Graz University of Technology

Richtlinie zur Informationssicherheit der Technischen Universität Graz

RL 92000 RLIS 114-01

Technische Universität Graz
Rechbauerstraße 12
A-8010 Graz
Telefon +43 (0) 316 873 / 0

	Erstellt	Geprüft	Freigegeben
Name	*Reinfried O. Peter/Manfred Stepponat*	*Claudia von der Linden*	*Rektoratsbeschluss*
Datum	*30.04.2021*	*28.05.2021*	*15.06.2021*
Klassifizierung	Vertraulichkeit niedrig	Verfügbarkeit niedrig	Integrität mittel

Zweck

Diese Richtlinie legt Regelungen fest, um die Informationssicherheit an der Technischen Universität Graz (TU Graz) sicherzustellen. Die Informationssicherheit dient dem Schutz von Daten, personenbezogenen Daten, Informationen und dem daraus entstandenem Wissen unabhängig vom gewählten Medium (elektronisch, schriftlich, mündlich etc.). Es soll dabei der Schutz der Informationen vor unberechtigtem Zugriff, unbefugter Kenntnisnahme und Preisgabe, vor Verlust, Zerstörung und vor Veränderung sichergestellt und die Nachvollziehbarkeit von Daten- und Informationsflüssen ermöglicht werden. Sie stellt somit insbesondere die Vertraulichkeit, Verfügbarkeit und Integrität unserer und der uns anvertrauten Daten- und Informationsbestände sicher.

Geltungsbereich

Diese Richtlinie gilt verpflichtend für alle Angehörigen der TU Graz im Sinne des Universitätsgesetzes.
Dritte, d.h. Personen, die nicht Angehörige der TU Graz sind, sind über vertragliche und sonstige Vereinbarungen in den jeweils relevanten Punkten zu verpflichten.

Verteiler

Mitteilungsblatt
TU4U

Gegenseitige Beziehungen

Es gelten die Verantwortlichkeiten gemäß dem Vollmachten- und Richtlinien-Handbuch der TU Graz.

Mitgeltende Unterlagen

Betriebsvereinbarung zur Telearbeit (Homeoffice)
Richtlinie für *Mobile Endgeräte* der TU Graz
EU Datenschutz-Grundverordnung (DSGVO) i.d.g.F.
Datenschutzgesetz (DSG) i.d.g.F.
Datenschutzerklärung der TU Graz
Satzungsteil Datenschutzordnung der TU Graz
Rahmeinbetriebsvereinbarung über die automationsgestützte Verarbeitung personenbezogener Daten von Arbeitnehmerinnen und Arbeitnehmern
Forschungsorganisationsgesetz (FOG) i.d.g.F.
Verhaltenskodex (Compliance Richtlinie der TU Graz)

Prozessverantwortung und Kontakt

Prozessverantwortung: Leitung des Zentralen Informatikdienst (ZID)
Kontakt für technische und Informationssicherheitsfragen: it-security@tugraz.at

Inhaltsverzeichnis

TEIL A Informationssicherheitsorganisation der TU Graz

In diesem Teil werden allgemeine organisatorische und strukturelle Regelungen festgelegt. Es ergeben sich keine unmittelbaren Handlungsanweisungen für den Einzelnen.

1. Die Regelungshierarchie zu Informationssicherheit

1.1. Zweck

Die Regelungshierarchie zu Informationssicherheit der TU Graz verdeutlicht die Abhängigkeiten zwischen Regelungen auf unterschiedlichen Stufen in Form einer hierarchischen Struktur und sorgt für die notwendigen begrifflichen Abgrenzungen.

1.2. Ebenen der Regelungshierarchie

1.2.1. Strategische Vorgaben

Die oberste Ebene „Strategische Vorgaben“ umfasst die langfristige Ausrichtung der TU Graz, Mission, Vision, Leitbilder, Entwicklungspläne, Schwerpunktprogramme, Leistungsvereinbarungen etc.

