Technische Universität Dresden

Ordnung für die informationstechnischen Einrichtungen und Dienste und zur Informationssicherheit der TU Dresden (IT-Ordnung)

Vom 18. Februar 2021

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 Artikel 5 des Gesetzes vom 17. Dezember 2020 (SächsGVBl. S. 731) geändert worden ist, hat das Rektorat der Technischen Universität Dresden in seiner Sitzung am 16. Februar 2021 nachfolgende Ordnung erlassen.

Inhaltsübersicht

Abschnitt 1: Allgemeine Bestimmungen

§ 1
Geltungsbereich

(1) Die vorliegende Ordnung gilt für den Betrieb und die Nutzung von IT-Infrastruktur an der TU Dresden sowie für deren Nutzerinnen und Nutzer.

(2) Unter IT-Infrastruktur der TU Dresden werden alle informationstechnischen Einrichtungen, IT-Systeme (Hard- und Software) und IT-Kommunikationsnetze sowie die zur Verfügung gestellten Dienste (inkl. VoIP) verstanden.

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

(4) Die Festlegungen dieser Ordnung sind bei Vereinbarungen und Verträgen mit An-Instituten der TU Dresden sowie außeruniversitären Einrichtungen, die direkt an das Netz der TU Dresden angeschlossen sind oder über dieses Teilnehmende des Deutschen Forschungsnetzes (DFN) sind, zu beachten.

(5) Die Freiheit von Wissenschaft, Forschung und Lehre bleibt durch diese Ordnung unberührt, insbesondere wenn deren Gegenstand IT-Forschung ist.

§ 2
Gegenstand der Ordnung

Gegenstand dieser Ordnung sind die Nutzungsmöglichkeiten und -rechte bzgl. der IT-Infrastruktur der TU Dresden und die diesbezüglichen Konditionen sowie die aus der Nutzung resultierenden Pflichten. Weiterhin sind die für einen hochschulweiten Informationssicherheitsprozess erforderlichen Verantwortungsstrukturen, die Aufgabenzuordnung sowie die Zusammenarbeit der Beteiligten geregelt.

§ 3
Begriffsbestimmungen und Regelungsinhalte

(1) Nutzerinnen und Nutzer im Sinne dieser Ordnung sind alle natürlichen und juristischen Personen der geschlossenen Nutzergruppe, die die IT-Infrastruktur der TU Dresden mit den zugehörigen Diensten zu Zwecken nach § 14 Absatz 1 und Absatz 3 in Anspruch nehmen.

(2) Der geschlossenen Nutzergruppe gehören ausschließlich Mitglieder und Angehörige der TU Dresden sowie sonstige natürliche Personen (Gäste), die die Voraussetzungen nach § 14 Absatz 2 Satz 2 erfüllen, an.

(3) Dritte bzw. Dritter ist jede natürliche und juristische Person außerhalb der geschlossenen Nutzergruppe.

(4) Administratorinnen und Administratoren im Sinne dieser Ordnung sind inhaltlich und technisch Verantwortliche und Zuständige sowie kontrollbefugte Personen für die IT-Infrastruktur der TU Dresden. Als Administratorinnen und Administratoren sind grundsätzlich nur Mitglieder oder Angehörige der TU Dresden zugelassen. Ausnahmen regelt § 13.

(5) Verarbeiten ist das Erheben, Speichern, Verändern, Anonymisieren, Übermitteln, Nutzen, Bereitstellen, Sperren und Löschen von Daten, ungeachtet der dabei angewendeten Verfahren.

(6) Benutzerkonto im Sinne dieser Ordnung sind alle Daten, insbesondere ZIH-Login, Passwort und E-Mail-Adresse, die einer Nutzerin bzw. einem Nutzer zur ordnungsgemäßen Nutzung der IT-Infrastruktur der TU Dresden mit den zugehörigen Diensten zugeordnet werden.

(7) Benutzerkennung im Sinne dieser Ordnung ist das ZIH-Login und das Passwort.

(8) DFN-PKI im Sinne dieser Ordnung ist die Public Key Infrastruktur des Deutschen Forschungsnetzes, an der die TU Dresden teilnimmt. Es wird die fortgeschrittene elektronische Signatur zur Verfügung gestellt. Maßgeblich sind hierbei die Zertifizierungsrichtlinien der DFN-PKI. Die fortgeschrittene Signatur der DFN-PKI ist an der TU Dresden anzuwenden, wenn nicht durch eine Rechtsvorschrift oder Verträge die Schriftform angeordnet bzw. vertraglich vereinbart ist.

(9) IT-Verfahren ist die Gesamtheit aller Einrichtungen und Dienste, bei denen Daten für einen bestimmten, näher zu bezeichnenden Zweck, verarbeitet werden.

(10) Informationssicherheit ist als umfassender Begriff für den Schutz von Informationen anzusehen und bezieht sich, ungeachtet der Art und Weise der Verarbeitung, auf den Schutz aller relevanten Informationen, einschließlich personenbezogener Daten. Dabei bezeichnet Informationssicherheit insbesondere einen Zustand, in dem die Risiken für die Sicherheitsziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz von Informationen und IT durch angemessene technische und organisatorische Maßnahmen auf ein tragbares Maß reduziert sind.

(11) IT-Notfall ist ein länger andauernder Ausfall von IT-Prozessen oder IT-Ressourcen mit hohem oder sehr hohem Schaden.

Abschnitt 2: Verantwortlichkeiten, Zuständigkeiten und Haftung

§ 4
TU Dresden

(1) Die TU Dresden stellt sicher, dass Nutzerinnen und Nutzer an der TU Dresden IT-Infrastruktur und Dienste zur Nutzung für Zwecke nach § 14 Absatz 1 und Absatz 3 zur Verfügung stehen.

