Handreichung zur IT-Ordnung[1] - Stand 10. März 2021

Vorwort

Die Bereitstellung von IT-Infrastruktur an Hochschulen wirft im Nutzungsverhältnis eine Vielzahl von Fragen auf, für die ein Regelungsbedürfnis besteht. So besteht ein Bedürfnis zur Aufstellung grundlegender Regeln, die eine möglichst störungsfreie, ungehinderte und sichere Nutzung der IT-Infrastruktur gewährleisten. In diesem Zusammenhang stellen sich insbesondere die Fragen, welche grundlegenden Rechte und Pflichten den Betreiber:innen von IT-Infrastruktur sowie den zugelassenen Nutzer:innen zukommen und welche Zuständigkeiten innerhalb der Einrichtung bestehen.

Benutzungsordnungen dienen der grundsätzlichen und inhaltlichen Ausgestaltung des öffentlich-rechtlichen Nutzungsverhältnisses zwischen der Einrichtung und den Nutzer:innen, die IT-Infrastruktur in Anspruch nehmen. Sie erlangen somit für Benutzungsverhältnisse in Hochschulen besondere Bedeutung. Als verbindliches Regelungswerk für das Nutzungsverhältnis sind in Benutzungsordnungen alle Rechte und Pflichten der Beteiligten, Zuständigkeiten und insbesondere die Ermächtigungsgrundlagen für Sanktionen, wie etwa den Ausschluss von Nutzer:innen wegen missbräuchlicher Nutzung, enthalten. Für die rechtliche Einordnung als Rechtsnorm oder Verwaltungsnorm ist die Benennung des Regelungswerks als „Benutzungsordnung“, „Nutzungsrichtlinien“, „IT-Ordnung“ etc. unerheblich.

Als förmliche Ordnungen erlassene Benutzungsordnungen sind verbindliche Rechtsvorschriften, die die Universität als verwaltungsrechtliche Personalkörperschaft des öffentlichen Rechts Kraft ihrer Rechtssetzungskompetenz für Selbstverwaltungsaufgaben auf der Grundlage des jeweiligen Landeshochschulgesetzes erlassen kann. Sie binden alle Mitglieder und Angehörigen der Hochschule sowie sonstige Nutzer:innen, die aufgrund einer Zulassung die IT-Infrastruktur und IT-Dienste der Einrichtung in Anspruch nehmen[2].

Daher hat das Erweiterte Rektorat der TU Dresden auf Grund von § 13 Abs. 5 SächsHSFG mit Wirkung vom 18.02.2021 die Ordnung für die informationstechnischen Einrichtungen und Dienste und zur Informationssicherheit der TU Dresden (IT-Ordnung) erlassen.

Der vorliegenden Erläuterungen sollen den Betreiber:innen von IT-Infrastruktur und IT-Diensten, den Nutzer:innen und den Administrator:innen eine Hilfestellung bei der Anwendung der IT-Ordnung an der TU Dresden sein. Die jeweiligen Paragraphen und Absätze sind mit fortlaufenden Randnummern (Rd. 1 bis 22) markiert. Die zugehörigen Erläuterungen sind mit der entsprechenden Randnummer versehen.

Die folgenden Erläuterungen beziehen sich auf Anfragen der Mitglieder und Angehörige der TU Dresden. Sofern weiterer Erläuterungsbedarf besteht, wird die Handreichung erweitert. Bitte wenden Sie sich hierzu an das SG 3.5 Informationssicherheit (informationssicherheit@tu-dresden.de).

[1] Ordnung für die informationstechnischen Einrichtungen und Dienste und zur Informationssicherheit der TU Dresden (IT-Ordnung) in der Fassung vom 18.02.2021

[2] DFN - Rechtsguide - I. Benutzungsverhältnis

Inhaltsverzeichnis

Abschnitt 1: Allgemeine Bestimmungen

Ordnungstext
§ 1 Geltungsbereich

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

(Rd. 1)

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

(Rd. 2)

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

(Rd. 3)