1.2.2. Sicherheitspolitik inkl. -strategie und -organisation

Die Sicherheitspolitik und -strategie drückt die Ansichten und Einstellungen sowie die Verantwortungshaltung des Rektorats aus, unter anderem in Form von Grundsatzaussagen (Prinzipien) und strategischen Formulierungen. Sie beschreibt auf einer übergeordneten Ebene, was zu tun ist, beinhaltet das Mandat für die Umsetzung ihres Inhalts, d.h. erteilt den ausdrücklichen Auftrag dazu, gibt Ziele vor und legt Verantwortlichkeiten fest. Die Einhaltung der Sicherheitspolitik und -strategie durch die Angesprochenen ist verpflichtend.
Beispiel einer Formulierung: „Die Vertraulichkeit von Information muss entsprechend den gesetzlichen Vorgaben und ihrer Sensitivität gewährleistet sein.“

1.2.3. Sicherheitsrichtlinienabschnitte

Die Sicherheitsrichtlinienabschnitte sind verbindliche Regelwerke zum Zweck der Umsetzung der Sicherheitspolitik und -strategie. Sie erwähnen Personen, Technologien, Methoden und Prozeduren auf prozessorientierter Ebene und erläutern, wie das, was in der Sicherheitspolitik und -strategie festgelegt ist, umzusetzen ist. Ihre Einhaltung ist verpflichtend.
Beispiel: “Sensible Daten und Informationen, die über Netzwerke übertragen werden, sind zu verschlüsseln. Dabei sind die Normen *X* und *Y* einzuhalten.“

1.2.4. Sicherheitsstandards (Technikstandards)

Technische Standards sind verbindliche Regelwerke zum Zweck der Umsetzung der Prozessstandards. Sie beschreiben Prozeduren, Konfigurationsparameter und sonstige Details auf technischer Ebene und erläutern, wie das, was in den Prozessstandards festgelegt ist, umzusetzen ist. Ihre Einhaltung ist verpflichtend.
Beispiel: „E-Mails sind mittels S/MIME folgendermaßen zu verschlüsseln: *abc*. Die Verschlüsselung von ruhenden Daten ist folgendermaßen zu konfigurieren: *xyz*.“

1.2.5. Arbeitsanweisungen/ Unterstützende Dokumente und Materialien

Arbeitsanweisungen

Arbeitsanweisungen sind konkrete Anleitungen, die die Einzelne oder den Einzelnen bei der Einhaltung der Richtlinien und Standards unterstützen. Ihre Einhaltung ist verpflichtend.
Beispiel einer Arbeitsanweisung: „Dokumente mit personenbezogenen Daten in Papierform sind zu schreddern."

Unterstützende Dokumente und Materialien

Z.B. Sensibilisierungsunterlagen wie Schulungspräsentationen, Poster, E-Mails, Erklärungstexte und Erläuterungen auf der Homepage des ZID.

2. Informationssicherheitspolitik

2.1. Zweck

Die Vermittlung von Wissen und Kenntnis in Forschung und Lehre ist ein Leitziel der TU Graz. Auch in der Mitarbeiterführung ist es der TU Graz ein Anliegen, umfassend und transparent zu kommunizieren, damit ihre Mitarbeiter in Anbetracht aller relevanten Informationen die für die TU Graz richtige Entscheidungen treffen können.
Gleichzeitig ist der TU Graz die Wahrung der Privatsphäre ihrer Angehörigen und sonstiger Personen ein zentrales Anliegen. Auch in Forschung und Lehre können Daten anfallen, die schützenswert sind. Solche Daten werden nur jene Personen zugänglich gemacht, welche sie für die Erfüllung Ihrer Aufgaben benötigen.
Die Informationssicherheitspolitik der TU Graz drückt die Ziele und die Verantwortungshaltung der Universitätsleitung aus und schafft damit den Rahmen für nachhaltiges Informationssicherheitsmanagement.
Von dieser Sicherheitspolitik umfasst sind alle Erscheinungsformen von Information, sei es in elektronisch verarbeiteter, schriftlicher oder mündlicher Form, oder in anderer Weise kommuniziert.
Nicht umfasst von dieser Sicherheitspolitik sind die Funktionen Objektschutz, Brandschutz, Arbeitsplatzsicherheit, Arbeitsmedizin und sonstige, nicht in erster Linie informationsbezogene Themenkreise.