(2) Die TU Dresden übernimmt keine Garantie dafür, dass die informationstechnischen Einrichtungen und Dienste sowie die an der TU Dresden eingesetzte Software fehlerfrei und jederzeit ohne Unterbrechung verfügbar sind. Eventuelle Datenverluste infolge technischer Störungen sowie die Kenntnisnahme vertraulicher Daten durch unberechtigte Zugriffe Dritter können nicht ausgeschlossen werden.

(3) Die TU Dresden übernimmt keine Verantwortung für die zur Verfügung gestellte Software. Weiterhin haftet die TU Dresden nicht für den Inhalt, insbesondere für die Richtigkeit, Vollständigkeit und Aktualität der Informationen, zu denen sie lediglich den Zugang zur Nutzung vermittelt.

(4) Die TU Dresden haftet im Übrigen nur bei grober Fahrlässigkeit und Vorsatz ihrer Beschäftigten, ausgenommen für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesund-

heit. Die Haftungseinschränkung gilt ebenfalls nicht, wenn eine schuldhafte Verletzung wesentlicher Pflichten vorliegt, deren Einhaltung für die Erreichung des Zwecks von besonderer Bedeutung und der TU Dresden dies bekannt ist. In diesem Fall ist die Haftung der TU Dresden auf typische, bei der Begründung des Nutzungsverhältnisses vorhersehbare Schäden begrenzt. Für mittelbare Schäden oder Folgeschäden wird keine Haftung übernommen.

§ 5
CDIO

(1) Der CDIO (Chief Officer Digitalisierung und Informationsmanagement) entwickelt Strategien für die Digitalisierung in Lehre, Forschung und Verwaltung sowie für den verantwortungsvollen Umgang mit IT. Sie bzw. er ist für die Weiterentwicklung von IT-Diensten sowie die Absicherung von IT-Ausstattung und IT-Administration an der TU Dresden zuständig und verfolgt deren Umsetzung.

(2) Der CDIO ist Mitglied des Erweiterten Rektorats.

(3) Der CDIO wird von einem strategisch ausgerichteten Gremium, dem CDIO Strategie-Rat, unterstützt. Der CDIO Strategie-Rat besteht aus

1. den Bereichs-CDIOs,
2. den CDIOs der Zentralen Wissenschaftlichen Einrichtungen, des Universitätsklinikum Carl Gustav Carus Dresden und der Sächsischen Landes- und Universitätsbibliothek, soweit diese nicht in Personalunion nach Nummer 1 Mitglied sind,
3. der Leiterin bzw. dem Leiter des Dezernats Planung und Organisation sowie der Leiterin bzw. dem Leiter des Sachgebiets Informationssicherheit als Vertretung der Zentralen Universitätsverwaltung,
4. der Direktorin bzw. dem Direktor des ZIH.

Der CDIO übernimmt den Vorsitz des CDIO Strategie-Rats und beruft diesen ein.

(4) Des Weiteren wird der CDIO durch den IT-Koordinierungsstab unterstützt. Dieser adressiert Themen und Absprachen zum operativen Betrieb der IT-Infrastruktur und der aufsetzenden Dienste und kann diesbezüglich Beschluss-Vorschläge in den CDIO Strategie-Rat einbringen. Der IT-Koordinierungsstab setzt sich aus den IT-Referentinnen und IT-Referenten der Bereiche und der Zentralen Wissenschaftlichen Einrichtungen sowie aus Vertretern aller Mitgliedsgruppen der Universität zusammen. Der CDIO übernimmt den Vorsitz des IT-Koordinierungsstabs und beruft diesen ein.

(5) Der CDIO kann zur Vorbereitung seiner Entscheidungen insbesondere themen- bzw. fachbezogen besetzte Arbeits- und Projektgruppen einrichten.

§ 6
Sachgebiet Informationssicherheit

(1) Die Verantwortung für die Herstellung und dauerhafte Aufrechterhaltung eines angemessenen Niveaus der Informationssicherheit nach dem Stand der Technik liegt bei dem Erweiterten Rektorat, vertreten durch den CDIO. Das Erweiterte Rektorat setzt für die Wahrnehmung der Aufgaben zur Informationssicherheit das Sachgebiet Informationssicherheit ein. Das Sachgebiet handelt bei der Erfüllung seiner diesbezüglichen Aufgaben fachlich unabhängig. Artikel 38 der EU-Datenschutzgrundverordnung (DSGVO) vom 27. April 2016 bzw. § 8 Absatz 2 des Sächsischen Informationssicherheitsgesetzes (SächISichG) bleiben unberührt.

(2) Im Sachgebiet Informationssicherheit sind mindestens die bzw. der Datenschutzbeauftragte der TU Dresden, die bzw. der Beauftragte für Informationssicherheit der TU Dresden sowie das TUD-CERT organisatorisch zusammengefasst.

(3) Das Sachgebiet Informationssicherheit wird von der bzw. dem Datenschutzbeauftragten geleitet. Das TUD-CERT wird von der bzw. dem Beauftragten für Informationssicherheit geleitet.

(4) Das Sachgebiet Informationssicherheit stellt zur Einhaltung der Sicherheitsziele angepasste Prozesse, Aktions- und Reaktionspläne in Abstimmung mit dem CDIO und dem Erweiterten Rektorat bereit.

§ 7
Zentrum für Informationsdienste und Hochleistungsrechnen (ZIH)

(1) Das Zentrum für Informationsdienste und Hochleistungsrechnen (ZIH) ist grundsätzlich für die zentrale IT-Infrastruktur der TU Dresden zuständig und verantwortlich. Die Dienste sind in einem laufend fortzuschreibenden Business-Service-Katalog zu dokumentieren. Der Betrieb weiterer zentraler Dienste ist im Einvernehmen mit dem CDIO durch andere Struktureinheiten möglich.