Erläuterungen	
„IT-Infrastruktur" definiert i.S.d. Ordnung die Gesamtheit der technischen Infrastruktur (Räume, Netze, Server, Clients etc.) mit allen damit verbundenen IT-Diensten und der installierten Software, unabhängig davon, in welcher Art und Weise Dienste erbracht bzw. Hard- oder Software betrieben werden. Im folgenden Text der Erläuterung wird der Begriff IT-Infrastruktur in diesem Sinne verwendet.	**1**
Für Doktorand:innen wird z.B. auf die „Ordnung zur Verarbeitung von personenbezogenen Daten in der Promotionsphase an der TU Dresden" verwiesen. Für Informationen steht die Graduiertenakademie zur Verfügung.	**2**
Die Regelungen dieser Ordnung finden insbesondere dann keine Anwendung, wenn der Gegenstand der Forschung die Informations- und Datenverarbeitung auf Basis dafür bereitgestellter IT-Infrastruktur ist.	**3**

Ordnungstext
§ 3 Begriffsbestimmungen und Regelungsinhalte

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

(Rd. 4)

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

(Rd. 5)

(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.

(Rd. 6)

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

(Rd. 7)

Erläuterungen

4

Die Betreiber von **öffentlichen** Internetdiensten (z.B. Provider wie die Deutsche Telekom, Vodafone, 1und1 etc.) haben schon jetzt umfangreiche Verpflichtungen zur Protokollierung von Verbindungsdaten und zur Gewährung von Möglichkeiten zur Überwachung des Datenverkehrs für staatliche Sicherheitsinstitutionen zu erfüllen. Darüber hinaus bestehen für diese Anbieter:innen umfangreiche Melde- und Genehmigungspflichten bei der Bundesnetzagentur.

Hochschulen sind hiervon weitgehend ausgenommen, weil davon ausgegangen wird, dass sie ihre Dienste ausschließlich einer **geschlossenen Benutzergruppe** zur Verfügung stellen.
Eine geschlossene Benutzergruppe liegt dann vor, wenn die verbundenen Teilnehmer:innen einen gemeinsamen beruflichen Zweck verfolgen. Bei einer offenen Benutzergruppe hingegen stehen die Dienste jeder beliebigen bzw. jedem beliebigen Dritten zur Verfügung. An Hochschulen wird die Nutzung von IT-Infrastruktur nur den Bediensteten, dem wissenschaftlichen Personal und den Studierenden zur Verfügung gestellt, nicht aber Dritten, so dass eine geschlossene Benutzergruppe vorliegt. Die Hochschulen sind auch öffentliche Stellen der Länder. Damit finden die §§ 91 ff. TKG Anwendung. Zur geschlossenen Benutzergruppe gehören daher Mitglieder und Angehörige der TU Dresden. Gäste der TU Dresden, wenn diese die IT-Infrastruktur der TU Dresden zeitlich begrenzt in Anspruch nehmen müssen, können ebenfalls Mitglied der geschlossenen Benutzergruppe sein. Dies sind z.B. Gastwissenschaftler:innen, Mitarbeiter:innen von Drittmittelpartnern, externe Administratoren:innen etc. Insoweit sind diese Personen nicht als Dritte anzusehen.

Für die Hochschulen entstehen, insbesondere auf Grund der dann geltenden weiteren Bestimmungen des TKG, beträchtliche Verpflichtungen und Kosten, wenn sie den Status der geschlossenen Benutzergruppe verlieren würden. Dies gilt es unter allen Umständen zu vermeiden. Somit ist eine Nutzung durch Dritte, die nicht der geschlossenen Benutzergruppe angehören, untersagt.

