



Amtliche Bekanntmachungen

Herausgegeben im Auftrag des Rektors von der Abteilung Hochschulrechtliche, akademische u. hochschulpolitische Angelegenheiten,
Straße der Nationen 62, 09111 Chemnitz - Postanschrift: 09107 Chemnitz

Nr. 29/2012

27. Juli 2012

Inhaltsverzeichnis

Rahmenordnung für die Nutzung der Informations- und Kommunikationsdienste und Seite 1355
die Informationssicherheit an der Technischen Universität Chemnitz
(IuK-Rahmenordnung) vom 27. Juli 2012

Rahmenordnung für die Nutzung der Informations- und Kommunikationsdienste und die Informationssicherheit an der Technischen Universität Chemnitz (IuK-Rahmenordnung) vom 27. Juli 2012

Auf der Grundlage von § 13 Abs. 5 Satz 1 i.V.m. § 83 Abs. 2 Satz 1 des Gesetzes über die Hochschulen im Freistaat Sachsen (Sächsisches Hochschulgesetz – SächsHSG) vom 10. Dezember 2008 (SächsGVBl. S. 900), das zuletzt durch Artikel 5 des Gesetzes vom 4. Oktober 2011 (SächsGVBl. S. 380, 391) geändert worden ist, hat das Rektorat nachstehende Ordnung erlassen:

Inhaltsverzeichnis

1. Abschnitt - Allgemeine Bestimmungen

- § 1 Geltungsbereich
- § 2 Gegenstand der Ordnung

2. Abschnitt - Informations- und Kommunikationsdienste

- § 3 Nutzungszweck und Zulassung zur Nutzung
- § 4 Verarbeitung personenbezogener Daten
- § 5 Kommunikationsnetz, Host- und Domainnamen
- § 6 Zentrale Benutzererkennung
- § 7 E-Mail
- § 8 Telekommunikation
- § 9 Informationssysteme
- § 10 Software
- § 11 Sanktionen bei Missbrauch
- § 12 Haftung des Nutzers
- § 13 Haftung der Technischen Universität Chemnitz
- § 14 Rechte und Pflichten des Administrators
- § 15 Rechte und Pflichten des Leiters einer Struktureinheit

3. Abschnitt - Informationssicherheit

- § 16 Beteiligte im Informationssicherheitsprozess
- § 17 Informationssicherheits-Management-Team (SMT)
- § 18 IT-Sicherheitsbeauftragter der Universität
- § 19 IT-Sicherheitsbeauftragte der Fakultäten, Zentralen Einrichtungen und der Verwaltung (Dezentrale IT-Sicherheitsbeauftragte)
- § 20 Informationssicherheitskonzept
- § 21 Notfallpläne
- § 22 Übergangsbestimmungen
- § 23 Inkrafttreten

In dieser Ordnung gelten grammatisch maskuline Personenbezeichnungen gleichermaßen für Personen männlichen und weiblichen Geschlechts. Frauen können die Funktionsbezeichnungen dieser Ordnung in weiblicher Form führen.

1. Abschnitt Allgemeine Bestimmungen

§ 1 Geltungsbereich

(1) Diese Ordnung gilt für alle informations- und kommunikationstechnischen Einrichtungen, Systeme und Dienste der Technischen Universität Chemnitz, für deren Nutzung und für die Gesamtheit der Benutzer.

(2) Die Festlegungen dieser Ordnung und der hieraus entstehenden Rahmenrichtlinien sind bei Vereinbarungen und Verträgen mit An-Instituten und außeruniversitären Einrichtungen, die direkt an das Kommunikationsnetz der Technischen Universität Chemnitz angeschlossen sind oder über dieses Teilnehmer des Deutschen Forschungsnetzes (DFN) sind, zu beachten.

(3) Die Inanspruchnahme der in Absatz 1 genannten Einrichtungen und Dienste ist ausschließlich durch Mitglieder einer geschlossenen Benutzergruppe und zu Zwecken des § 3 dieser Ordnung zulässig. Zur geschlossenen Benutzergruppe gehören abschließend folgende Personen:

1. Mitglieder und Angehörige der Technischen Universität Chemnitz, sowie
2. sonstige natürliche Personen, die die in Absatz 1 genannten Einrichtungen und Dienste zur Erfüllung von Aufgaben nach § 3 zeitlich begrenzt in Anspruch nehmen (Gäste).

§ 2 Gegenstand der Ordnung

Gegenstand dieser Ordnung ist die Regelung sowohl der Nutzungsmöglichkeiten und Rechte als auch der verbindlich einzuhaltenden Pflichten für die in § 1 Abs. 1 genannten Einrichtungen, Systeme und Dienste. Weiterhin sind die Festlegungen der zur Realisierung eines hochschulweiten Informationssicherheitsprozesses erforderlichen Verantwortungsstrukturen, einer Aufgabenzuordnung sowie die Zusammenarbeit der Beteiligten geregelt.

2. Abschnitt Informations- und Kommunikationsdienste

§ 3 Nutzungszweck und Zulassung zur Nutzung

(1) Die Zulassung zur Nutzung erfolgt ausschließlich zu Zwecken, welche der Erfüllung der, der Technischen Universität Chemnitz nach § 5 SächsHSG obliegenden Aufgaben einschließlich der insoweit erforderlichen Verwaltungstätigkeit, insbesondere auch der nach § 6 SächsHSG, dienen.

