PKI-Signatur zu signieren, sofern die Nutzerin/der Nutzer der Mitgliedergruppe der Mitarbeiter gemäß § 57 Abs. 2 SächsHSFG angehört.

(2) Der E-Mail-Versand von schutzwürdigen personenbezogenen Daten sowie anderer Daten mit erhöhtem Schutzbedarf darf nur verschlüsselt erfolgen.

(3) Für dienstliche Zwecke ist eine automatisierte Weiterleitung eingehender E-Mails an Postfächer außerhalb der Domäne @htw-dresden.de unzulässig. Auch das Verlangen, eine automatisierte Weiterleitung von E-Mails einzurichten, ist unzulässig.

(4) Der ein- und ausgehende E-Mail-Verkehr der HTW Dresden erfolgt über das zentrale Gateway (Mailrelay). Das ZID trifft alle erforderlichen Maßnahmen zum ordnungsgemäßen Betrieb des Mailrelay.

(5) Alle ein- und ausgehenden E-Mails mit ungültigen Absenderadressen werden automatisch abgewiesen.

(6) Für alle ein- und ausgehenden E-Mails findet eine Virenprüfung statt. Virenbehaftete E-Mails können abgewiesen werden.

(7) Jede eingehende E-Mail wird vor ihrer Weiterverarbeitung nach dem Stand der Technik auf SPAM bewertet.

§ 8 Besondere Bestimmungen für Webseiten

(1) Für die allgemeine Internetpräsentation ist grundsätzlich der Webauftritt der Hochschule über das zentrale Content Management System (CMS) Typo3 zu nutzen.

(2) Für Kooperationsprojekte mit externen Partnern sowie bei speziellen Funktionsanforderungen kann ein Webauftritt außerhalb des CMS der HTW Dresden umgesetzt werden. Die Vorgaben der HTW Dresden zum Corporate Design sowie geltende rechtliche Vorgaben (z.B. bezüglich des Impressums, zum Datenschutz und zur Barrierefreiheit) sind zu beachten. Dem Rektorat sind mindestens zwei Ansprechpersonen für den Webauftritt nebst deren Kontaktdaten zu benennen.

§ 9 Besondere Bestimmungen für die Beschaffung, Nutzung und Aussonderung von Hard- und Software sowie sonstigen IT-Diensten

(1) Die Beschaffung von Hard- und Software sowie sonstigen IT-Diensten bzw. die Produktivsetzung von für Verwaltungsaufgaben vorgesehene selbst erstellte Software oder IT-Diensten bedarf der vorherigen Zustimmung des Leiters/der Leiterin des ZID, bzw. bei dezentraler Hardware der/des Datenverarbeitungs(DV)-Beauftragen. Die Zustimmung kann insbesondere bei unzureichender Qualitätssicherung, Kompatibilität oder unrealistischem Betriebskonzept versagt werden.

(2) Die Beschaffung von Hard- und Software sowie sonstigen IT-Diensten richtet sich im Übrigen nach der Beschaffungsordnung der HTW Dresden.

(3) Für die Einrichtung und Nutzung der durch die HTW Dresden beschafften Software sind die Nutzungsbedingen/Lizenzbestimmungen des jeweiligen Lizenzgebers maßgeblich, z.B. im Hinblick auf die Anzahl der Lizenzen, Nutzungszweck, die Nutzungsdauer oder die Nutzung von akademischen Lizenzen oder Bildungslizenzen zur Verwendung für kommerzielle Projekte oder Verwaltungsaufgaben.

(4) Die Nutzung von privat erworbener Software für dienstliche Zwecke setzt die Zulässigkeit durch die Lizenzbestimmungen des jeweiligen Lizenzgebers voraus und bedarf der vorherigen Zustimmung der Beauftragten für Informationssicherheit. Die Zustimmung kann widerrufen werden.

(5) Nach Ablauf der Nutzungsfrist gemäß den Nutzungsbedingungen ist die Software zu deinstallieren.