Die Verantwortung der Administrator:innen bezieht sich ausschließlich auf die zu betreibende IT-Infrastruktur.	**5**
Elektronische Signaturen haben eine Vertrauens- und Identitätsfunktion durch die Möglichkeit zur digitalen Authentifizierung von Personen. Eine fortgeschrittene Signatur der DFN-PKI ermöglicht es allen Mitgliedern und Angehörigen der TU Dresden, elektronische Dokumente und E-Mails digital zu signieren (digitale Unterschrift). Diese elektronische Signatur kann für alle Verfahren zu Anwendung kommen, in denen die Schriftform, d.h. eine eigenhändige Unterschrift, nicht rechtlich bzw. gesetzlich bestimmt ist. Beantragung, Einrichtung und Nutzung von Zertifikaten	**6**
Ein Notfall ist ein Schadensereignis, bei dem Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren. Die Verfügbarkeit der entsprechenden Prozesse oder Ressourcen kann innerhalb einer geforderten Zeit nicht wiederhergestellt werden. Der Geschäftsbetrieb ist stark beeinträchtigt. Eventuell vorhandene SLAs (Service Level Agreements) können nicht eingehalten werden. Es entstehen hohe bis sehr hohe Schäden, die sich signifikant und in nicht akzeptablem Rahmen auf die Aufgabenerfüllung der TU Dresden auswirken. Notfälle können nicht mehr im allgemeinen Tagesgeschäft abgewickelt werden, sondern erfordern eine gesonderte Notfallbewältigungsorganisation. Wann genau ein Notfall für die TU Dresden bzw. eine ihrer Organisationseinheiten eintritt, muss anhand der jeweiligen Geschäftsprozesse betrachtet und definiert werden.	**7**

Abschnitt 2: Verantwortlichkeiten, Zuständigkeiten und Haftung

Ordnungstext

§ 6 Sachgebiet Informationssicherheit

(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.

(Rd. 8)

Erläuterungen

Das Computer Emergency Response Team (Computer-Notfallteam) der TU Dresden (TUD-CERT) hat zur Aufgabe und zum Ziel, alle Mitglieder und Angehörigen der TU Dresden bestmöglich bei der Verhinderung und Aufklärung von Cyberangriffen sowie bei der Behandlung von Sicherheitsvorfällen zu unterstützen. Dies wird insbesondere durch präventive (Warnungen, Schulungen), reaktive (Vorfallsmanagement) und forensische (digtal-forensische Untersuchungen nach Vorfällen) Maßnahmen realisiert.	**8**

Ordnungstext **§ 7 Zentrum für Informationsdienste und Hochleistungsrechnen (ZIH)**	
(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. (Rd.9)	
Erläuterungen	
In Datenverteilerräumen sind ab der Umstellung auf Voice over IP (VoIP) keine anderweitigen Nutzungen mehr zulässig. Das ZIH berät hinsichtlich Migration von dezentralen Dienste auf die zentralen Angebote und unterstützt bei der Erstellung des Dienstkonzepts. Für die Unterbringung von Servern und IT-Komponenten von TU-Struktureinheiten, die zur Dienstleistung nötig sind und für die das ZIH keinen alternativen zentralen Dienst anbietet, steht der Housing-Bereich des ZIH zur Verfügung. Die Nutzung kann erst nach vorheriger Abstimmung mit dem ZIH erfolgen.	**9**
Ordnungstext **§ 8 Dezentrale IT-Organisation**	
(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. (Rd. 10)	
(5) Die IT-Referentin bzw. der IT-Referent ist gegenüber den IT-Service-Teams (die sich aus den IT-Administrator:innen der Struktureinheiten zusammensetzen), sofern vorhanden, zur Umsetzung der unter Absatz 1 genannten Aufgaben der Bereichs-CDIOs und der CDIOs der Zentralen Wissenschaftlichen Einrichtungen weisungsbefugt. (Rd. 10)	

Erläuterungen

Im Rahmen des zur Verfügung stehenden Globalhaushalts für die Bereiche werden die Bereichs-CDIOs an den Entscheidungen zu IT-Beschaffungsmaßnahmen größer 25 T€ beteiligt. Die Bereichs-CDIO sind in die entsprechenden Gremien und Prozesse des Bereichs einzubinden, insbesondere in das Bereichskollegium. Die Nutzerinnen und Nutzer im Sinne dieser Ordnung sind verpflichtet, die Bereichs-CDIOs/ZWE-CDIOs bzw. deren Vertreterinnen und Vertreter bei der Wahrnehmung Ihrer Aufgaben zu unterstützen sowie deren Hinweise und Festlegungen zu beachten. Der IT-Referentin bzw. dem IT-Referenten eines Bereiches/ZWE/ZUV sind IT-Administrator:innen direkt unterstellt, für diese Personen im direkten Unterstellungsverhältnis gilt die Weisungsbefugnis im Umfang einer Führungskraft. Darüber hinaus haben die IT-Referent:innen auch die fachliche Weisungsbefugnis gegenüber den IT-Administrator:innen, die im Bereich an den Fakultäten, Professuren bzw. Instituten organisatorisch angebunden sind. Somit bilden alle IT-Administrator:innen eines Bereiches das IT-Service-Team.	**10**

Ordnungstext

§ 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.