(2) Vom ZIH werden, der technischen Entwicklung folgend, die erforderlichen Maßnahmen zur Verhinderung und Beseitigung des Missbrauchs von IT-Systemen getroffen. Die Errichtung und der Betrieb von zentralen sicherheitstechnischen Einrichtungen und Diensten erfolgt grundsätzlich in Verantwortung und Zuständigkeit des ZIH. Bei wesentlichen Maßnahmen, insbesondere denen, die die gesamte TU Dresden betreffen, entscheidet der CDIO. Die Nutzerinnen und Nutzer werden von den erforderlichen Maßnahmen rechtzeitig, transparent und in verständlicher Form in Kenntnis gesetzt.

(3) Die Errichtung und der Betrieb von aktiven Netzkomponenten in dezentraler Zuständigkeit und Verantwortung sind nur im Benehmen mit dem ZIH und im Einvernehmen mit dem CDIO zugelassen. Sofern in Datenverteilerräumen VoIP-Einrichtungen betrieben werden, sind diese Räume dem ZIH zugeordnet und werden ausschließlich zweckgebunden zum Betrieb des Datenkommunikationsnetzes verwendet. Den Zugang zu diesen Datenverteilerräumen bestimmt das ZIH nach pflichtgemäßem Ermessen und insbesondere gemäß § 19 Absatz Satz 1. Wird Infrastruktur der TU Dresden nicht zentral bereitgestellt, kann diese im Einvernehmen mit dem ZIH und dem Sachgebiet Informationssicherheit sowie im Einvernehmen mit dem CDIO in Verantwortung der Bereiche betrieben werden.

(4) Die Einzelheiten der Nutzungsmöglichkeiten und -bedingungen der Einrichtungen und Dienste nach § 7 Absatz 1 bis 3 regelt das ZIH in dessen Benutzungsordnungen.

(5) Die Bestimmungen aus § 7 Absatz 1 bis 4 sind auf andere Struktureinheiten der TU Dresden entsprechend anzuwenden, wenn von diesen zentrale IT–Infrastrukturen zur Verfügung gestellt und betrieben werden.

§ 8
Dezentrale IT-Organisation

(1) Die Bereichs-CDIOs und die CDIOs der Zentralen Wissenschaftlichen Einrichtungen sind in ihrem Zuständigkeitsbereich insbesondere verantwortlich für:

1. die Umsetzung der durch das Erweiterte Rektorat vorgegebenen Digitalisierungsstrategie und der vom CDIO getroffenen Entscheidungen,
2. die strategische Planung und Entwicklung der IT-basierten Dienstleistungen im Rahmen der jeweiligen Struktureinheit sowie
3. die Umsetzung der Bestimmungen dieser Ordnung für alle in der jeweiligen Struktureinheit betriebenen informationstechnischen Einrichtungen mit den zugehörigen Diensten.

(2) Die Bereichs-CDIOs und die CDIOs der Zentralen Wissenschaftlichen Einrichtungen werden von den jeweiligen Leitungen der Struktureinheit, der sie angehören vorgeschlagen und vom CDIO bestellt. Bei Themen, die Digitalisierung und Informationssicherheit betreffen, binden die Leitungen der Bereiche den Bereichs-CDIO ein. Die CDIOs der Zentralen Wissenschaftlichen Einrichtungen haben sich entsprechend mit ihren Leitungen abzustimmen. Die Bereichs-CDIOs und CDIOs der Zentralen Wissenschaftlichen Einrichtungen sind in der Umsetzung der Digitalisierungsstrategie sowie der Sicherstellung der IT-basierten Dienstleistungen durch die Leitungen der Bereiche und der Zentralen Wissenschaftlichen Einrichtungen zu unterstützen.

(3) Zur Erfüllung der übertragenen Verantwortlichkeiten werden die Bereichs-CDIOs und die CDIOs der Zentralen Wissenschaftlichen Einrichtungen durch eine IT-Referentin bzw. einen IT-Referenten unterstützt.

(4) Die dezentrale IT-Versorgung und -Administration erfolgt durch (dezentrale) IT-Service-Teams.

(5) Die IT-Referentin bzw. der IT-Referent ist gegenüber den IT-Service-Teams (die sich aus den IT-Administratorinnen und IT-Administratoren der Struktureinheiten zusammensetzen), sofern vorhanden, zur Umsetzung der unter Absatz 1 genannten Aufgaben der Bereichs-CDIOs und der CDIOs der Zentralen Wissenschaftlichen Einrichtungen weisungsbefugt.

(6) Die Nutzerinnen und Nutzer im Sinne dieser Ordnung sind verpflichtet, Hinweise und Festlegungen der Bereichs-CDIOs und CDIOs der Zentralen Wissenschaftlichen Einrichtungen zu beachten.

§ 9
Leiterin bzw. Leiter der Struktureinheit

(1) Die Leiterin bzw. der Leiter der Struktureinheit ist für die Einhaltung der Bestimmungen dieser Ordnung in ihrem bzw. seinem Verantwortungsbereich verantwortlich.

(2) Sie bzw. er hat in ihrem bzw. seinem Verantwortungsbereich eine oder mehrere Zuständige bzw. einen Zuständigen für die IT-Infrastruktur zu benennen. Diese sind der zugeordneten IT-Referentin bzw. dem zugeordneten IT-Referenten mitzuteilen. Änderungen sind laufend aktualisiert mitzuteilen.