(2) Die Nutzung der Einrichtungen, Systeme und Dienste nach § 1 Abs. 1 für andere Zwecke ist nur zulässig, wenn sie geringfügig ist, die Nutzung der Informations- und Kommunikationsdienste durch die anderen Nutzer nicht behindert oder stört und die dienstliche Aufgabenerfüllung nicht beeinträchtigt wird.

(3) Die Vergabe von Nutzungsberechtigungen für die Einrichtungen, Systeme und Dienste nach § 1 Abs. 1 erfolgt zeitlich befristet.

(4) Das Rektorat kann im Ausnahmefall abweichend von den Absätzen 1 und 2 die Nutzung der Einrichtungen, Systeme und Dienste nach § 1 Abs. 1 für weitere Zwecke genehmigen. Für die Nutzung von Software gilt § 10.

(5) Einrichtungen, Systeme und Dienste nach § 1 Abs. 1 dürfen unberechtigten Nutzern nicht zugänglich gemacht werden.

§ 4

Verarbeitung personenbezogener Daten

(1) Der Aufwand für Datenschutz- und Datensicherungsmaßnahmen muss in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen. Für die Beurteilung der Schutzwürdigkeit (Sensibilität) personenbezogener Daten gilt die Schutzbedarfsfeststellung nach § 20 Abs. 1 Nr. 3. Als Grundlage für die Zulässigkeit der Verarbeitung und den Schutz solcher Daten dient die Gesamtschutz-Stufe.

(2) Die Verarbeitung von personenbezogenen Daten ist ohne die Erstellung, Umsetzung und Kontrolle eines Informationssicherheitskonzeptes nach § 20, in denen die besonderen Sicherheitsvorkehrungen definiert werden, unzulässig. Es sind nach dem jeweiligen Stand der Technik Maßnahmen zu treffen und zu dokumentieren, um zu gewährleisten, dass

- nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
- personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),
- personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
- jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),
- festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
- die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, so dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

(3) Jede Struktureinheit kann die Verarbeitung fremder Dateien, die personenbezogene Informationen enthalten, auf ihren Rechnern in Ausnahmefällen im Auftrag eines Dritten zulassen. Verantwortlich für die Zulässigkeit der Datenverarbeitung, für die Vorgaben zur Einhaltung der Bestimmungen zum Datenschutz sowie für die Kontrolle deren Umsetzung ist der Auftraggeber.

(4) Für die Veröffentlichung personenbezogener Daten auf elektronischem Wege (Telefon-, Lehrveranstaltungsverzeichnisse, Forschungsinformationssysteme u. a.) finden die einschlägigen Bestimmungen des Sächsischen Datenschutzgesetzes in der jeweils gültigen Fassung Anwendung. Anderenfalls ist eine schriftliche Einwilligung des Betroffenen erforderlich.

§ 5

Kommunikationsnetz, Host- und Domainnamen

(1) Der Betrieb des Kommunikationsnetzes (Campusnetz) obliegt dem Universitätsrechenzentrum (im Folgenden URZ). Das URZ definiert dabei in Abstimmung mit dem am Rektorat verorteten CIO-Board Sicherheitsvorgaben und setzt diese Maßnahmen um. Alle Schutzmaßnahmen werden im Dokument "Schutzmaßnahmen im Kommunikationsnetz" fortgeschrieben.

- (2) Der Verantwortungsbereich des URZ erstreckt sich bis zum definierten Übergabepunkt am Kommunikationsnetz für das IP-Endgerät (z.B. Dosen-Port im Büro, WLAN-Infrastruktur). Ab diesem Übergabepunkt liegt die Verantwortung für das IP-Endgerät beim Nutzer bzw. Administrator. Der Nutzer bzw. Administrator ist verpflichtet, alle Maßnahmen für Datenschutz- und Sicherheit zu ergreifen.
- (3) Netzübergänge zwischen dem Kommunikationsnetz, dem Internet sowie Netze von Kooperationspartnern dürfen ausschließlich vom URZ realisiert werden.
- (4) Für die Technische Universität Chemnitz ist im weltweiten Domain Name Service (DNS) die Domain tu-chemnitz.de registriert. Das Universitätsrechenzentrum ("URZ") verwaltet die Domain sowie deren Subdomains.
- (5) Alle an das Kommunikationsnetz der Technischen Universität Chemnitz angeschlossenen Endgeräte sollen einen eindeutigen Namen (Hostnamen) in der Domain erhalten. Eindeutige Hostnamen werden nach dem Schema *Hostname.Subdomain.tu-chemnitz.de* gebildet. Für den Teil „Subdomain“ wird die Abkürzung der Fakultät, der Fachrichtung oder der jeweiligen zentralen Einrichtung verwendet. Über die Vergabe von Subdomains entscheidet das URZ. Der Teil „Hostname“ wird vom Nutzer festgelegt. Eine weitere Unterteilung in Untereinheiten ist möglich.
- (6) Der Eintrag von Hostnamen direkt unterhalb der Domain tu-chemnitz.de kann in Ausnahmefällen auf Antrag an das URZ erfolgen und bedarf der Zustimmung des Rektorates bzw. dessen Beauftragten.
- (7) Die Vergabe von IP-Adressen wird durch das URZ geregelt.