2.2. Ziele

Allgemeine Informationssicherheitsziele der TU Graz sind:

- Schutz vor unberechtigtem Zugriff, unbefugter Kenntnisnahme und Preisgabe von Information (Vertraulichkeit).
- Schutz vor Verlust und Zerstörung von Information (Verfügbarkeit).
- Schutz vor ungewollter und manipulativer Veränderung von Information (Integrität).
- Schutz vor Verlust der Nachvollziehbarkeit von Informationsflüssen.

Neben diesen allgemeinen Zielen sollen Informationssicherheitsmaßnahmen die folgenden, gleichwertigen Ziele wirksam unterstützen:

- Einhaltung gesetzlicher Vorgaben und vertraglicher Vereinbarungen.
- Positionierung der TU Graz als vertrauensvolle, zuverlässige Partnerin, insbesondere im Forschungsbereich.
- Sicherstellung der Kontinuität des Betriebs.
- Schadensvermeidung und Schadensbegrenzung durch vorbeugende Sicherheitsmaßnahmen.
- Gewährleistung eines den Risiken angemessenen Sicherheitsniveaus.
- Entwicklung und Förderung eines umfassenden Sicherheitsbewusstseins und einer Sicherheitskultur.
- Unterstützung und Förderung der mit sicherheitsrelevanten Aufgaben betrauten Personen.

2.3. Umsetzung

Die Umsetzung dieser Sicherheitspolitik baut auf folgenden Säulen auf:

- **Informationssicherheitsstrategie**
  Details dazu finden sich im Abschnitt *Informationssicherheitsstrategie*.
- **Informationssicherheitsorganisation**
  Details dazu finden sich im Abschnitt *Informationssicherheitsorganisation*.

2.4. Pflichten des Einzelnen

Aus Sicht der Universitätsleitung ist Informationssicherheit ein wichtiges Thema. Die Ziele und die abgeleiteten Sicherheitsmaßnahmen werden von ihr daher in jeder Hinsicht getragen und unterstützt. Aufgrund der großen Bedeutung der Informationssicherheit sind alle Angehörigen der TU Graz sowie alle anderen Personen, die mit Daten und Informationen der TU Graz in Berührung kommen, verpflichtet, die auf sie anwendbaren Sicherheitsbestimmungen zu beachten und einzuhalten.

3. Informationssicherheitsstrategie

3.1. Zweck

Die Informationssicherheitsstrategie legt die langfristige Vorgehensweise bei der Umsetzung der Informationssicherheitspolitik der TU Graz, basierend auf grundlegenden Prinzipien, fest. Die dabei angestrebten Sicherheitsziele entsprechen den in der Informationssicherheitspolitik der TU Graz angeführten Zielen.

3.2. Angestrebtes Sicherheitsniveau

Die TU Graz setzt Sicherheitsmaßnahmen um, die sich durch eine Ausgeglichenheit zwischen Sicherheitsanforderungen einerseits und Funktionalität, Leistungsfähigkeit, Wirtschaftlichkeit sowie Bedienkomfort andererseits auszeichnen.
In Bezug auf die Vertraulichkeit, Verfügbarkeit, Integrität und Unverfälschtheit von Daten und Informationen strebt die TU Graz an, ein angemessenes Sicherheitsniveau zu implementieren.

Aus den ermittelten Schutzbedürfnissen[1] sind folglich entsprechende Maßnahmen[2] abzuleiten, wobei *Good Practices*[3] und „der Stand der Technik“ als Grundlage angesehen werden.

3.3. Prinzipien zur Erreichung der angestrebten Informationssicherheitsziele

3.3.1. Berücksichtigung von Informationssicherheit

Die Informationssicherheit wird in allen Vorhaben mitberücksichtigt.
Dies bedeutet insbesondere, dass die Informationssicherheit in Projekten als ein eigenständiges Projektziel und als gleichwertiges Ziel neben Funktionalität und Leistungsfähigkeit bei der Entwicklung, der Beschaffung und dem Einsatz von informationsverarbeitenden Systemen betrachtet wird.

Die verantwortliche Person ist dafür zuständig, sicherzustellen, dass der Schutzbedarf der Daten und Informationen berücksichtigt wird.

3.3.2. Orientierung an *Good Practice* Ansätzen

Informationssicherheit an der TU Graz orientiert sich an anerkannten Normen sowie folgenden *Good Practice*-Ansätzen:

- ISO/IEC 2700x[4]
- Österreichisches Informationssicherheitshandbuch[5]
- BSI Grundschutz[6]

Darüber hinaus können auch andere, international oder national anerkannte Normen und *Best Practice* Ansätze verwendet werden, die auf Besonderheiten einer Einsatzumgebung abgestimmt sind oder zwingend berücksichtigt werden müssen.

