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

Vom 5. Januar 2016

Die vorliegende Ordnung wurde vom Rektorat der Technischen Universität Dresden in der Sitzung am 5. Januar 2016 beschlossen.

Inhaltsübersicht

Abschnitt 1: Allgemeine Bestimmungen

§ 1
Geltungsbereich

(1) Diese Ordnung gilt für die Nutzung der IT Infrastruktur der TU Dresden durch alle Benutzerinnen und Benutzer.

(2) Unter IT Infrastruktur werden alle informationstechnischen Einrichtungen, IT-Systeme (Hardware und Software), Netze und Telefonien sowie die darauf zur Verfügung gestellten Dienste verstanden.

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

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

§ 2
Gegenstand der Ordnung

Gegenstand dieser Ordnung ist sowohl die Regelung der Nutzungsmöglichkeiten und Rechte, als auch die verbindlich einzuhaltenden Pflichten der Benutzerinnen und Benutzer für die in § 1 genannten Einrichtungen und Dienste. Weiterhin sind die zur Realisierung eines hochschulweiten Informationssicherheitsprozesses 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 einer geschlossenen Benutzergruppe, die die IT Infrastruktur mit den zugehörigen Diensten der TU Dresden zu Zwecken nach § 15 Abs. 1 und Abs. 3 in Anspruch nehmen.

(2) Der geschlossenen Benutzergruppe gehören ausschließlich Mitglieder und Angehörige der TU Dresden sowie sonstige natürliche Personen (Gäste), die die Voraussetzungen nach § 15 Abs. 2 Satz 2 erfüllen, an.

(3) Dritter ist jede natürliche und juristische Person außerhalb der geschlossenen Benutzergruppe, die nicht der TU Dresden angehört.

(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 § 14.

(5) Verarbeiten ist das Erheben, Speichern, Verändern, Anonymisieren, Übermitteln, Nutzen, 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 nach § 2 Nr. 2 des Signaturgesetzes (SigG)[i] 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 Schriftform angeordnet ist.

(9) Groupware im Sinne dieser Ordnung sind alle Dienste der IT Infrastruktur der TU Dresden, die dem Zweck der Kommunikation und Zusammenarbeit der Mitglieder der geschlossenen Benutzergruppe dienen.

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

(11) 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.

§ 4
Besondere Namenskonventionen

(1) Alle an das Datennetz der TU Dresden angeschlossenen Endgeräte sollen einen eindeutigen Namen (Hostnamen) unterhalb dieser Domain erhalten. Das ZIH verwaltet die Domain „tu-dresden.de“ 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 verwendet werden. Der Teil „Hostname“ wird vom Nutzer festgelegt. Eine weitere Unterteilung in Untereinheiten ist möglich.

(3) Der Eintrag von Hostnamen direkt unterhalb der Domain „tu-dresden.de“, d.h. DNS-Namen ohne den Teil „Struktureinheit“ nach § 4 Abs. 2, kann auf Antrag an das ZIH erfolgen und bedarf der Zustimmung des Rektorates bzw. deren hierfür Beauftragten.

(4) Die Nutzung weiterer eigener Domainnamen (z.B. .de, .eu, .org) nach § 4 Abs. 1 und 2 kann im Sinne einer Ausnahmeregelung erteilt werden und bedarf der Zustimmung des Rektorates bzw. deren Beauftragten. Die Registrierung erfolgt auf Antrag an das ZIH.

(5) Für alle Domains nach § 4 wird durch das ZIH der Nameservice (DNS) realisiert.

(6) Abweichungen sind nur im Benehmen mit dem CIO zugelassen.

Abschnitt 2: Verantwortlichkeiten, Zuständigkeiten und Haftung

§ 5
TU Dresden

(1) 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.

(2) 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.

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

§ 6
CIO und CIO-Beirat

(1) Der (kollektive) CIO ist das durch das Rektorat eingesetzte zuständige Gremium für die Belange der Informationstechnik sowie der Informationssicherheit der TU Dresden. Im CIO sind die Kanzlerin bzw. der Kanzler und die Prorektorin für Universitätsplanung bzw. der Prorektor für Universitätsplanung entscheidungsberechtigt. Entscheidungen im CIO sollen in der Regel gemeinschaftlich erfolgen. Entscheidungen zur IT-Strategie trifft der CIO in Abstimmung mit dem CIO-Beirat.