(Rd. 11)

Zur wirksamen Umsetzung der IT-Ordnung auf allen Ebenen der TU Dresden ist es unabdingbar, dass die Leitung der Struktureinheiten auf deren Einhaltung in ihrem Verantwortungsbereich achten, um v.a. die Funktionsfähigkeit der Universität zu gewährleisten, den sorgfältigen Umgang mit Arbeitsmitteln sicher zu stellen und u.U. Schaden für die TU Dresden abzuwenden (Pflicht zur Wahrung der Belange der TU Dresden).	**11**

Ordnungstext

§ -10 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.

(Rd. 12)

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

(Rd. 12)

(3) Die technische Organisation und Umsetzung von Datenschutz- und -sicherungsmaßnahmen liegt in der Zuständigkeit - der Administrator:innen.

(Rd. 12)

(4) Im Falle einer dezentralen Nutzer:innenverwaltung nach § -15 Abs. 5 verwaltet die Administrator:innen insbesondere die erteilten Benutzungsberechtigungen und Bestandsdaten der Nutzer:innen, die in ihrem Zuständigkeitsbereich liegen.

(Rd. 12)

(5) Die Administrator:innen sind auch mit Hilfe automatisierter Methoden berechtigt, die Inanspruchnahme der Datenverarbeitungssysteme und Software durch die einzelnen Nutzer:innen 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 Nutzer:innen,**
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.**

(Rd. 12)

(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, können die Administrator:innen die Nutzung von Ressourcen vorübergehend einschränken oder einzelne Benutzer:innenkennungen vorübergehend sperren. Die betroffenen Nutzer:innen 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 Nutzer:in unterbleiben. Für einen Missbrauch müssen tatsächliche und dokumentierte Anhaltspunkte vorliegen.

(Rd. 12)

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

(Rd. 12)

(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, können die Administrator:innen, 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 Nutzer:in einzuholen. In jedem Fall sind die betroffenen Nutzer:innen unverzüglich über die getroffenen Maßnahmen zu unterrichten. Zur Aufklärung und Unterbindung von Missbräuchen oder soweit dies bei der Verfolgung von Straftaten erforderlich ist, können die Information der Nutzer:innen unterbleiben. Für einen Missbrauch oder für eine Straftat müssen tatsächliche und dokumentierte Anhaltspunkte vorliegen.

(Rd. 12)

(9) Die Administrator:innen sind verpflichtet, alle Maßnahmen, insbesondere solche nach § 10 Abs. 5, 6 und 8, nachvollziehbar zu dokumentieren.

(Rd. 12)