§ 6

Zentrale Benutzererkennung

- (1) Für die nach § 1 Abs. 3 nutzungsberechtigten Personen werden vom URZ eindeutige Benutzerkennungen gebildet und verwaltet. Der Benutzerkennung sind dienstbezogene Identifikationsmerkmale zugeordnet (Passworte, PINs, Chipkarten u.ä.). Die Kenntnis bzw. der Besitz eines zu einer Benutzerkennung zugeordneten Identifikationsmerkmals identifiziert einen Nutzer gegenüber einem Dienst und bildet die Basis für die Erteilung von Berechtigungen bei deren Benutzung. Die Benutzerkennung bleibt bis zur Aktivierung durch den Nutzer entsprechend dem § 21 des Gesetzes zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz – SächsDSG) vom 25. August 2008 (SächsGVBl. S. 330), zuletzt geändert durch das Zweite Gesetz zur Änderung des Sächsischen Datenschutzgesetzes vom 14. Juli 2011 (SächsGVBl. S. 270) für die Nutzung gesperrt. Ist die zentrale Benutzerkennung gesperrt, können alle Dienste nicht genutzt werden, die über die zentrale Benutzerkennung authentifiziert werden. Für bestimmte Dienste kann eine gesonderte Freischaltung der Benutzerkennung notwendig sein. Vor Aktivierung der zentralen Benutzerkennung ist die Benutzerordnung des URZ anzuerkennen.
- (2) Für den Nutzerkreis nach § 1 Abs. 3 Nr. 1 findet zur Sicherstellung des Vorhandenseins der Nutzungsbefugnis nach § 1 Abs. 3 Nr. 1 sowie zur eindeutigen Identifizierung und damit zur Aktualität der Benutzerkennung regelmäßig ein Datenabgleich zwischen dem URZ und der zuständigen personalverwaltenden Stelle bzw. dem Studentenservice statt. Dazu werden Daten übermittelt und vom URZ verarbeitet.
- (3) Für den Nutzerkreis nach § 1 Abs. 3 Nr. 2 kann die Verarbeitung von personenbezogenen Daten zur Sicherstellung des Vorhandenseins der Nutzungsbefugnis nach § 1 Abs. 3 Nr. 2 sowie zur eindeutigen Identifizierung und damit zur Aktualität der Benutzerkennung nur auf Antrag an das URZ erfolgen. Der Antrag bedarf der Schriftform, wenn nicht wegen besonderer Umstände eine andere Form als angemessen erscheint. Die Identität des Antragstellers muss jedoch zweifelsfrei feststellbar sein.

(4) Die Nutzer sind verpflichtet, ausschließlich mit den Benutzerkennungen und Identifikationsmerkmalen zu arbeiten, deren Nutzung ihnen im Rahmen der Zulassung gestattet wurde. Die Weitergabe von Identifikationsmerkmalen ist unzulässig. Jeder Nutzer hat dafür Sorge zu tragen, dass unberechtigten Personen die Nutzung seiner Benutzungskennung verwehrt wird. Dazu gehören die sorgfältige Wahl eines nicht einfach zu erratenden Passwortes und dessen regelmäßige Änderung. Dem Nutzer ist es untersagt, fremde Identifikationsmerkmale zu ermitteln, in Besitz zu nehmen und zu nutzen. Für Administratoren gelten die Regelungen in § 14.

(5) Das Sperren zentraler Benutzerkennungen auf Grundlage des § 11 erfolgt durch die Leitung des URZ bzw. deren Beauftragte.

§ 7 E-Mail

(1) Der ein- und ausgehende E-Mail Verkehr der Technischen Universität Chemnitz erfolgt über das zentrale Mailrelay am URZ. Das URZ trifft alle erforderlichen Maßnahmen zum ordnungsgemäßen Betrieb des Mailrelays.

(2) Für alle ein- und ausgehenden E-Mails findet eine Prüfung auf Schadprogramme statt. E-Mails mit als schädlich erkanntem Inhalt werden abgewiesen.

(3) Jede ein- und ausgehende E-Mail wird auf Spam-Merkmale untersucht. Entsprechend nutzerspezifischer Einstellungen werden als Spam eingestufte E-Mails abgewiesen, gelöscht oder markiert. Da Fehlbewertungen nicht vollständig ausgeschlossen werden können, übernimmt das URZ keine Haftung dafür, dass ausschließlich Spam-Mails und dass alle Spam-Mails als solche erkannt werden.

(4) Alle ein- und ausgehenden E-Mails mit ungültigen Absender- oder Empfängeradressen werden automatisch abgewiesen.

(5) Die Festlegung sowie die technische und administrative Umsetzung der erforderlichen Maßnahmen nach Abs. 1 bis 4 wird in einer E-Mail-Dienstbeschreibung des URZ im Benehmen mit dem Datenschutzbeauftragten der Technischen Universität Chemnitz dokumentiert und fortgeschrieben.

(6) E-Mail-Adressen für die Studierenden werden aus *Vorname.Nachname@sJAHR.tu-chemnitz.de* gebildet. Für alle anderen Nutzergruppen werden E-Mail-Adressen aus *Vorname.Nachname@Subdomain.tu-chemnitz.de* gebildet. Bei Namensdopplungen werden andere Formen gebildet.