(2) Der CIO-Beirat besteht aus dem CIO, den Bereichs-CIOs, den IT-Referentinnen und IT-Referenten der Bereiche, der Zentralen Einrichtungen und der ZUV sowie der Vertreterin bzw. dem Vertreter des Studentenrats und des Personalrates. Er bereitet Entscheidungen des CIO vor, entwickelt die IT-Strategie und kommuniziert diese in die Bereiche, die Zentra-

len Einrichtungen und die ZUV. Er kommuniziert TU-intern alle Fragen bzgl. Informationstechnik sowie zur Informationssicherheit.

§ 7
Stabsstelle für Informationssicherheit

(1) Die Verantwortung für die Herstellung und dauerhafte Aufrechterhaltung eines angemessenen Niveaus der Informationssicherheit nach dem Stand der Technik liegt beim Rektorat. Das Rektorat setzt für die Wahrnehmung der Aufgaben zur Informationssicherheit die Stabsstelle für Informationssicherheit ein. Die Stabsstelle handelt bei der Erfüllung ihrer Aufgaben fachlich unabhängig. §11 des Gesetzes über die informationelle Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz – SächsDSG)[ii] bleibt unberührt.

(2) In der Stabsstelle für Informationssicherheit sind mindestens die bzw. der Datenschutzbeauftragte der TU Dresden und die bzw. der IT-Sicherheitsbeauftragte der TU Dresden organisatorisch zusammengefasst.

(3) Die Stabsstelle für Informationssicherheit stellt zur Einhaltung der Sicherheitsziele angepasste Prozesse, Aktions- und Reaktionspläne bereit.

§ 8
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 CIO durch andere Einrichtungen 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 daher grundsätzlich in Verantwortung und Zuständigkeit des ZIH. Bei wesentlichen Maßnahmen, insbesondere denen, die die gesamte TU Dresden betreffen, entscheidet der CIO abschließend. 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 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 § 21 Abs. 1. Wird IT Infrastruktur der TU Dresden nicht zentral bereitgestellt, kann diese im Benehmen mit dem ZIH und nach Würdigung durch die Stabsstelle für Informationssicherheit in Verantwortung der Bereiche betrieben werden.

(4) Die Einzelheiten der Nutzungsmöglichkeiten und -bedingungen der Einrichtungen und Dienste nach § 8 Abs. 1 - 3 bestimmt die Direktorin bzw. der Direktor des ZIH in Benutzungsordnungen im Rahmen der rechtlichen Bestimmungen und, soweit diese nicht bereits von dieser Ordnung erfasst sind, in eigener Verantwortung und Zuständigkeit nach pflichtgemäßem Ermessen.

(5) Die Bestimmungen aus § 8 Abs. 1 - 4 sind auf andere Struktureinheiten der TU Dresden entsprechend anzuwenden, wenn von diesen zentrale informationstechnische Einrichtungen und Dienste zur Verfügung gestellt und betrieben werden.

§ 9
Bereichs-CIO

(1) Die Bereichs-CIOs werden von der Universitätsleitung ernannt.

(2) Sie sind in ihrem Zuständigkeitsbereich insbesondere
1. verantwortlich für die strategische Planung und Entwicklung der IT-basierten Dienstleistungen,
2. zuständig für die Umsetzung der durch das Rektorat vorgegebenen IT-Strategie sowie der vom CIO getroffenen Entscheidungen und
3. zuständig für die Umsetzung der Bestimmungen dieser Ordnung für alle in ihrem Bereich betriebenen informationstechnischen Einrichtungen mit den zugehörigen Diensten.

(3) Die Nutzerinnen und Nutzer im Sinne dieser Ordnung sind verpflichtet, die Bereichs-CIOs bei der Wahrnehmung Ihrer Aufgaben zu unterstützen sowie deren Hinweise und Festlegungen zu beachten.

§ 10
Leiterin bzw. Leiter der Struktureinheit

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

(2) Sie bzw. er hat in ihrem bzw. seinem Verantwortungsbereich eine oder mehrere inhaltlich und technisch Zuständige bzw. einen inhaltlich und technisch Zuständigen für die IT Infrastruktur zu benennen und diese bzw. diesen dem Bereichs-CIO laufend aktualisiert mitzuteilen.