Im Rollenmodell der TU Dresden sind diverse IT-Rollen beschrieben, dabei werden unterschiedliche Rollen für Administrator:innen/Betreuer:innen/Ansprechpartner:innen betrachtet: ▪ IT – Ansprechpartner:in ▪ Arbeitsplatzbetreuer:in ▪ Pool Administrator:in ▪ Pool-Disponent:in ▪ Pool-Aufsicht ▪ Server-Administrator:in ▪ Netzwerk-Ansprechpartner:in ▪ Domänen-Administrator:in Die Aufgaben der o.g. Rollen sind insbesondere: IT – Ansprechpartner:in: ▪ Allg. Ansprechpartner:in zu IT-Themen (z.B. Bedarfsfragen bezüglich Hardware) ▪ Multiplikator:in für relevante Informationen aus dem CDIO Strategie-Rat und IT-Koordiniserungsstab ▪ Erster, lokaler Ansprechpartner:in bei Sicherheitsvorfällen (z.B. zur Trennung eines PC vom Netzwerk) Arbeitsplatzbetreuer:in: ▪ Umsetzung der Vorgaben zu IT-Themen ▪ Bereitstellung und Betreuung von IT-Technik für die Endanwender:innen ▪ Erstinstallation von PCs ▪ Installation von Software ▪ Durchführen von Software-Updates ▪ Anbinden von peripheren Endgeräten Pooladministrator:in: ▪ Umsetzung der Vorgaben zu IT-Themen ▪ Entwicklung und Umsetzung eines an die fachspezifischen Anforderungen ausgerichteten rechnergestützten Poolkonzeptes ▪ Installation, Wartung und Sicherstellung der Verfügbarkeit der Arbeitsplätze, Server, Netzwerkkomponenten und peripheren Endgeräte ▪ Planung und Umsetzung spezifischer Mechanismen zur flexiblen Softwareverteilung, zum Management von Software-Updates, zur Sicherstellung von Datenschutz und Datensicherheit und zur Unterstützung der Lehrenden und Studierenden ▪ Entwicklung eines Organisationsmodells zum Poolbetrieb ▪ Anleitung des Pooldisponent:in und der Poolaufsichten Pool-Disponent:in: ▪ Organisation der Poolbetriebsführung o Öffnungszeiten o Nutzer:innenordnung o Schließkonzept o Verwaltung der Zugangskontrolle ▪ Organisation der Poolbetreuung o SHK/WHK Verträge	**12**

- Schulung

Pool-Aufsicht:
- fachliche und technische Unterstützung der Lehrenden und Studierenden,
- organisatorische Aufgaben und Sicherstellung des geregelten Poolbetriebs
- Erster Ansprechpartner:in für Poolnutzer:innen

Server-Administrator:in:
- Umsetzung der Vorgaben zu IT-Themen
- Auswahl, Beschaffung von Serverkomponenten bzw. Auswahl einer geeigneten virtuellen Umgebung
- Erstinstallation
- Installation von Software
- Durchführen von Software-Updates
- Konfiguration der Dienste
- Betrieb der Server
- Monitoring der Server
- Dokumentation der Serverlandschaft

Netzwerk-Ansprechpartner:in:
- Lokale Verwaltung der IP Adressen, sofern dies delegiert wurde
- Abstimmung mit anderen Ansprechpartner:innen und Nerzwerktechniker:innen
- Patchen und Anschluss der Endgeräte
- Erster Ansprechpartner:in bei Netzwerkproblemen
- Dyport-Verwaltung, wenn nicht übergeordnet verwaltet
- VoIP Abstimmung mit zentralem VoIP-Verwalter:in

Domänen-Administrator:in:
- Umsetzung der Vorgaben zu IT Themen
- Verwaltung von Berechtigungen in den zugewiesenen Organisationseinheiten
- Zuweisung von Gruppenrichtlinien
- Softwareverteilung aus Repository
- Verwaltung von Gruppenrechten und –mitgliedschaften

Für weiterführende Informationen zum Rollenmodell steht das Dezernat 6 zur Verfügung.

Leitfaden für Administrator:innen (Ansprechpartner: Herr Dr. Lohse)
Rechtliche Hinweise des DFN-Vereins für IT-Administrator:innen

Abschnitt 3: Nutzung

Ordnungstext

§ 15 Nutzerinnen- und Nutzerverwaltung

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

(Rd. 13)

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

(Rd. 14)

Erläuterungen

Eine Besonderheit sind sogenannte Funktionslogins, wie z.B. DezernatX@tu-dresden.de. Hierbei muss seitens der für das Funktionslogin Verantwortlichen (Antragsteller des Funktionslogins) sichergestellt werden, dass nur Befugte (z.B. mehrere Sekretariate) Zugriff auf dieses Login erhalten. Diesen Befugten kann das ZIH-Login und Passwort zur Kenntnis gegeben werden. Für weiterführende Informationen steht der Service-Desk der TU Dresden zur Verfügung.	**13**
Vorzulegen sind dazu insbesondere ein Betriebs- und ein Sicherheitskonzept mit einem Votum des SG 3.5 Informationssicherheit. Die Nutzer:innenverwaltung garantiert die Beschränkung der Nutzung auf die „geschlossene Benutzer:innengruppe“, für die der DFN-Verein der TU Dresden einen Internet-Zugang bereitstellt. Ein anonymer Zugang beliebiger Nutzer:innen zu den Ressourcen der TU und ins Internet ist auszuschließen.	**14**