(7) Bei Bedarf wird eine strukturbezogene oder funktionsbezogene E-Mail-Adresse bestehend aus *struktureinheit@Subdomain.tu-chemnitz.de* oder *funktion@Subdomain.tu-chemnitz.de* vergeben.

(8) Detaillierte Regelungen zur Vergabe und Nutzung von E-Mail-Adressen sind in entsprechenden Dienstvereinbarungen festzulegen.

§ 8 Telekommunikation

(1) Zur Wahrung des Fernmeldegeheimnisses werden die nach dem Stand der jeweils aktuellen Technik erforderlichen Maßnahmen getroffen, um den Schutz der Sprachkommunikation sicherzustellen. Diese Maßnahmen sind in einem Sicherheitskonzept zu dokumentieren.

(2) Weiterhin gelten die Festlegungen der Dienstvereinbarung zwischen der Technischen Universität Chemnitz und dem Personalrat der Technischen Universität Chemnitz über den Betrieb und die Nutzung eines auf Voice-over-IP basierenden Telekommunikationssystems in der jeweils gültigen Fassung.

§ 9

Informationssysteme

(1) Das URZ betreibt für die Technische Universität Chemnitz zentrale Informationssysteme (z.B. Webserver) und setzt erforderliche Schutzmaßnahmen um. Alle Maßnahmen werden in entsprechenden Dienstbeschreibungen dokumentiert.

(2) Der Betrieb dezentraler Informationssysteme erfolgt in Verantwortung der jeweiligen Struktureinheit. Die Struktureinheit ist für die Umsetzung aller notwendigen Schutzmaßnahmen verantwortlich.

§ 10

Software

(1) Die Mitglieder, Angehörigen und Gäste der Technischen Universität Chemnitz dürfen Software ausschließlich zur Lösung von Aufgaben nach § 3 Abs. 1 einsetzen.

(2) Beim Einsatz von Software sind die für das jeweilige Produkt gültigen Lizenzbestimmungen einzuhalten.

(3) Kopien von Softwareprodukten dürfen nur in dem Umfang angefertigt werden, der zum Schutz der Anwendung notwendig ist (Sicherungskopie).

(4) Die private Nutzung der von der Technischen Universität Chemnitz erworbenen Software setzt voraus, dass diese Nutzungsform in Vertrags- oder Lizenzbestimmungen bzw. vom Hersteller ausdrücklich genehmigt ist und dass keine dienstlichen Belange entgegenstehen.

(5) Eine dienstliche Nutzung von Software der Technischen Universität Chemnitz auf privater Hardware muss in den jeweiligen Vertrags- oder Lizenzbestimmungen gestattet sein.

(6) Die Nutzung von privat erworbener Software für dienstliche Zwecke muss durch die Lizenzbestimmungen abgedeckt sein und bedarf der Zustimmung des Leiters der Struktureinheit.

(7) Je nach Softwarevertrag erhält der Nutzer das zeitlich unbefristete oder zeitlich befristete Nutzungsrecht. Ist die Nutzung zeitlich befristet, so ist nach Ablauf dieser Nutzungsfrist die Software in eigener Verantwortung und ohne Aufforderung des URZ zu deinstallieren. Zudem sind die Sicherungskopien unverzüglich zu vernichten.

§ 11

Sanktionen bei Missbrauch

(1) Nutzer können vorübergehend oder dauerhaft in der Benutzung der Einrichtungen, Systeme und Dienste nach § 1 Abs. 1 eingeschränkt oder ganz ausgeschlossen werden, wenn diese

- schuldhaft gegen diese Ordnung verstoßen (missbräuchliches Verhalten) oder
- die Informations- und Kommunikationsdienste sowie Software der Technischen Universität Chemnitz schuldhaft für rechtswidrige, insbesondere auch strafbare Handlungen missbrauchen oder
- der Technischen Universität Chemnitz durch sonstiges schuldhaftes rechtswidriges Nutzerverhalten Nachteile zufügen oder
- den Versuch einer Handlung nach Nummer 1 bis 3 begehen

(2) Maßnahmen nach Absatz 1 sollen erst nach vorheriger Anhörung erfolgen.

(3) Im Fall des hinreichend begründeten Verdachts des Vorliegens einer Handlung nach Absatz 1, können die betreffenden Nutzer vorübergehend in der Benutzung eingeschränkt oder ganz ausgeschlossen werden, bis die Sach- und Rechtslage hinreichend geklärt ist. Absatz 5 gilt entsprechend.

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

(5) Eine dauerhafte Nutzungseinschränkung oder der vollständige Ausschluss eines Nutzers von der weiteren Nutzung kommt nur bei schwerwiegenden bzw. wiederholten Verstößen im Sinne von Absatz 1 sowie dann in Betracht, wenn 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 vom Ausgeschlossenen in schriftlicher Form auf dem Dienstweg bzw. im Fall von Studenten über den zuständigen Dekan glaubhaft zu machen.