§ 11
Besondere Rechte und Pflichten der Administratorinnen und Administratoren

(1) Die Administration der IT Infrastruktur nach § 1 Abs. 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 Organisation und Umsetzung von Datenschutz- und -sicherungsmaßnahmen liegt in der Verantwortung der Administratorinnen und Administratoren.

(4) Im Falle einer dezentralen Nutzerverwaltung nach § 16 Abs. 6 verwaltet die Administratorin bzw. der Administrator insbesondere die erteilten Benutzungsberechtigungen und Bestandsdaten der Benutzerinnen und Benutzer, 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 § 11 Abs. 5, 6 und 8, nachvollziehbar zu dokumentieren.

§ 12
Haftung der Nutzerinnen und Nutzer

(1) Die Nutzerin bzw. der Nutzer haftet im Rahmen der rechtlichen Vorgaben für alle Schäden, die der Universität 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.

§ 13
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 Rechen- und Kommunikationstechnik sowie Software der TU Dresden für strafbare Handlungen missbrauchen oder
3. der TU Dresden durch sonstiges rechtswidriges Nutzerverhalten Nachteile zufügen.

(2) Maßnahmen nach Abs. 1 sollen grundsätzlich 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 Abs. 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 Abs. 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))[iii],
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.

§ 14
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 der Stabsstelle für Informationssicherheit vertraglich zu vereinbaren.

Abschnitt 3: Nutzung

§ 15
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 Technischen Universität Dresden.

(2) Die Zulassung zur Nutzung erfolgt ausschließlich für die Mitglieder der geschlossenen Benutzergruppe. Gäste nach § 3 Abs. 2 können nur zeitlich begrenzt Mitglied der geschlossenen Benutzergruppe sein. Voraussetzung für die Aufnahme von Gästen in die geschlossene Benutzergruppe ist die Feststellung der Erforderlichkeit der Inanspruchnahme der genannten Einrichtungen und Dienste zur Erfüllung der Aufgaben des Gastes an der TU Dresden nach § 15 Abs. 1.

(3) Soweit dies rechtlich nicht anders bestimmt ist, ist die Nutzung der IT Infrastruktur nach § 1 Abs. 1 für andere als im § 15 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 Nutzung der IT Infrastruktur nach § 1 Abs. 1 dieser Ordnung oder Teilen hiervon für andere Zwecke zu nutzen. In Zweifelsfällen ist dies durch die Stabsstelle für Informationssicherheit zu würdigen und eine bindende Entscheidung des CIO 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 die Stabsstelle für Informationssicherheit zu wenden. Der CIO entscheidet in diesen Fällen über die Zulassung zur Nutzung abschließend.

§ 16
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 § 16 Abs. 1 dürfen die Daten verarbeitet werden, die zur eineindeutigen Identifikation der Nutzerin bzw. des Nutzers sowie zur Sicherstellung des ordnungsgemäßen Geschäftsablaufes an der TU Dresden erforderlich sind.

(3) Daten nach § 16 Abs. 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.

(4) Nach dem Ausscheiden der Nutzerin bzw. des Nutzers 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.

(5) Die Nutzerinnen und Nutzer sind verpflichtet, ausschließlich mit den Benutzerkennungen zu arbeiten, deren Nutzung ihnen im Rahmen der Zulassung gestattet wurde. Die Weitergabe der Benutzerkennung ist unzulässig. 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 und dessen regelmäßige Änderung. Der Nutzerin bzw. dem Nutzer ist es untersagt, fremde Benutzerkennungen zu ermitteln und zu nutzen.

(6) Eine dezentrale Nutzerverwaltung ist zugelassen, wenn die zentrale Nutzerverwaltung nach § 16 Abs. 1 die erforderlichen Funktionalitäten nicht aufweisen und dies zur Erfüllung der Aufgaben der Struktureinheiten erforderlich ist. Für dezentrale Benutzerverwaltungen sind bezüglich der Informationssicherheit die gleichen Anforderungen wie an die zentrale Benutzerverwaltung des ZIH maßgebend.