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

Ordnungstext

§ 16 Namenskonventionen

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

(Rd. 15)

Erläuterungen

Für die Bereitstellung von Domains ist ausschließlich das ZIH zuständig. Dieses bezieht die Domains über die externen Domain-Dienstleister (das DFN und die Firma INWX). Die Beantragung einer neuen Domain wird über den Web-Support websupport@tu-dresden.de gesteuert, um ggf. Abweichungen von der Namenskonvention mit einer entsprechenden Beschlussvorlage klären zu lassen und ggf. weitere Anforderungen zu klären. Nach dortiger Beratung erfolgt der komplette Service bis zur Bereitstellung durch das ZIH. Die Beantragung von Subdomains bzw. Hostnamen unter tu-dresden.de erfolgt über den Service-Desk (servicedesk@tu-dresden.de) beim ZIH. Weitere Informationen sind im Service-Katalog des ZIH unter DNS zu finden.	**15**

Ordnungstext

§ 17 Besondere Bestimmungen für- E-Mail

(7) Jede eingehende E-Mail wird vor ihrer Weiterverarbeitung nach dem Stand der Technik - auf SPAM bewertet. Dabei können die Nutzer:innen die Bewertung selbst konfigurieren sowie festlegen, ob die dann als SPAM bewerteten E-Mails abgewiesen werden oder als SPAM bewertet zugestellt werden sollen.

(Rd. 16)

(8) Durch das wissenschaftliche und nichtwissenschaftliche Personal abzusendende E-Mails (aus der Domäne @tu-dresden.de) sind mit einer elektronischen Signatur nach § 3 Abs. 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.

(Rd. 17)

(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.

(Rd. 18)

(10) Für wissenschaftliche Zwecke ist eine Weiterleitung von E-Mails nach Ausscheiden der Nutzer:in 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.

(Rd. 19)

Erläuterungen

Jede eingehende E-Mail wird von aktuellen Tools seitens des ZIH auf SPAM überprüft und nach verschiedenen Kriterien bewertet. Die Nutzer:innen haben über Einstellungen in ihrem Mail-Client die Möglichkeit, zu entscheiden, wie mit den entsprechend bewerteten Nachrichten verfahren wird. Eine entsprechende Konfigurationshilfe ist hier zu finden.	**16**
Abgehende E-Mails sind grundsätzlich zu verschlüsseln, sofern dies technisch möglich ist. Dies ist unter dem Begriff „grundsätzlich" zu verstehen. Weitere Informationen (insbesondere zur Nutzung von OWA Web App) sind auf der Webseite des ZIH zu Exchange zusammengestellt. Sofern der bzw. die Empfänger:in kein Mitglied bzw. Angehöriger der TU Dresden ist und kein Zertifikat zur Verschlüsselung besitzt (z.B. Industriepartner:in, Bewerber:in) steht der Dienst SecureMail zur verschlüsselten Kommunikation zur Verfügung. Weitere Informationen zu SecureMail sind zu finden unter: https://tu-dresden.de/securemail	**17**
Eine automatisierte Weiterleitung von dienstlichen E-Mails kann dazu führen, dass sensible Informationen und Daten den Einflussbereich der TU Dresden verlassen und bei Dritten verarbeitet werden, die keiner Kontrolle der TU Dresden unterliegen. Darüber hinaus ist davon auszugehen, dass der bzw. die Absender:in in der Regel keine Kenntnis davon hat, dass seine E-Mail, die er an einen Empfänger:in an der TU Dresden versendet, an einen externen Dienstleister weitergeleitet wird. Ausführliche Hinweise sind hier zu finden.	**18**
Weiterführende Informationen zum Nachsendeportal hier zu finden.	**19**

Ordnungstext

§ 18 Richtlinien für Webseiten

(1) Struktureinheiten der TU Dresden sind angehalten, sich über den zentralen Webauftritt der TU Dresden zu präsentieren. Für Kooperationsprojekte mit externen Partner:innen 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.