3.3.3. Klassifizierung durch Data-Owner

Die Klassifizierung (Schutzbedarfsfeststellung) sowie Autorisierung zur Nutzung der Daten und Informationen erfolgt durch deren *Data-Owner*[7], die Umsetzung der Vorgaben durch deren *Custodian*[8].

3.3.4. Anwendung des *Need-To-Know* Prinzips

Die Autorisierung zur Nutzung von schützenswerten Daten und Informationen orientiert sich an der auszuführenden Aufgabe. Das bedeutet, jeder Person sind nur jene Daten und Informationen zugänglich zu machen, die für die Erfüllung ihrer Aufgaben bzw. Ausübung Ihrer Rolle notwendig sind (Prinzip des notwendigen Wissens).

---

[1] siehe 3.4.3.
[2] Maßnahmen können organisatorischer, technischer und physischer Natur sein.
[3] Darunter wird eine grundsätzliche Normen- und Standardorientierung verstanden, z.B. an ISO/IEC Normen, COBIT und Branchenstandards (z.B. Gesundheitswesen).
[4] https://security.tugraz.at/iso27k (kostenpflichtige Norm)
[5] https://security.tugraz.at/sicherheitshandbuch
[6] https://security.tugraz.at/BSI
[7] Dieser Begriff ist vergleichbar mit dem des Auftraggebers/Verantwortlichen im Datenschutzrecht. *Data-Owner* (Dateneigentümer) sind z.B. Fachabteilungen, Institute, Beteiligungen, assoziierte Vereine, Kooperationspartner, Projektteams.
[8] Dieser Begriff ist vergleichbar mit dem der Dienstleisterin oder des Dienstleisters/der Auftragsverarbeiterin oder des Auftragsverarbeiters im Datenschutzrecht.

3.3.5. Anwendung des *Least-Privilege* Prinzips

Personen, Benutzer, Systeme, Programme etc. verfügen über so wenig Zutritts- bzw. Zugriffsrechte wie möglich. Das bedeutet, dass Rechte u.a. zum Betreten von Räumen, zum Lesen bzw. Anlegen, Schreiben, Ändern, Löschen von schützenswerten Daten, Ausführen von Programmen oder zur Übertragung von Berechtigungen, gemessen an der durchzuführenden Aufgabe, im jeweils geringstmöglichen Ausmaß erteilt sind (Prinzip der Vermeidung überschießender Rechte).

3.4. Vorgehensweisen zur Erreichung der angestrebten Ziele

Die zu wählenden Sicherheitsmaßnahmen sind durch das Informationssicherheitskernteam (ISKT) anhand von anerkannten Methoden und Standards nachvollziehbar herzuleiten, zu begründen, zu dokumentieren und anschließend regelmäßig aber auch anlassbezogen, auf ihre Wirksamkeit hin zu untersuchen.

3.4.1. Erfassung

Daten- und Informationsbestände inklusive dazugehöriger Prozesse und Ressourcen sind strukturiert zu erfassen und zu dokumentieren.

3.4.2. Zuordnung

Den Daten- und Informationsbeständen, dazugehörigen Prozessen und Ressourcen[9] sind eindeutige *Data-Owner* und *Custodian* zuzuordnen.

3.4.3. Ermittlung des Schutzbedarfs und Erstellung von Sicherheitskonzepten

Der Schutzbedarf der Daten- und Informationsbestände und der zugehörigen Prozesse und Ressourcen ist zu ermitteln, gegebenenfalls mit Hilfe entsprechend detaillierter Risikoanalysen und nach gängigen, anerkannten Methoden, zumindest entsprechend dem Stand der Technik und gemäß *Good Practices*.

Ausgehend vom Schutzbedarf sind entsprechende Sicherheitskonzepte[10] zu entwickeln und zu dokumentieren.