(3) Die Leiterin bzw. der Leiter der Struktureinheit legt für die eigene IT-Infrastruktur eine Verfahrensverantwortliche bzw. einen Verfahrensverantwortlichen fest, die bzw. der diese IT-Infrastruktur dokumentiert.

§ 10
Besondere Rechte und Pflichten der Administratorinnen und Administratoren

(1) Die Administration der IT-Infrastruktur nach § 1 Absatz 1 muss kooperativ, sachgerecht und zweckgebunden erfolgen. Dabei sind insbesondere die Bestimmungen zum Daten- und Fernmeldegeheimnis sowie die Grundsätze der Datenvermeidung und Datensparsamkeit zu beachten.

(2) Die Administratorinnen und Administratoren sind verpflichtet, Informationsquellen zu Sicherheitsproblemen zu verfolgen und auf Hinweise zur Beseitigung von Sicherheitslücken zu reagieren.

(3) Die technische Organisation und Umsetzung von Datenschutz- und -sicherungsmaßnahmen liegt in der Zuständigkeit der Administratorinnen und Administratoren.

(4) Im Falle einer dezentralen Nutzerinnen- und Nutzerverwaltung nach § 15 Absatz 5 verwaltet die Administratorin bzw. der Administrator insbesondere die erteilten Benutzungsberechtigungen und Bestandsdaten der Nutzerinnen und Nutzer, die in ihrem bzw. seinem Zuständigkeitsbereich liegen.

(5) Die Administratorin bzw. der Administrator ist 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

1. zur Gewährleistung eines ordnungsgemäßen Systembetriebs,
2. zur Ressourcenplanung und Systemadministration,
3. zum Schutz der personenbezogenen Daten anderer Nutzerinnen und Nutzer,
4. zu Abrechnungszwecken,
5. für die rechtzeitige Erkennung und Beseitigung von Systemschwachstellen und Störungen oder für die Fehlersuche oder
6. zur Aufklärung und Unterbindung einer rechtswidrigen oder missbräuchlichen Nutzung erforderlich ist.

(6) 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 von Missbräuchen erforderlich ist, kann die Administratorin bzw. der Administrator die Nutzung von Ressourcen vorübergehend einschränken oder einzelne Benutzerkennungen vorübergehend sperren. Die betroffenen Nutzerinnen und Nutzer sind unverzüglich, sofern mit vertretbarem Aufwand möglich, über die getroffenen Maßnahmen zu unterrichten. Insbesondere zur Aufklärung und Unterbindung von Missbräuchen kann die vorherige Information der Nutzerin bzw. des Nutzers unterbleiben. Für einen Missbrauch müssen tatsächliche und dokumentierte Anhaltspunkte vorliegen.

(7) Für die Protokollierung, Einsichtnahme und Übermittlung von personenbezogenen Nutzerdaten gelten die einschlägigen gesetzlichen und rechtlichen Bestimmungen.

(8) 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 von Missbräuchen erforderlich ist, kann die Administratorin bzw. der Administrator, sofern keine rechtlichen Gründe entgegenstehen, im Benehmen mit der bzw. dem Datenschutzbeauftragten, Einsicht in nutzereigene Daten nehmen. Hierfür ist, sofern möglich, die vorherige Einwilligung der betroffenen Nutzerin bzw. des betroffenen Nutzers einzuholen. In jedem Fall sind die betroffenen Nutzerinnen und Nutzer unverzüglich über die getroffenen Maßnahmen zu unterrichten. Zur Aufklärung und Unterbindung von Missbräuchen oder soweit dies bei

der Verfolgung von Straftaten erforderlich ist, kann die Information der Nutzerin bzw. des Nutzers unterbleiben. Für einen Missbrauch oder für eine Straftat müssen tatsächliche und dokumentierte Anhaltspunkte vorliegen.

(9) Die Administratorin bzw. der Administrator ist verpflichtet, alle Maßnahmen, insbesondere solche nach § 10 Absatz 5, 6 und 8, nachvollziehbar zu dokumentieren.

§ 11
Haftung der Nutzerinnen und Nutzer

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

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

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

§ 12
Sanktionen bei Missbrauch

(1) Nutzerinnen und Nutzer können vorübergehend oder dauerhaft in der Benutzung eingeschränkt oder ganz ausgeschlossen werden, wenn diese
1. schuldhaft gegen diese Ordnung verstoßen (missbräuchliches Verhalten) oder
2. die IT-Infrastruktur der TU Dresden für strafbare Handlungen missbrauchen oder
3. der TU Dresden durch sonstiges rechtswidriges Nutzerverhalten Nachteile zufügen.

(2) Maßnahmen nach Absatz 1 sollen erst nach vorheriger Anhörung erfolgen. Der bzw. dem Betroffenen ist Gelegenheit zur Stellungnahme zu geben.

(3) Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass ein Verhalten nach Absatz 1 gegeben ist, kann eine weitere Nutzung untersagt und unterbunden werden, bis die Sach- und Rechtslage geklärt ist.

(4) Vorübergehende Nutzungseinschränkungen sind aufzuheben, sobald eine ordnungsgemäße Nutzung wieder gewährleistet ist.

(5) Eine dauerhafte Nutzungseinschränkung oder der vollständige Ausschluss einer Nutzerin bzw. eines Nutzers von der weiteren Nutzung kommt nur bei schwerwiegenden bzw. wiederholten Verstößen im Sinne von Absatz 1 in Betracht, wenn auch künftig ein ordnungsgemäßes Verhalten nicht zu erwarten ist. Die Einschränkung bzw. der Ausschluss kann auf Antrag oder von Amts wegen aufgehoben werden, sofern die Wiederholungsgefahr nicht mehr besteht. Dies ist von der bzw. von dem Ausgeschlossenen glaubhaft zu machen.