(6) Auf die folgenden Straftatbestände wird besonders hingewiesen:

- Ausspähen von Daten (§ 202a StGB),
- Abfangen von Daten (§ 202b StGB),
- Vorbereiten des Ausspähens und Abfangens von Daten (§ 202 c StGB),
- Datenveränderung (§ 303a StGB) und Computersabotage (§ 303b StGB),
- Computerbetrug (§ 263a StGB),
- Verbreitung pornographischer und gewalt- und tierpornographischer Schriften und gleichgestellter Darstellungen (§§ 184, 184a, 11 Abs. 3 StGB)
- Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Schriften und gleichgestellter Darstellungen (§§ 184b, 184c, 11 Abs. 3 StGB),
- Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB) und Volksverhetzung (§ 130 StGB),
- Gewaltdarstellung (§ 131 StGB)
- Beschimpfungen von Bekenntnissen, Religionsgesellschaften und Weltanschauungsvereinigungen (§ 166 StGB)
- Ehrdelikte wie Beleidigung oder Verleumdung (§§ 185 ff. StGB),
- Fälschung beweiserheblicher Daten (§ 269 StGB) und Täuschung im Rechtsverkehr bei Datenverarbeitung (§ 270 StGB)
- Strafbare Urheberrechtsverletzungen, z. B. durch lizenz- und urheberrechtswidrige Nutzung, Vervielfältigung und Weitergabe (§ 106 ff. UrhG).

(7) Des Weiteren kommen gegen Beschäftigte und Beamte der Technischen Universität Chemnitz arbeits- bzw. disziplinarrechtliche Maßnahmen in Betracht. Bei strafbarem Verhalten bzw. bei einem entsprechenden hinreichenden Verdacht soll Strafanzeige erstattet werden.

§ 12

Haftung des Nutzers

(1) Die Haftung ergibt sich aus den gesetzlichen Bestimmungen. Hingewiesen wird insbesondere auf zivilrechtliche Schadensersatzansprüche, das Urheber- und Markenrecht. Weiterhin kommt eine strafrechtliche Verantwortlichkeit in Betracht.

(2) Der Nutzer haftet für alle Nachteile, die der Technischen Universität Chemnitz durch die missbräuchliche oder rechtswidrige Verwendung der Informations- und Kommunikationsdienste sowie von Software nach § 10 bzw. durch Nichteinhaltung seiner Verpflichtung aus dieser Ordnung entstehen.

(3) Der Nutzer haftet auch für Schäden, die im Rahmen der ihm zur Verfügung gestellten Zugriffs- und Nutzungsmöglichkeiten infolge der Nutzung durch Dritte entstanden sind, wenn er deren Nutzung zu vertreten hat.

(4) Der Nutzer hat die Technische Universität Chemnitz von allen Ansprüchen freizustellen, wenn Dritte diese wegen eines missbräuchlichen oder rechtswidrigen Verhaltens des Nutzers auf Schadensersatz, Unterlassung oder in sonstiger Weise in Anspruch nehmen.

(5) Hiervon unberührt bleiben die einschlägigen arbeitsvertraglichen oder dienstrechtlichen Haftungseinschränkungen sowie die hierzu entwickelten Grundsätze der Rechtsprechung.

§ 13

Haftung der Technischen Universität Chemnitz

(1) Die Technische Universität Chemnitz übernimmt keine Garantie oder Gewährleistung dafür, dass die Informations- und Kommunikationsdienste sowie die an der Universität eingesetzte Software fehlerfrei und jederzeit ohne Unterbrechung verfügbar sind. Insbesondere können eventuelle Datenverluste infolge technischer Störungen sowie die Kenntnisnahme vertraulicher Daten durch unberechtigte Zugriffe Dritter nicht ausgeschlossen werden. Die Verwendung privat erworbener Software des Nutzers erfolgt auf dessen eigenes Risiko. Eine Haftung der Technischen Universität Chemnitz ist bei der Verwendung solcher Software durch den Nutzer ausgeschlossen.

(2) Die Technische Universität Chemnitz übernimmt keine Verantwortung, Gewährleistung oder Garantie für die zur Verfügung gestellte Software. Weiterhin haftet die Technische Universität Chemnitz nicht für den Inhalt, insbesondere nicht für die Richtigkeit, Vollständigkeit und Aktualität der Informationen, zu denen sie lediglich den Zugang zur Nutzung vermittelt.

(3) Die Technische Universität Chemnitz haftet im Übrigen nur bei grober Fahrlässigkeit und Vorsatz ihrer Mitarbeiter.

§ 14

Rechte und Pflichten des Administrators

(1) Die Administration von Rechnern muss kooperativ, sachgerecht und zweckgebunden erfolgen. Bei Mehrnutzersystemen ist eine abgestimmte Nutzerverwaltung erforderlich. Anonyme Benutzungsformen von Rechnern am Kommunikationsnetz sind, mit Ausnahme frei zugänglicher Informationsrechner bzw. -systeme und im Rahmen von genehmigten Veranstaltungen, unzulässig.

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

(3) Die Organisation von Datensicherungsmaßnahmen liegt in der Verantwortung der Administratoren.

(4) Der Administrator verwaltet die erteilten Benutzungsberechtigungen und Bestandsdaten der Benutzer, die in seinem Verantwortungsbereich liegen.