Abschnitt 4: Besondere Bestimmungen für Groupware, E-Mail und Telefax

§ 17
Besondere Bestimmungen – Groupware

(1) Ziel des Einsatzes von Groupware-Systemen sind insbesondere die Sicherstellung und Vereinfachung arbeitsorganisatorischer Maßnahmen für die Zusammenarbeit von Nutzerinnen und Nutzern, Personengruppen, Teams und Gremien sowie das Kommunikationsmanagement.

(2) Die Leiterin bzw. der Leiter der Struktureinheit kann die Nutzung eines Groupware-Systems oder Teilen hiervon nur in dem Umfang anordnen, soweit dies zur ordnungsgemäßen Durchführung des Dienst- oder Arbeitsverhältnisses erforderlich ist.

(3) Die Zugriffsrechte sind transparent und nachvollziehbar zu gestalten und zu dokumentieren.

(4) Innerhalb von Groupware-Systemen dürfen ausschließlich die Daten, insbesondere Daten mit Personenbezug, verarbeitet werden, die zur ordnungsgemäßen und sachgerechten Erbringung des Dienstes erforderlich sind.

(5) Insbesondere für Groupware-Systeme gelten die einschlägigen gesetzlichen und rechtlichen Bestimmungen zur Vorabkontrolle und Aufnahme in das Verfahrensverzeichnis (Fußnote). Die Betreiber sind verpflichtet, hierzu rechtzeitig und vor Aufnahme des Produktivbetriebes der Stabsstelle für Informationssicherheit die erforderlichen Unterlagen zur Verfügung zu stellen. [1]

§ 18
Besondere Bestimmungen – E-Mail und Telefax

(1) Für Zwecke nach § 15 Abs. 1 sind die Nutzerinnen und Nutzer verpflichtet, ausschließlich die E-Mail-Adressen zu verwenden, die folgenden Namenskonventionen entsprechen: für das wissenschaftliche und nichtwissenschaftliche Personal: vorname.nachname[y]@tu-dresden.de und für die Studierenden und Gäste: vorname.nachname[y]@mailbox.tu-dresden.de. Für bestehende dezentrale E-Mail-Adressen gilt bzgl. der Empfangsberechtigung ein Bestandsschutz.

(2) E-Mail-Adressen und zentrale E-Mail-Verteilerlisten werden, sowie 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 Arbeitsverhält-

---

[1] § 10 des Gesetzes zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz – SächsDSG)vom 25. August 2003; rechtsbereinigt mit Stand vom 31. Juli 2011, Mitteilung des Prorektors für Universitätsplanung 2/2015 Führung eines Verfahrensverzeichnisses für die Verarbeitung von personenbezogenen und anderen besonders schutzwürdigen Daten

nisses, 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.

(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 Standardeinstellungen auf SPAM überprüft. Da Fehlbewertungen nicht vollständig ausgeschlossen werden können, übernimmt das ZIH keine Haftung dafür, dass ausschließlich SPAM-Mails als solche erkannt werden.

(8) Abzusendende E-Mails sind grundsätzlich mit einer elektronischen Signatur nach § 3 Abs. 8 zu signieren und zu verschlüsseln. Der Versand per E-Mail von besonders schutzwürdiger personenbezogener Daten sowie anderer Daten mit erhöhten 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 für einen begrenzten Zeitraum zulässig. Das ZIH stellt hierfür einen entsprechenden Dienst zur Verfügung. Automatisierte Weiterleitungen zu anderen Zwecken oder mit anderen kommunikationstechnischen Einrichtungen oder Diensten sind unzulässig.

(11) In den Struktureinheiten ist über Arbeitsanweisungen insbesondere unter entsprechender Anwendung der Bestimmungen der VwV Dienstordnung[iv] sowie unter Einhaltung der gesetzlichen und rechtlichen Bestimmungen mindestens Folgendes zu regeln:

1. Maßnahmen zum Schutz von personenbezogenen und anderen Daten mit erhöhtem Schutzbedarf bei elektronischer Kommunikation,
2. Kommunikationsweg sowie Registrierung von ein- und ausgehenden E-Mails,
3. Absenderberechtigung,
4. Abwesenheitsmitteilungen,
5. Archivierung von E-Mails und
6. Vertretungsregelungen.