(6) Auf die folgenden Straftatbestände wird besonders hingewiesen:

1. Ausspähen von Daten (§ 202a Strafgesetzbuch (StGB)),
2. Abfangen von Daten (§ 202b StGB),
3. Vorbereiten des Ausspähens und Abfangens von Daten (§ 202 c StGB),
4. Datenveränderung (§ 303a StGB) und Computersabotage (§ 303b StGB),
5. Computerbetrug (§ 263a StGB),
6. Verbreitung pornographischer Darstellungen (§ 184b StGB),
7. Abruf oder Besitz kinderpornographischer Darstellungen (§ 184 StGB),
8. Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB)
9. Volksverhetzung (§ 130 StGB),
10. Ehrdelikte wie Beleidigung oder Verleumdung (§ 185 ff. StGB),
11. Strafbare Urheberrechtsverletzungen (§ 106 ff. Urheberrechtsgesetz (UrhG)).

(7) Des Weiteren kommen gegen Beschäftigte der TU Dresden arbeits- bzw. disziplinarrechtliche Maßnahmen in Betracht.

(8) Bei strafbarem Verhalten kann Strafanzeige erstattet werden.

§ 13
Dritte

Nur in begründeten Ausnahmefällen und unter Berücksichtigung des Schutzbedarfes der zu verarbeitenden Informationen können Dritte mit dem Betrieb oder der Betreuung der IT-Infrastruktur beauftragt werden. Dies ist im Benehmen mit dem Sachgebiet Informationssicherheit vertraglich zu vereinbaren.

Abschnitt 3: Nutzung

§ 14
Nutzungszweck und Zulassung zur Nutzung

(1) Die Errichtung und der Betrieb der IT-Infrastruktur sowie die Zulassung zur Nutzung der IT-Infrastruktur erfolgt ausschließlich zu Zwecken von Forschung, Lehre und Studium, der Aus- und Weiterbildung sowie zu Zwecken der universitären Verwaltung und zur Erfüllung sonstiger Aufgaben der TU Dresden.

(2) Die Zulassung zur Nutzung erfolgt ausschließlich für die Mitglieder und Angehörigen der geschlossenen Nutzergruppe. Gäste nach § 3 Absatz 2 können nur zeitlich begrenzt Mitglied der geschlossenen Nutzergruppe sein. Voraussetzung für die Aufnahme von Gästen in die geschlossene Nutzergruppe ist die Feststellung der Erforderlichkeit der Inanspruchnahme der genannten Einrichtungen und Dienste zur Erfüllung der Aufgaben des Gastes an der TU Dresden nach § 14 Absatz 1.

(3) Soweit dies rechtlich nicht anders bestimmt ist, ist die Nutzung der IT-Infrastruktur nach § 1 Absatz 1 für andere als im § 14 Absatz 1 Satz 1 genannte Zwecke zulässig, wenn sie geringfügig ist, die Nutzung der IT-Infrastruktur durch die anderen Nutzerinnen und Nutzer nicht behindert oder stört und die dienstliche Aufgabenerfüllung nicht beeinträchtigt wird.

(4) In besonderen Fällen kann die zuständige Leiterin bzw. der zuständige Leiter der Struktureinheit untersagen, die IT-Infrastruktur nach § 1 Absatz 1 dieser Ordnung oder Teilen hiervon für andere Zwecke zu nutzen. In Zweifelsfällen ist dies durch das Sachgebiet Informationssicherheit zu bewerten und eine Entscheidung des CDIO der TU Dresden herbeizuführen.

(5) Die Nutzung von Hard- und Software ist nur zugelassen, wenn diese dem Stand der Technik entspricht und geeignete und angemessene Maßnahmen zum Schutz der darauf verarbeiteten Daten getroffen wurden. Der zuständigen Administratorin bzw. dem zuständigen Administrator obliegt die entsprechende Prüfung. Diese bzw. dieser kann die Nutzung ggf. einschränken oder vollständig unterbinden. In Zweifelsfällen hat sie bzw. er sich direkt an das Sachgebiet Informationssicherheit zu wenden. Der CDIO entscheidet in diesen Fällen über die Zulassung zur Nutzung abschließend.

(6) Die IT-Infrastruktur darf nicht zur individuellen Leistungs- und Verhaltenskontrolle der Beschäftigten der TU Dresden genutzt werden.

§ 15
Nutzerinnen- und Nutzerverwaltung

(1) Für die Nutzerinnen und Nutzer wird beim ZIH ein zentrales Benutzerkonto in elektronischer Form gebildet und verwaltet.

(2) Für die Verwaltung des zentralen Benutzerkontos nach § 15 Absatz 1 dürfen die Daten verarbeitet werden, die zur eineindeutigen Identifikation der Nutzerin bzw. des Nutzers, zum ordnungsgemäßen Betrieb der IT-Infrastruktur sowie zur Sicherstellung des ordnungsgemäßen Geschäftsablaufes an der TU Dresden erforderlich sind. Daten nach § 15 Absatz 2 dürfen an informationstechnische Einrichtungen und Dienste nur übermittelt werden, wenn im Einzelfall festgestellt und nachgewiesen wird, dass die Verarbeitung dieser Daten für den ordnungsgemäßen Betrieb dieser Einrichtungen und Dienste erforderlich sind.

(3) Scheidet eine Nutzerin bzw. ein Nutzer aus, wird das zentrale Benutzerkonto nach 14 Tagen gesperrt und spätestens nach 15 Monaten gelöscht. Von der Löschung sind auch die mit dem Konto verbundenen Daten betroffen.