(6) Audits über den Einsatz von Software, die beispielsweise durch den Hersteller verlangt werden, sind im Vorfeld mit der/dem Beauftragten für Informationssicherheit der HTW Dresden abzustimmen. Mit vorheriger Zustimmung der/des Beauftragten für Informationssicherheit ist die Administratorin/der Administrator berechtigt, die für die Auswertungen benötigten Angaben bereitzustellen. Die/der Vorgesetzte ist hierüber vorab zu informieren.

§ 10 Rechte und Pflichten der Administratorinnen und Administratoren

(1) Die Administratorinnen und Administratoren sind für den ihnen zugeordneten Bereich -auch mit Hilfe automatisierter Methoden- berechtigt, die Inanspruchnahme der Datenverarbeitungssysteme und Software durch die einzelnen Nutzerinnen und Nutzer zu dokumentieren und auszuwerten, jedoch nur soweit dies zur Gewährleistung eines

ordnungsgemäßen Systembetriebs, zur Ressourcenplanung und Systemadministration, zum Schutz der personenbezogenen Daten anderer Nutzerinnen und Nutzer, zu Abrechnungszwecken, für die rechtzeitige Erkennung und Beseitigung von Systemschwachstellen und Störungen oder für die Fehlersuche oder zur Aufklärung und Unterbindung einer unzulässigen oder pflichtwidrigen Nutzung z.B. bei dem Verdacht eines Cyberangriffs erforderlich ist.

(2) Administratorinnen und Administratoren sind in ihrem Verantwortungsbereich berechtigt, die Nutzung von IT-Ressourcen sowie Hard- und Software nach § 5 Abs. 5 vorübergehend einzuschränken oder einzelne Benutzerkennungen vorübergehend zu sperren. Die Administratorinnen und Administratoren haben die betroffenen Nutzerinnen und Nutzer über die getroffenen Maßnahmen zu unterrichten, sofern dies mit vertretbarem Aufwand möglich ist. Zur Aufklärung und Unterbindung unzulässiger Nutzungen kann die Information der Nutzerin oder des Nutzers unterbleiben. Für eine unzulässige oder pflichtwidrige Nutzung müssen tatsächliche und dokumentierte Anhaltspunkte vorliegen.

(3) Administratorinnen und Administratoren sowie Personen, die lokale Administrationsrechte besitzen, sind verpflichtet,

a) die Administration der IT-Infrastruktur kooperativ, sachgerecht und zweckgebunden zu erledigen,

b) insbesondere die Bestimmungen zum Daten- und Fernmeldegeheimnis sowie die Grundsätze der Datenvermeidung und Datensparsamkeit zu beachten,

c) unverzüglich verfügbare Sicherheitsupdates einzuspielen, Gegenmaßnahmen für End-of-Service-Systeme zu ergreifen, regelmäßig Systeme auf Schwachstellen, funktionierenden Virenschutz und Firewallabsicherung zu prüfen,

d) Informationsquellen zu Sicherheitsproblemen zu verfolgen und auf Hinweise zur Beseitigung von Sicherheitslücken unverzüglich zu reagieren,

e) Hard- und Software vor Einrichtung und Nutzung auf die Einhaltung des Standes der Technik zu überprüfen sowie angemessene Maßnahmen zum Schutz der darauf verarbeiteten Daten zu treffen,

f) Administrationsmaßnahmen nachvollziehbar zu dokumentieren. Dies gilt insbesondere für Maßnahmen nach § 10 Absatz 1 und 2.

§ 11 Rechte und Pflichten der Nutzerinnen und Nutzer

Nutzerinnen und Nutzer sind verpflichtet,

a) die Namenskonventionen für E-Mails nach § 6 Abs. 3 zu beachten,

b) die besonderen Bestimmungen für die E-Mail-Nutzung gemäß § 7 Abs. 1 bis 3 zu beachten,

c) die besonderen Bestimmungen für Webseiten gemäß § 8 zu beachten,

d) die besonderen Bestimmungen für die Beschaffung, Nutzung und Aussonderung von Hard- und Software und sonstigen IT-Diensten gemäß § 9 zu beachten,

e) dafür Sorge zu tragen, dass Computer nicht unberechtigt genutzt werden oder dienstfremde Personen Zugriff auf dienstliche Informationen erhalten. Dafür ist insbesondere die Benutzeroberfläche der Computer auch bei kurzer Abwesenheit zu sperren,