(12) Das ZIH stellt die technischen Möglichkeiten zur Einhaltung dieser Regelung bereit. Die Stabsstelle für Informationssicherheit stellt zur Einhaltung der Sicherheitsziele angepasste Prozesse, Aktions- und Reaktionspläne bereit.

(13) Die Übertragung von sensiblen personenbezogenen Daten per Telefax soll nur in Ausnahmefällen erfolgen, wobei angemessene Sicherheitsvorkehrungen zu treffen sind.

Abschnitt 5: Datenschutz

§19
Verarbeitung von personenbezogenen und anderen besonders schutzwürdigen Daten

(1) Der Aufwand für den Schutz von personenbezogenen oder besonders schutzwürdigen Daten muss in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen. Für die Verarbeitung personenbezogener Daten gelten die hierfür einschlägigen gesetzlichen und rechtlichen Bestimmungen. Die Empfehlungen der bzw. des Sächsischen Datenschutzbeauftragten sind zu beachten.

(2) Für den Nachweis der getroffenen Schutzmaßnahmen nach § 19 Abs. 1 sind insbesondere die Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[v], in der jeweils aktuellen Fassung maßgeblich.

Abschnitt 6: Software

§ 20
Software-Beschaffung, -Verwaltung, -Nutzung und -Lizenzierung

(1) Beim Einsatz von Software sind die für das Projekt gültigen Lizenzbestimmungen des Herstellers und die Software-Nutzungsbedingungen des ZIH bzw. des Dezernats Organisation und Prozessmanagement einzuhalten. Die TU Dresden ist immer Lizenznehmerin.

(2) Alle für die dienstliche Nutzung zu beschaffenden Software-Produkte an der TU Dresden sind im Benehmen mit dem Dezernat Organisation und Prozessmanagement 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) Der Abschluss von Campusverträgen obliegt grundsätzlich dem ZIH.

(4) 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.

(5) 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.

(6) Studierendenlizenzen sind der Nutzung durch Studierende auf deren privaten Rechnern vorbehalten. Ausnahmen sind nur mit Zustimmung des Softwareherstellers möglich.

(7) 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. Zudem sind die Sicherungskopien unverzüglich zu vernichten. Ist der Verbleib einer Sicherungskopie für Archivierungszwecke dringend erforderlich, so ist die Genehmigung des Herstellers diesbezüglich einzuholen.

(8) Die Nutzerin bzw. der Nutzer ist berechtigt, die Software nur in der lizenzierten (beim ZIH bestellten) 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.

(9) Bei Ausscheiden der Nutzerin bzw. des Nutzers aus dem Dienstverhältnis mit der TU Dresden sind alle Lizenzen dem jeweiligen Lizenzpool der Struktureinheit zurückzuführen.

(10) Das ZIH ist berechtigt im Falle einer Lizenzüberprüfung (Audit) durch den Software-Hersteller eine TU-weite Überprüfung in Abstimmung mit der Stabsstelle für Informationssicherheit durchzuführen.

(11) Von Softwareherstellern verlangte Audits über den Einsatz der Software sind mit der Stabsstelle für 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.

(12) Bei der Benutzung von Software, Dokumentationen und anderen Daten sind die gesetzlichen Vorgaben, insbesondere zum Urheberrechtsschutz, einzuhalten und die Lizenzbedingungen, unter denen Software, Dokumentationen und Daten zur Verfügung gestellt werden, zu beachten. Dies gilt auch für Open-Source-Software. Insbesondere ist bei allen angebotenen Download-Möglichkeiten für Software unter der GNU General Public Licence (GPL) darauf zu achten, dass die GPL gewahrt wird.

Abschnitt 7: Informationssicherheit

§ 21
Grundsätze

(1) Zur Erreichung und Aufrechterhaltung eines angemessenen und ausreichenden Informationssicherheitsniveaus sind für die TU Dresden insbesondere die Standards und Maßnahmenkataloge 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.

§ 22
Besondere Informationssicherheitsziele

Die nach § 19 Abs. 2 getroffenen Schutzmaßnahmen sollen in Abhängigkeit vom Sachverhalt und vom Schutzbedarf der Daten insbesondere folgende Schutzziele erreichen.

(1) Vertraulichkeit
Sie erfordert, dass Informationen lediglich von autorisierten Benutzerinnen bzw. autorisierten Benutzern gelesen bzw. modifiziert werden können.