(4) Die Nutzerinnen und Nutzer sind verpflichtet, ausschließlich mit den Benutzerkennungen zu arbeiten, deren Nutzung ihnen im Rahmen der Zulassung gestattet wurde. Jede Nutzerin bzw. jeder Nutzer hat dafür Sorge zu tragen, dass unberechtigten Personen die Nutzung ihres bzw. seines Benutzerkontos verwehrt wird. Dazu gehören die sorgfältige Wahl eines nicht einfach zu erratenden Passwortes gemäß der Passwortrichtlinie des ZIH. Die Weitergabe des Passworts ist unzulässig. Der Nutzerin bzw. dem Nutzer ist es untersagt, fremde Benutzerkennungen zu ermitteln und zu nutzen.

(5) Eine dezentrale Nutzerinnen- und Nutzerverwaltung ist zugelassen, wenn die zentrale Nutzerinnen- und Nutzerverwaltung nach § 15 Absatz 1 die erforderlichen Funktionalitäten nicht aufweisen und dies zur Erfüllung der Aufgaben der Struktureinheiten erforderlich ist. Für dezentrale Nutzerinnen- und Nutzerverwaltung sind bezüglich der Informationssicherheit die gleichen Anforderungen wie an die zentrale Nutzerinnen- und Nutzerverwaltung des ZIH maßgebend. Dies ist über das Sachgebiet Informationssicherheit und den CDIO im Vorab zur Genehmigung vorzulegen.

Abschnitt 4: Besondere Bestimmungen für Namenskonventionen, E-Mail und Web-Applikationen

§ 16
Namenskonventionen

(1) Alle an das Datennetz der TU Dresden angeschlossenen Endgeräte sollen einen eindeutigen Namen (Hostnamen) unterhalb der Domain „tu-dresden.de“ erhalten. Das ZIH verwaltet diese Domain sowie deren Subdomains.

(2) Eindeutige Hostnamen werden nach dem Schema „Hostname.Struktureinheit.tu-dresden.de“ gebildet. Für den Teil „Struktureinheit“ kann die Abkürzung des Bereichs, der Fakultät, der Fachrichtung, der Zentralen Universitätsverwaltung (ZUV) oder der jeweiligen Zentralen Einrichtung (ZE) verwendet werden. Der Teil „Hostname“ wird von der Nutzerin bzw. vom Nutzer festgelegt. Eine weitere Unterteilung in Untereinheiten ist möglich.

(3) Für alle Domains nach § 16 wird der Nameservice (DNS) durch das ZIH realisiert.

§ 17
Besondere Bestimmungen für E-Mail

(1) Für Zwecke nach § 14 Absatz 1 sind die Nutzerinnen und Nutzer verpflichtet, ausschließlich die E-Mail-Adressen zu verwenden, die im Grundsatz folgenden Namenskonventionen entsprechen: für das wissenschaftliche und nichtwissenschaftliche Personal: vorname.nachname[y]@tu-dresden.de und für die Studierenden und Gäste: vorname.nachname[y]@mail.tu-dresden.de. Dabei sind Sonderzeichen unzulässig. Studentische Hilfskräfte zählen zur Gruppe der Studierenden (Primärrolle). Für bestehende dezentrale E-Mail-Adressen gilt bzgl. der Empfangsberechtigung ein Bestandsschutz.

(2) E-Mail-Adressen und zentrale E-Mail-Verteilerlisten werden, soweit dies rechtlich nicht anders bestimmt ist, im ZIH gebildet und verwaltet. Die Bildung und Nutzung von E-Mail-Verteilerlisten ist nur zulässig, soweit dies zur Durchführung des Dienst- oder Arbeitsverhältnisses, zur Durchführung organisatorischer Maßnahmen sowie für Ausbildungs-, Prüfungs- oder wissenschaftliche Zwecke erforderlich ist.

(3) Bei Bedarf können strukturbezogene oder funktionsbezogene E-Mail-Adressen bestehend aus struktureinheit@tu-dresden.de oder funktion@tu-dresden.de vergeben werden. Diese sind über das Self-Service Portal des ZIH zu beantragen.

(4) Der ein- und ausgehende E-Mail-Verkehr der TU Dresden erfolgt über das zentrale Gateway (Mailrelay) am ZIH. Das ZIH 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. Dabei können die Nutzerinnen und Nutzer die Bewertung selbst konfigurieren

sowie festlegen, ob die dann als SPAM bewerteten E-Mails abgewiesen werden oder als SPAM bewertet zugestellt werden sollen.

(8) Durch das wissenschaftliche und nicht-wissenschaftliche Personal abzusendende E-Mails (aus der Domäne @tu-dresden.de) sind mit einer elektronischen Signatur nach § 3 Absatz 8 zu signieren und grundsätzlich zu verschlüsseln. Der E-Mail-Versand von besonders schutzwürdigen personenbezogenen Daten sowie anderer Daten mit erhöhtem Schutzbedarf in unverschlüsselter Form ist unzulässig.

(9) Für dienstliche Zwecke ist eine automatisierte Weiterleitung eingehender E-Mails an Postfächer außerhalb der Infrastruktur der TU Dresden unzulässig. Auch das Verlangen, eine automatisierte Weiterleitung von E-Mails einzurichten, ist unzulässig.

(10) Für wissenschaftliche Zwecke ist eine Weiterleitung von E-Mails nach Ausscheiden der Nutzerin bzw. des Nutzers auf Antrag zulässig. Das ZIH stellt hierfür einen entsprechenden Dienst (Nachsendeportal) zur Verfügung. Automatisierte Weiterleitungen zu anderen Zwecken oder mit anderen kommunikationstechnischen Einrichtungen oder Diensten sind unzulässig.