(5) Soweit dies zur Störungsbeseitigung, zur Systemadministration und -erweiterung oder aus Gründen der Systemsicherheit, zum Schutz der nutzereigenen Daten sowie zur Aufklärung und Unterbindung von Handlungen nach § 11 Abs. 1 erforderlich ist, kann der Administrator die Nutzung der Ressourcen vorübergehend einschränken oder einzelne Benutzerkennungen vorübergehend sperren. Sofern möglich, sind die betroffenen Nutzer hierüber im Voraus zu unterrichten. Zur Aufklärung und Unterbindung von Handlungen nach § 11 Abs. 1 kann, bis zur Aufklärung der Sach- und Rechtslage, die vorherige Information des Nutzers unterbleiben. Für einen Missbrauch müssen tatsächliche und dokumentierte Anhaltspunkte vorliegen

(6) Der Administrator ist berechtigt, die Inanspruchnahme der Informations- und Kommunikationsdienste in seinem Verantwortungsbereich durch die einzelnen Nutzer auszuwerten, soweit dies erforderlich ist:

1. zur Gewährleistung eines ordnungsgemäßen Systembetriebs,
2. zur Ressourcenplanung und Systemadministration,
3. zum Schutz der personenbezogenen Daten anderer Nutzer,
4. zu Abrechnungszwecken,
5. für das Erkennen und Beseitigen von Störungen sowie
6. zur Aufklärung und Unterbindung von Handlungen nach § 11 Abs. 1.

(7) Unter den Voraussetzungen von Abs. 6 Nr. 1, 5, 6 und soweit dies zur Beseitigung aktueller Störungen oder zur Aufklärung und Unterbindung von Handlungen nach § 11 Abs. 1 unbedingt

erforderlich ist, ist der Administrator berechtigt, unter Beachtung des Datengeheimnisses bzw. der geltenden datenschutzrechtlichen Bestimmungen und vorheriger Information des Nutzers Zugriff auf die benutzereigenen Dateien zu nehmen. Liegen erhebliche und dokumentierte Anhaltspunkte für eine Handlung nach § 11 Abs. 1 vor, kann die vorherige Information des Nutzers bis zur Aufklärung der Sach- und Rechtslage nach § 11 Abs. 3 unterbleiben.

(8) Alle Maßnahmen nach Abs. 5, 6 und 7 sind nachvollziehbar zu dokumentieren. Der Nutzer ist von den getroffenen Maßnahmen unverzüglich in Kenntnis zu setzen.

(9) Die Übermittlung von Nutzungsdaten durch den Administrator an Dritte ist unzulässig, soweit das SächsHSG, die datenschutzrechtlichen Bestimmungen oder die Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 des Gesetzes vom 25. Juni 2012 (BGBl. I S. 1374) geändert worden ist, in ihren jeweils gültigen Fassungen keine Ausnahmen fordern oder zulassen.

(10) Vom Softwarehersteller verlangte Audits über den Einsatz der Software sind mit dem Datenschutzbeauftragten der Technischen Universität Chemnitz abzustimmen. Nach Unterrichtung des Leiters der Struktureinheit ist der Administrator berechtigt, die für die Auswertungen benötigten Angaben bereitzustellen.

§ 15

Rechte und Pflichten des Leiters einer Struktureinheit

(1) Der Leiter einer Struktureinheit ist für die Gewährleistung des ordnungsgemäßen Betriebes der Informations- und Kommunikationseinrichtungen, Systeme und Dienste in seinem Verantwortungsbereich einschließlich der Veranlassung erforderlicher Sicherheitsmaßnahmen zuständig.

(2) Der Leiter einer Struktureinheit ist für den ordnungsgemäßen Umgang der ihm zugeordneten Personen nach § 1 Abs. 3 Satz 2 Nr. 1 mit den genutzten Einrichtungen der Informationstechnologie sowie den Softwareressourcen und für die Einhaltung dieser Ordnung zuständig. Dies gilt ebenso für Personen nach § 1 Abs. 3 Satz 2 Nr. 2, deren Nutzung der Einrichtungen nach § 1 Abs. 1 sowie der Software in der jeweiligen Struktureinheit erfolgt.

(3) Der Leiter einer Struktureinheit hat, soweit dies der Umfang des Betriebes der Informations- und Kommunikationseinrichtungen oder der dort eingesetzten Systeme und Dienste erfordert, in seinem Verantwortungsbereich einen oder mehrere Administratoren benennen. Der Administrator muss in einem Dienst- oder Vertragsverhältnis zur Technischen Universität Chemnitz stehen.

(4) Die Administratoren sind durch den Leiter auf das Datengeheimnis nach § 6 SächsDSG zu verpflichten.

3. Abschnitt Informationssicherheit

§ 16

Beteiligte im Informationssicherheitsprozess

(1) Die strategische Zuständigkeit für den Informationssicherheitsprozess obliegt dem Rektorat. Bei der Wahrnehmung seiner Verantwortlichkeit wird das Rektorat durch das als Rektoratskommission nach § 83 Abs. 3 Satz 2 SächsHSG eingesetzte CIO-Board sowie das Informationssicherheits-Management-Team (SMT) nach § 17 unterstützt.

(2) Die weiteren Beteiligten im Informationssicherheitsprozess sind:

1. der IT-Sicherheitsbeauftragte der Technischen Universität Chemnitz nach § 18,
2. der Datenschutzbeauftragte der Technischen Universität Chemnitz,
3. die dezentralen IT-Sicherheitsbeauftragten nach § 19,

4. das URZ,
5. alle Einrichtungen der Technischen Universität Chemnitz, die nach § 1 dieser Ordnung Informations- und kommunikationstechnische Einrichtungen sowie Systeme der Universität mit den zugehörigen elektronischen Informations- und Kommunikationsdiensten in Anspruch nehmen.