(2) Integrität
Sie erfordert, dass Informationen gegen unbeabsichtigte Veränderung und vorsätzliche Verfälschung zu schützen sind.

(3) Verfügbarkeit
Sie erfordert, dass der Zugriff auf Informationen innerhalb eines vereinbarten Zeitrahmens gewährleistet ist.

(4) Authentizität
Bezeichnet die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit einer Information.

(5) Transparenz
Sie erfordert, dass die Verfahrensweisen bei der Verarbeitung von Informationen vollständig zu dokumentieren sind, so dass sie in zumutbarer Zeit nachvollzogen werden können.

(6) Verbindlichkeit/Nichtabstreitbarkeit
Sie erfordert, dass „kein unzulässiges Abstreiten durchgeführter Handlungen“ bei der Verarbeitung von Informationen möglich ist. Erreichbar ist sie beispielsweise durch elektronische Signaturen.

§ 23
Rechte und Pflichten der Stabsstelle für Informationssicherheit

(1) Die Stabsstelle für 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 die Stabsstelle für Informationssicherheit bei der Erfüllung ihrer Aufgaben unterstützen. Der Stabsstelle für Informationssicherheit steht ein umfassendes Informationsrecht über Angelegenheiten zu, die für die Informationssicherheit relevant sind. Dazu sind der Stabsstelle für Informationssicherheit rechtzeitig alle Informationen zur Verfügung zu stellen, die zur Erfüllung ihrer Aufgaben von Bedeutung sein können. Sie kann alle Informationen verlangen, die für ihren Aufgabenbereich erforderlich sind.

(3) Der Stabsstelle für Informationssicherheit werden insbesondere folgende Aufgaben und Rechte zugewiesen:

1. Steuerung und Koordinierung des Informationssicherheitsprozesses an der TU Dresden,
2. Unterstützung des Rektorates 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 rechtliche Vorgaben zur Informationssicherheit,
7. umfassende Kontrolle und Bewertung 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 und Errichtung und Betrieb von technischen Einrichtungen mit besonderer Bedeutung für die Informationssicherheit,
10. jährliche Vorlage eines Tätigkeitsberichtes beim CIO und Abstimmung über die im Grundsatz zu bearbeitenden Themen des folgenden Berichtszeitraumes,
11. verbindliche Stellungnahmen zur Informationssicherheit mit Genehmigung des CIO,
12. Stellungnahmen und Hinweise mit Beachtenspflicht in eigener Verantwortung,
13. direkte sowie zeitnahe Information bei besonderer Eilbedürftigkeit und im Einzelfall gegenüber dem CIO oder eines Mitgliedes des Rektorates,
14. Planung, Organisation und Durchführung von Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit für Mitglieder und Angehörige der TU Dresden und
15. Beratung und Unterstützung der Mitglieder und Angehörigen der TU Dresden bei Fragen der Informationssicherheit.

§ 24
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 der Stabsstelle für Informationssicherheit mitzuteilen. Es ist gemäß den an der TU Dresden einschlägigen rechtlichen Bestimmungen zu verfahren.

Abschnitt 8: Schlussbestimmungen

§ 25
Inkrafttreten und Außerkrafttreten

Die Ordnung tritt am Tage nach der Veröffentlichung in den Amtlichen Bekanntmachungen der Technischen Universität Dresden in Kraft. Mit Inkrafttreten dieser Ordnung tritt die Ordnung für die Rechen- und Kommunikationstechnik und die Informationssicherheit an der TU Dresden vom 08. Januar 2009 außer Kraft.

Dresden, den 5. Januar 2016

Der Rektor
der Technischen Universität Dresden

Prof. Dr.-Ing. habil. DEng/Auckland Hans Müller-Steinhagen

Anlage: Verzeichnis der aufgeführten gesetzlichen Bestimmungen, Verwaltungsverordnungen und Standards

---

[i] Signaturgesetz (SigG)

[ii] Sächsisches Datenschutzgesetz (SächsDSG)

[iii] Strafgesetzbuch (StGB)

[iv] VwV Dienstordnung

[v] Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Die Bestimmungen sind in der jeweils gültigen Fassung anzuwenden.