(11) In den Struktureinheiten ist über Arbeitsanweisungen mindestens Folgendes zu regeln: Absenderberechtigung, Abwesenheitsmitteilungen und Vertretungsregelungen. Das ZIH stellt die technischen Möglichkeiten zur Einhaltung dieser Regelung bereit.

§ 18
Richtlinien für Webseiten

Struktureinheiten der TU Dresden sind angehalten, sich über den zentralen Webauftritt der TU Dresden zu präsentieren. Für Kooperationsprojekte mit externen Partnern sowie bei speziellen Funktionsanforderungen sind Ausnahmen zulässig, wobei die jeweiligen Vorgaben der TU Dresden zum Corporate Design sowie geltende Rechtsordnungen (v.a. bezüglich Impressum, Datenschutz und Barrierefreiheit) zu beachten sind. Zu diesen Anforderungen berät und unterstützt das Sachgebiet Web und Video, bei Datenschutzfragen in Kooperation mit Sachgebiet Informationssicherheit. Die letzte Entscheidung über zulässige Ausnahmen trifft der CDIO, ausgehend von einer durch das Sachgebiet Web und Video eingebrachten Entscheidungsvorlage.

Abschnitt 5: Informationssicherheit und Datenschutz

§ 19
Grundsätze

(1) Der Aufwand für den Schutz von personenbezogenen oder besonders schutzwürdigen Daten nach dem Stand der Technik muss in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen. Für die Verarbeitung personenbezogener Daten gelten die hierfür einschlägigen gesetzlichen und rechtlichen Bestimmungen. Für den Nachweis der nach Satz 1 getroffenen Schutzmaßnahmen sind insbesondere die Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in der jeweils aktuellen Fassung maßgeblich.

(2) Die Informationssicherheit ist ein zu bewertendes und herbeizuführendes Leistungsmerkmal von IT-Verfahren. Für die zentralen IT-Verfahren ist deshalb insbesondere der Schutzbedarf durch die jeweiligen Fachverantwortlichen festzulegen, für dezentrale IT-Verfahren durch die jeweils verantwortlichen Vorgesetzten.

§ 20
Rechte und Pflichten des Sachgebietes Informationssicherheit

(1) Das Sachgebiet Informationssicherheit muss bei allen Projekten, die deutliche Auswirkungen auf die Informationsverarbeitung haben, sowie bei der Einführung neuer Anwendungen und IT-Systeme beteiligt werden, damit sichergestellt ist, dass sicherheits- und datenschutzrelevante Aspekte ausreichend berücksichtigt werden.

(2) Die Struktureinheiten müssen das Sachgebiet Informationssicherheit bei der Erfüllung seiner Aufgaben unterstützen. Dem Sachgebiet Informationssicherheit steht ein umfassendes Informationsrecht über Angelegenheiten zu, die für die Informationssicherheit relevant sind. Dazu sind dem Sachgebiet Informationssicherheit rechtzeitig alle Informationen zur Verfügung zu stellen, die zur Erfüllung seiner Aufgaben von Bedeutung sein können. Es kann alle Informationen verlangen, die für seinen Aufgabenbereich erforderlich sind.

(3) Dem Sachgebiet Informationssicherheit werden insbesondere folgende Aufgaben und Rechte zugewiesen:

1. Steuerung und Koordinierung des Informationssicherheitsprozesses an der TU Dresden,
2. Unterstützung des Erweiterten Rektorates und des CDIO bei der Wahrnehmung der Verantwortlichkeiten zur Informationssicherheit,
3. Konzeption, Weiterentwicklung und Implementierung von Projekten mit Bezug zur Informationssicherheit,
4. Konzeption und Weiterentwicklung von hochschulinternen technischen und organisatorischen Standards zur Informationssicherheit,
5. Mitwirkung und Koordinierung bei der Erstellung von Ordnungen und Satzungen mit Bezug zur Informationssicherheit,
6. Beratung, Unterstützung und Kontrolle der Struktureinheiten bei der Umsetzung der rechtlichen Vorgaben zur Informationssicherheit,
7. umfassende Kontrolle und Bewertung von IT-Infrastrukturen der TU Dresden sowie von Verfahren bei denen personenbezogene oder andere besonders schutzwürdige Daten verarbeitet werden,
8. Initiierung, Prüfung und Bestätigung von Schutzbedarfsfeststellungen und Sicherheitskonzepten,
9. Untersuchung und Auswertung sicherheits- und datenschutzrelevanter Vorfälle sowie Errichtung und Betrieb von technischen Einrichtungen mit besonderer Bedeutung für die Informationssicherheit,
10. regelmäßige Berichterstattung beim CDIO zu Themen der Informationssicherheit,
11. verbindliche Stellungnahmen zur Informationssicherheit mit Genehmigung des CDIO,
12. Stellungnahmen und Hinweise gegenüber Struktureinheiten mit Beachtenspflicht in eigener Verantwortung,
13. direkte sowie zeitnahe Information bei besonderer Eilbedürftigkeit und im Einzelfall gegenüber dem CDIO und dem ZIH,
14. Planung, Organisation und Durchführung von Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit für Mitglieder, Angehörige und Gäste der TU Dresden und
15. Beratung und Unterstützung der Mitglieder, Angehörigen und Gäste der TU Dresden bei Fragen der Informationssicherheit.

§ 21
Mitteilungspflichten

In den Fällen eines
1. begründeten Verdachtes oder der Feststellung eines Verstoßes gegen die Bestimmungen dieser Ordnung,
2. begründeten Verdachtes oder der Feststellung eines Verlustes von Daten,
3. begründeten Verdachtes oder der Feststellung einer unberechtigten Einsichtnahme in Daten,
4. begründeten Verdachtes oder der Feststellung einer Kompromittierung der IT-Infrastruktur (Sicherheitsvorfälle)

ist dies unverzüglich und direkt dem Sachgebiet Informationssicherheit mitzuteilen.