3.4.4. Umsetzung der Sicherheitskonzepte

Die entstandenen Sicherheitskonzepte sind mit den bereits geplanten und umgesetzten Maßnahmen abzugleichen. Die sich daraus ergebenden weiteren erforderlichen Maßnahmen sind zu realisieren, und damit das jeweilige Konzept insgesamt umzusetzen. Die Konzepte und Maßnahmen sind laufend an die aktuellen Gegebenheiten anzupassen.

3.4.5. Übernahme von Restrisiken

Restrisiken sind festzuhalten und zu bewerten. Die Verantwortung für die Restrisiken ist im Innenverhältnis zum Rektorat durch den zuständigen *Data-Owner* zu übernehmen.

---

[9] Umfasst Personen, Gebäude und deren Einrichtung, IT-Infrastruktur, IT-Systeme, Applikationen (Programme) etc.

[10] Mit dem Begriff Sicherheitskonzept wird ein Bündel aus organisatorischen, technischen und physische Maßnahmen bezeichnet. Zu diesen Maßnahmen gehören neben der Entwicklung von Richtlinien und Standards auch Prozess- und Architekturbeschreibungen, technische Pläne und dazugehörige Maßnahmenbeschreibungen, Schulungsmaßnahmen etc.

3.4.6. Überprüfung der Einhaltung der Sicherheitskonzepte

Die Einhaltung der Sicherheitskonzepte ist durch geeignete Kontrollinstanzen[11], sowohl intern als auch durch dazu beauftragte Dritte, durch Stichproben periodisch zu überprüfen.

3.4.7. Dokumentation

Die im Rahmen der Erstellung und Umsetzung von Sicherheitskonzepten sowie im laufenden Betrieb durchgeführten Aktivitäten und Arbeitsergebnisse sind entsprechend zu dokumentieren, sodass deren Nachvollziehbarkeit gewährleistet ist.

4. Informationssicherheitsorganisation

Die oberste Entscheidungsebene in Informationssicherheitsfragen bilden und verantworten der/die Informationssicherheitsbeauftragte, die ZID-Leitung und das zuständige Vizerektorat.

4.1. Leitung der Informationssicherheit

Das Rektorat vergibt die Rolle eines Beauftragten für die Informationssicherheit der TU Graz. Die Stellvertretung hat die Leitung der Organisationseinheit ZID.

Die Aufgaben des/der Rolleninhabers*in „**Informationssicherheitsbeauftragter**“ **(ISB)** sind**:**

- Einführung und laufende Weiterentwicklung eines Informationssicherheitssystems (ISMS)
- Koordination der Aufgaben des Informationssicherheitskernteams (ISKT)
- Koordination der Tätigkeiten des Service IT-Recht/-Sicherheit des ZID
- Kommunikation der Thematik im zuständigen Vizerektorat, im Datenschutzbeirat und mit der Datenschutzkoordination
- Erarbeitung und Fortschreibung des Umsetzungsplans für die im Konzept zur Informationssicherheit TU-weit gewählten Maßnahmen
- Überwachung der Implementierung der Sicherheitsmaßnahmen
- Prozessverantwortlichkeit für die Informationssicherheit
- Prüfung, ob die Sicherheitsziele, die in der Politik zur Informationssicherheit formuliert sind, erreicht werden
- Sensibilisierung und Bewusstseinsbildung für Informationssicherheit an der TU Graz

4.2. Informationssicherheitskoordinator der Fakultät

Der/die Dekan/in ernennt für Entscheidungen betreffend der Informationssicherheit, die ausschließlich seine/ihre Fakultät betreffen, eine Person mit der Rolle **„Informationssicherheitskoordinator“**. Er/sie wird inhaltlich vom ISB, dem ISKT, dem ZID, der Datenschutzkoordination und der OE Recht und Versicherungsmanagement bei der Entscheidungsfindung unterstützt.

[11] Einzelgespräche durch ISKT, Interne Revision, externe Audits.

4.3. Informationssicherheitskernteam (ISKT)

Das ISKT besteht aus einer IT-Security-Engineer-Assistenz am ZID, den Informationssicherheitskoordinatoren sowie weiterer fachlich kompetenter Personen, die, je nach Fragestellung, mit der Datenschutzkoordination, der OE Recht und Versicherungsmanagement, der OE GuT sowie fachkompetenten Vertretern aus anderen Institutionen zusammen arbeitet.