(Rd. 20)

Erläuterungen

Ausnahmeanträge sind bei Bedarf an den Web-Support websupport@tu-dresden.de zu richten. Dabei ist es hilfreich, bereits eine kurze Begründung bzw. erste Informationen zum Projekt zu nennen (z.B. zu den Partner:innen und zur Rolle der TU Dresden). Ausgehend von der sich daran anschließenden Beratung und Klärung aller erforderlichen Aspekte der Webseite wird eine Empfehlung zur Entscheidung durch den CDIO ausgesprochen. Erst nach schriftlicher Freigabe durch den CDIO kann die gewünschte Ausnahme Anwendung finden. Ggf. findet eine abschließende Überprüfung der Webseite nach deren Livegang statt, um die Umsetzung der Barrierefreiheit und anderer Vorgaben zu überprüfen.	**20**

Abschnitt 5: Informationssicherheit und Datenschutz

Ordnungstext

§ 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.

(Rd. 21)

Erläuterungen

Es sind angemessene - d.h. verhältnismäßige - Schutzmaßnahmen nach dem Stand der Technik zu treffen. Die zu treffenden Schutzmaßnahmen sind maßgeblich vom Schutzbedarf der zu verarbeitenden Daten abhängig. Diese werden in der Richtlinie zur Informationssicherheit in der Mitteilung des Prorektors für Universitätsentwicklung 5/2017 beschrieben. Für weiterführende Informationen steht das SG 3.5 Informationssicherheit zur Verfügung.	**21**

Abschnitt 6: Software und Hardware

Ordnungstext

§ 22 Hardware- und Software-Beschaffung, -Verwaltung, -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.

(Rd. 22)

(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.

(Rd. 22)

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

(Rd. 22)

(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.

(Rd.22)

Erläuterungen

22

Die Beschaffung von Software unterliegt den Regeln der Beschaffungsrichtlinien der TUD.

Im Vorfeld der Beschaffung ist der Bedarf an Software mit dem ZIH und wenn es um Software zum Einsatz im administrativen Bereich geht, D6, einzubeziehen. Beide Organisationseinheiten stehen beratend zur Seite, sowohl, was die bereits zur Verfügung stehenden Softwareprodukte, als auch die Auswahl neuer Produkte angeht. Speziell im administrativen Bereich muss eine Prüfung erfolgen, ob vorhandene IT-Systeme einen neuen Bedarf an Software bereits abdecken können. Das betrifft sowohl vorhandene Lizenzen, als auch nutzbare Funktionalitäten (z.B. neue Funktionen im SAP).

Die Beschaffung neuer Software, die der Ausschreibung unterliegt, erfordert darüber hinaus umfangreiche Ausschreibungsdokumente gemäß EVB-IT. Die Beratung zur Erstellung dieser Unterlagen erfolgt im SG 1.2 und im Dezernat 6.

Weiterführende Informationen:
ZIH Softwarebeschaffung
Dezernat 6
SG 1.2 Zentrale Beschaffung und Anlagenbuchhaltung

Bei der privaten Nutzung von dienstlich bereitgestellter Software ist darauf zu achten, ob die jeweiligen Lizenzbestimmungen dies zulassen. Zum Beispiel kann die dienstlich bereitgestellte Software Sophos (Virenschutz) auch privat eingesetzt werden, weitere Informationen sind auf der Sophos-Webseite des ZIH zu finden.

Für Open-Source-Software entfallen in der Regel die Beschaffungsschritte, weil sie kostenfrei genutzt werden kann. Sofern Support-Verträge für Open-Source-Software erforderlich sind, gelten die o.g. Beschaffungsrichtlinien in gleicher Weise.

Open-Source-Lizenzen enthalten neben dem Recht der kostenfreien Nutzung zum Teil auch Pflichten, die einzuhalten sind. Dies gilt insbesondere für die Pflicht zur Veröffentlichung der Quellen in den GPL-Lizenzen (GNU Public Licence, es existieren verschiedene Versionen), sobald die Software in irgendeiner Form veröffentlicht oder verbreitet wird.	