f) für die Standardnutzung dienstlicher Geräte keinen Administrator-Account zu nutzen,

g) Datenträger auf dienstlich genutzten Notebooks zu verschlüsseln,

h) Daten auf den Laufwerken der HTW Dresden zu speichern,

i) Computer am Arbeitsplatz und andere an das Netzwerk der Hochschule angebundene Geräte bei Abwesenheit an Wochenenden, Feiertagen und während der Schließzeit über den Jahreswechsel auszuschalten. Ausnahmen gelten für betriebsnotwendige Monitoring-, Überwachungs- und Steuerungssysteme, z.B. im Dezernat Technik, im ZID sowie bei Forschungstätigkeiten mit Dauerversuchen.

j) die auf den Arbeitsgeräten installierten Schutzprogramme, insbesondere Antivirensoftware aktuell zu halten bzw. die Administratorin/ den Administrator bei Fehlermeldungen umgehend zu informieren,

k) dafür Sorge zu tragen, dass unberechtigten Personen die Nutzung des persönlichen Benutzerkontos verwehrt wird. Dazu gehören die sorgfältige Wahl eines nicht einfach zu erratenden Passwortes entsprechend den Vorgaben des ZID.

l) Passwörter für das persönliche Benutzerkonto nicht weiterzugeben,

m) fremde Passwörter weder zu ermitteln noch zu nutzen.

§ 12 Sanktionen bei Verstößen gegen die IT-Ordnung

(1) Nutzerinnen und Nutzer können vorübergehend oder dauerhaft in der Nutzung der IT-Infrastruktur eingeschränkt oder ganz ausgeschlossen werden, wenn diese schuldhaft gegen Regelungen dieser Ordnung verstoßen. Eine dauerhafte Nutzungseinschränkung oder ein dauerhafter Nutzungsausschluss kommt insbesondere bei Anhaltspunkten für strafbares Verhalten sowie wiederholten Verstößen gegen diese Ordnung in Betracht. Über die Wiederzulassung entscheidet die/der Beauftragte für Informationssicherheit.

(2) Bei Verstößen gegen diese Ordnung kommen gegen Beschäftigte der HTW Dresden arbeits- bzw. disziplinarrechtliche Maßnahmen (z.B. Abmahnung oder Kündigung, Verweis, Entfernung aus dem Dienst etc.) in Betracht.

(3) Bei strafbarem Verhalten kann Strafanzeige erstattet werden.

§ 13 Haftung der Nutzerinnen und Nutzer

(1) Die Nutzerin/der Nutzer haftet im Rahmen der rechtlichen Vorgaben für Schäden, die der HTW Dresden durch pflichtwidrige Verwendung der IT-Infrastruktur durch die Nutzerin bzw. den Nutzer oder dadurch entstehen, dass diese/dieser schuldhaft ihren/ seinen Pflichten aus dieser Ordnung nicht nachkommt.

(2) Die Nutzerin/der Nutzer haftet auch für Schäden, die im Rahmen der ihr/ihm zur Verfügung gestellten Zugriffs- und Nutzungsmöglichkeiten durch Drittnutzung entstanden sind, wenn sie/er diese Drittnutzung zu vertreten hat, insbesondere im Falle der unberechtigten Weitergabe eines Passwortes an Dritte.

(3) Die Nutzerin/der Nutzer hat die HTW Dresden im Rahmen der rechtlichen Vorgaben von allen Ansprüchen freizustellen, wenn Dritte die Hochschule wegen eines missbräuchlichen oder rechtswidrigen Verhaltens der Nutzerin/des Nutzers auf Schadenersatz bzw. Unterlassung verklagen oder in sonstiger Weise in Anspruch nehmen.

§ 14 Inkrafttreten

Die Ordnung tritt am Tage nach der Veröffentlichung im Bekanntmachungsblatt der HTW Dresden in Kraft.

Ausgefertigt am 08.05.2023 aufgrund des Beschlusses des Rektorates vom 02.05.2023.

Dresden, den 08.05.2023

Gez.

Prof. Dr. rer. nat. Katrin Salchert

Rektorin