(3) Das SMT ist für die Einbindung der Beteiligten nach Absatz 2 in den Informationssicherheitsprozess zuständig.

§ 17

Informationssicherheits-Management-Team (SMT)

(1) Mitglieder des SMT sind:

1. ein Vertreter des Rektorates,
2. ein Vertreter des CIO-Boards, soweit der Vertreter des Rektorates nach Nummer 1 diesem nicht angehört
3. der Datenschutzbeauftragte der Technischen Universität Chemnitz,
4. der IT-Sicherheitsbeauftragte der Technischen Universität Chemnitz nach § 18,
5. ein Vertreter der IT-Kommission nach § 7 der Ordnung des Universitätsrechenzentrums vom 25. Juli 2012 in der jeweils geltenden Fassung
6. ein Vertreter des URZ,
7. ein Vertreter der dezentralen IT-Sicherheitsbeauftragten nach § 19,

(2) Das SMT wird vom IT-Sicherheitsbeauftragten der Technischen Universität Chemnitz geleitet. Die Amtszeit des SMT entspricht der des Rektorates. Die Dauer der Amtszeit der Mitglieder in ihren jeweiligen Ämtern oder Funktionen nach dieser Ordnung oder anderen Regelungen außerhalb des SMT bleibt hiervon unberührt. Das SMT führt die Geschäfte über die Amtszeit hinaus bis zur Konstituierung eines neuen SMT fort.

(3) Das SMT unterstützt das Rektorat bei der Wahrnehmung der Verantwortlichkeiten zur Informationssicherheit. Es hat das Recht, sich in Sicherheitsfragen direkt an das Rektorat zu wenden. Die endgültige Entscheidung obliegt dem Rektorat.

(4) Das SMT ist für die Erstellung und Fortschreibung der Informationssicherheitsrahmenrichtlinie, sowie der Umsetzung und Überwachung des Informationssicherheitsprozesses verantwortlich. Die Struktureinheiten müssen das SMT bei der Erfüllung seiner Aufgaben unterstützen. Dem SMT steht ein umfassendes Informationsrecht über Angelegenheiten zu, die für die Informationssicherheit relevant sind. Dazu sind dem SMT rechtzeitig alle Informationen zur Verfügung zu stellen, die zur Erfüllung der Aufgaben von Bedeutung sein können. Das SMT kann alle Informationen verlangen, die für seinen Aufgabenbereich wichtig sind. Insbesondere gilt dies für die Prüfung und Analyse von IT-Sicherheitsvorfällen.

(5) Das SMT initiiert und bestätigt die für die zentralen IT-Verfahren erforderlichen Schutzbedarfsfeststellungen.

(6) Das SMT gibt die hochschulinternen technischen Standards zur Informationssicherheit vor. Außerdem veranlasst es die Schulung und Weiterbildung der dezentralen IT-Sicherheitsbeauftragten sowie die Unterstützung bei der Umsetzung der Informationssicherheitsrahmenrichtlinie.

(7) Die Einrichtungen der Universität sind verpflichtet, bei allen relevanten Planungen, Verfahren und Entscheidungen mit Bezug zur Informationssicherheit, die jeweils zuständigen dezentralen IT-Sicherheitsbeauftragten sowie das SMT zu beteiligen.

(8) Das SMT dokumentiert sicherheitsrelevante Vorfälle und erstellt jährlich einen Informationssicherheitsbericht.

§ 18

IT-Sicherheitsbeauftragter der Universität

(1) Dem IT-Sicherheitsbeauftragten obliegen folgende Aufgaben:

1. Steuerung und Koordinierung des Informationssicherheitsprozess
2. Unterstützung des Rektorates bei der Wahrnehmung der Verantwortlichkeiten zur Informationssicherheit,
3. Initiierung und Koordinierung der Erstellung der Informationssicherheitsrahmenrichtlinie der Universität,
4. Koordinierung sicherheitsrelevanter Projekte und Sicherstellung des Informationsflusses zwischen dem SMT und den dezentralen IT-Sicherheitsbeauftragten,
5. Untersuchung sicherheitsrelevanter Zwischenfälle und
6. Initiierung und Steuerung von Maßnahmen zur Sensibilisierung und Schulung zur Informationssicherheit

Der IT-Sicherheitsbeauftragte berichtet dem Rektorat und dem SMT über seine Tätigkeit.

(2) Dem IT-Sicherheitsbeauftragten der TU Chemnitz steht ein umfassendes Informationsrecht über Angelegenheiten zu, die für die Informationssicherheit relevant sind. Insbesondere gilt dies für die Prüfung und Analyse von IT-Sicherheitsvorfällen. Zu diesem Zweck ist er berechtigt, in konkreten Einzelfällen weitere fachkompetente Administratoren, dezentrale Sicherheitsbeauftragte und anderes Personal heranzuziehen.