Abschnitt 6: Software und Hardware

§ 22
Hardware- und Software-Beschaffung, Nutzung und Software-Lizenzierung

(1) Die Beschaffung von Hardware und Software ist in der Beschaffungsrichtlinie der TU Dresden (ausgenommen Medizinische Fakultät Carl Gustav Carus) festgelegt.

(2) Alle für die dienstliche Nutzung zu beschaffenden Software-Produkte an der TU Dresden sind im Benehmen mit dem Dezernat Planung und Organisation über das ZIH zu beantragen. Der Erwerb von Kleinstsoftware (Apps) in eigener Verantwortung ist zulässig, wenn vor Beschaffung geprüft wurde, dass die Software nicht in bestehenden Campusverträgen enthalten ist und ausreichende Mittel zur Verfügung stehen. Bezugsberechtigt sind Mitglieder, Angehörige und Gäste der TU Dresden mit eigener Kostenstelle, sofern es die Vertragsbedingungen des Herstellers zulassen.

(3) Die strategische und fachliche Zuständigkeit der Campusverträge und Rahmenverträge obliegt grundsätzlich dem CDIO, dem Dezernat Planung und Organisation und dem ZIH.

(4) Die Aussonderung von Hard- und Software erfolgt nach den Regularien der Inventarordnung der TU Dresden. Dabei sind die Festlegungen des BSI Grundschutzes zur Löschung gespeicherter Daten unbedingt zu beachten.

(5) Die Nutzerin bzw. der Nutzer ist berechtigt, die Software nur für die TU Dresden in der lizenzierten Anzahl und nur für Arbeiten in Forschung und Lehre auf den Rechnern in ihrem bzw. seinem Zuständigkeitsbereich zu nutzen. Für andere, z.B. gewerbliche, kommerzielle Zwecke oder Zwecke mit Gewinnerzielungsabsicht, gelten insbesondere die Lizenzbestimmungen bzw. Verträge für das jeweilige Softwareprodukt des Herstellers.

(6) Die private Nutzung der für dienstliche Zwecke erworbenen Software setzt voraus, dass diese Nutzungsform in Vertrags- oder Lizenzbestimmungen seitens der TU Dresden und vom Hersteller ausdrücklich genehmigt ist.

(7) Die Nutzung von privat erworbener Software für dienstliche Zwecke muss durch die Lizenzbestimmungen des Herstellers abgedeckt sein und bedarf der Zustimmung der bzw. des zuständigen Vorgesetzten.

(8) Studierendenlizenzen sind der Nutzung durch Studierende vorbehalten. Ausnahmen (Nutzung durch andere Personenkreise) sind nur mit Zustimmung des Softwareherstellers möglich.

(9) Je nach Softwarevertrag erhält die Nutzerin bzw. der Nutzer das zeitlich unbefristete oder zeitlich befristete Nutzungsrecht. Ist die Nutzung zeitlich befristet, so ist nach Ablauf dieser Nutzungsfrist die Software, ohne Aufforderung durch das ZIH, zu deinstallieren.

(10) Bei Ausscheiden der Nutzerin bzw. des Nutzers aus dem Beschäftigungs- oder Dienstverhältnis mit der TU Dresden sind zur Verfügung gestellte Hardware und alle Lizenzen an die jeweilige Struktureinheit zurückzuführen.

(11) Das ZIH ist berechtigt im Falle einer Lizenzüberprüfung (Audit) durch den Software-Hersteller eine TU Dresden-weite Überprüfung in Abstimmung mit dem Sachgebiet Informationssicherheit durchzuführen.

(12) Von Softwareherstellern verlangte Audits über den Einsatz der Software sind mit dem Sachgebiet Informationssicherheit der TU Dresden abzustimmen. Nach Unterrichtung der bzw. des Vorgesetzten ist die Administratorin bzw. der Administrator berechtigt, die für die Auswertungen benötigten Angaben bereitzustellen.

(13) Bei der Nutzung von Software, Dokumentationen und anderen Daten sind die gesetzlichen Vorgaben, insbesondere zum Urheberrechtsschutz und zur Barrierefreiheit, einzuhalten und die Lizenzbedingungen, unter denen Software, Dokumentationen und Daten zur Verfügung gestellt werden, zu beachten.

Abschnitt 7: IT-Notfallmanagement

§ 23
Inkrafttreten und Außerkrafttreten des IT-Notfallmanagement

(1) Die grundsätzliche Feststellung und die Dauer des IT-Notfallmanagement und der damit in Kraft tretenden Notfallpläne, Ausnahmeregelungen und Meldeketten obliegt dem CDIO. Das Erweiterte Rektorat wird parallel informiert.

(2) Ist eine einzelne Struktureinheit von einem IT-Notfall betroffen, obliegt die Feststellung der zuständigen Leiterin bzw. dem zuständigen Leiter der Struktureinheit im Einvernehmen mit dem Sachgebiet Informationssicherheit.

Abschnitt 8: Schlussbestimmungen

§ 24
Inkrafttreten und Außerkrafttreten

Die Ordnung tritt am Tage nach der Veröffentlichung in den Amtlichen Bekanntmachungen der TU Dresden in Kraft. Damit tritt die Ordnung für die informationstechnischen Einrichtungen und Dienste und zur Informationssicherheit der TU Dresden (IT-Ordnung) vom 7. Mai 2019 (Amtliche Bekanntmachungen der TU Dresden Nr. 08/2019 vom 17. Mai 2019, S. 592) außer Kraft.

Dresden, den 18. Februar 2021

Die Rektorin
der Technischen Universität Dresden

Prof. Dr. Ursula M. Staudinger