(3) Der IT-Sicherheitsbeauftragte darf selbst nicht für den Betrieb sicherheitsrelevanter Dienste und Verfahren verantwortlich sein. Er wird nach § 81 Abs. 1 Satz 1 Nr. 14 SächsHSG gewählt und bestellt. Seine Amtszeit entspricht der des Rektorates. Er führt die Geschäfte bis zur Bestellung seines Nachfolgers fort. Eine Wiederbestellung ist möglich.

§ 19

IT-Sicherheitsbeauftragte der Fakultäten, Zentralen Einrichtungen und der Verwaltung (Dezentrale IT-Sicherheitsbeauftragte)

(1) Die dezentralen IT-Sicherheitsbeauftragten und deren Stellvertreter werden für Fakultäten auf Vorschlag des Dekans vom Fakultätsrat, für Zentrale Einrichtungen durch den Direktor oder Leiter der Zentralen Einrichtung und für die Zentrale Universitätsverwaltung durch den Kanzler bestellt. Sie sind durch den Dekan oder den Direktor oder Leiter der Zentralen Einrichtung bzw. den Kanzler auf das Datengeheimnis (nach § 6 SächsDSG) zu verpflichten. Im Übrigen gilt § 18 Abs. 3 Satz 1.

(2) Die dezentralen IT-Sicherheitsbeauftragten sind für die Umsetzung aller mit dem SMT abgestimmten Sicherheitsbelange bei den IT-Systemen und Anwendungen sowie den Mitarbeitern in ihren Zuständigkeitsbereichen verantwortlich. Sie sind verpflichtet, sich auf dem Gebiet der Informationssicherheit weiterzubilden und ihr Wissen auf dem aktuellen Stand zu halten. § 18 Abs. 1 gilt für den jeweiligen Zuständigkeitsbereich der dezentralen IT-Sicherheitsbeauftragten entsprechend.

(3) Die Einsetzung von dezentralen IT-Sicherheitsbeauftragten entbindet die Leiter einer Struktureinheit nicht von ihrer Gesamtverantwortung für die Informationssicherheit in ihrem Zuständigkeitsbereich.

§ 20

Informationssicherheitskonzept

(1) Das Informationssicherheitskonzept der Technischen Universität Chemnitz besteht aus:

1. dieser Rahmenordnung,
2. der vom SMT zu erstellenden und fortzuschreibenden Informationssicherheitsrahmenrichtlinie,
3. der Schutzbedarfsfeststellung für die IuK-Verfahren der Universität und
4. den Notfallplänen nach § 21.

(2) Die Informationssicherheitsrahmenrichtlinie ist das zentrale Dokument im Informationssicherheitskonzept der Universität. Sie enthält die verbindlichen, grundsätzlich anzuwendenden Verfahren und Maßnahmen, durch deren Umsetzung die Informationssicherheit für die Universität sicherzustellen ist.

(3) Das Informationssicherheitskonzept orientiert sich an den Prinzipien, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI), insbesondere im BSI Standard 100-2 (IT-Grundschutz-Vorgehensweise) und in den IT-Grundschutzkatalogen, vorgegeben sind.

§ 21

Notfallpläne

(1) Die Notfallpläne sind von den Fakultäten, Zentralen Einrichtungen und der Zentralen Universitätsverwaltung der Technischen Universität Chemnitz unter Leitung der jeweils zuständigen dezentralen IT-Sicherheitsbeauftragten zu erstellen und zu aktualisieren. Die Notfallpläne berücksichtigen alle relevanten Einrichtungen und Systeme im jeweiligen Zuständigkeitsbereich.

(2) Für die Notfallpläne sind die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu beachten.

§ 22

Übergangsbestimmungen

(1) Der IT-Sicherheitsbeauftragte der Universität nach § 18 und die dezentralen IT-Sicherheitsbeauftragten nach § 19 werden spätestens 4 Monate nach dem Inkrafttreten dieser Ordnung eingesetzt. Das SMT für die Amtsperiode 2012/2017 konstituiert sich unmittelbar hiernach, spätestens bis zum Ablauf des 6. Monats nach dem Inkrafttreten dieser Ordnung.

(2) Die Informationssicherheitsrahmenrichtlinie, die Schutzbedarfsfeststellung sowie die Notfallpläne sind innerhalb von 11 Monaten nach dem Inkrafttreten dieser Ordnung in Kraft zu setzen.

(3) § 4 Abs. 1 Sätze 2 und 3 sowie Abs. 2 Satz 1 tritt nach dem Inkrafttreten des Informationssicherheitskonzeptes nach § 20, spätestens jedoch mit Ablauf des 12. Monats nach dem Inkrafttreten dieser Ordnung, in Kraft.

(4) Soweit Funktionsträger nach dieser Ordnung erstmalig bestellt werden, dauert deren Amtszeit bis zum Ende der Amtszeit des Rektorates der Wahlperiode 2012/2017. Die Amtszeit verkürzt sich durch die spätere Bestellung entsprechend.

§ 23

Inkrafttreten

Diese Ordnung tritt am Tag nach ihrer Veröffentlichung in den Amtlichen Bekanntmachungen der Technischen Universität Chemnitz in Kraft.

Ausgefertigt aufgrund des Beschlusses des Rektorates vom 24. Juli 2012.

Chemnitz, den 27. Juli 2012

Der Rektor
der Technischen Universität Chemnitz

Prof. Dr. Arnold van Zyl