Aufgaben des ISKT:

- Tätigkeit als Kompetenzzentrum in Informationssicherheitsfragen gegenüber den in der Politik zur Informationssicherheit im Geltungsbereich genannten Organisationseinheiten
- Ermittlung der für den Prozess notwendigen Ressourcen
- Formulierung von Vorgehensweisen bspw. betreffend Risikoanalyse und -management
- Durchführung von Risikoanalysen und -management zur Informationssicherheit
- Erarbeitung und Aktualisierung des Konzepts zur Informationssicherheit (Politik, Strategie, Richtliniendokumente, Sicherheitsstandards etc.)
- Umsetzung der gewählten Maßnahmen zur Informationssicherheit
- Kontrolle der Effektivität der Maßnahmen im laufenden Betrieb
- Informationsaufbereitung und -weiterleitung in Bezug auf Angelegenheiten des laufenden Betriebs

4.4. *Computer Emergency Response Team* (CERT)

Das CERT setzt sich aus ausgewählten und fachlich kompetenten Angehörigen des ZID zusammen.

Aufgaben des CERT:

- Reaktion auf Vorfälle
- Präventionsmaßnahmen
- Berichten an das ISKT
- Kommunikation mit übergeordneten CERT-Institutionen (ACOnet, CERT.at)
- Unterstützung des ZID-Service IT-Recht/-Sicherheit

TEIL B Regelungen für alle Angehörigen der TU Graz

In diesem Teil der Richtlinie werden generelle Handlungsanweisungen festgeschrieben, die von allen Angehörigen der TU Graz einzuhalten sind, damit sowohl der Datenschutz als auch die Informationssicherheit sichergestellt werden können.
Für Studierende der TU Graz gilt der *Abschnitt Nutzung von IT-Endgeräten durch Studierende an der TU Graz.*
Regelungen für Angehörige der TU Graz, die besondere technische Aufgaben übernommen haben, finden sich in Teil C.

5. Klassifizierung von Daten und Informationen

5.1. Zweck

Die TU Graz stellt ihren Angehörigen und Dritten die Daten, Informationen sowie technische Informations- und Kommunikationssysteme (IKT-Systeme) zur Erfüllung ihrer Aufgaben zur Verfügung.
Ein wesentlicher Aspekt ist dabei der ordnungsgemäße Umgang mit Daten und Informationen in Bezug auf Vertraulichkeit, Verfügbarkeit, und Integrität. Dabei kommt insbesondere den Einrichtungen in Lehre und Forschung sowie den Dienstleistungseinrichtungen eine tragende Rolle zu. Darüber hinaus ist bei der Verwendung derartiger Daten und Informationen die Eigenverantwortung der Bediensteten in besonderem Maße gefordert.
Das Klassifizierungsschema bezieht sich auf alle Arten von Daten, seien es handschriftliche, maschinelle oder elektronische Aufzeichnungen, unabhängig vom Datenträger, z.B. auf elektronischen Datenträgern, auf Mikrofilm oder auf Papier, und gilt ungeachtet dessen, ob diese Daten und Informationen mündlich, schriftlich oder in digitaler Form ausgetauscht werden.
Konkrete Handlungsanweisungen für den Umgang mit klassifizierten Daten finden Sie auf der Homepage des ZID.

5.2. Klassifizierungsbereiche

Daten bzw. Datenkategorien und Informationen sind jeweils in den Bereichen Vertraulichkeit, Verfügbarkeit und Integrität anhand der unten beschriebenen Schadensszenarien, soweit sie auf die Daten und Informationen anwendbar sind, zu klassifizieren. Die Schadensszenarien dienen als Hilfestellung um den Bedarf an Vertraulichkeit, Verfügbarkeit und Integrität der Daten und Informationen feststellen zu können.
Der Schutzbedarf für die Daten und die Information ergibt sich aus der Klassifizierung in den Bereichen Vertraulichkeit, Verfügbarkeit und Integrität. Die Vertraulichkeit und Integrität sind separat von der Verfügbarkeit zu klassifizieren, wobei für die Gesamtklassifizierung beider Bereiche jeweils das Maximumprinzip zur Anwendung kommt. Sobald in der Prüfung eines der beiden Bereiche (Vertraulichkeit und Integrität bzw. Verfügbarkeit) einmal das Schutzbedürfnis *hoch* festgestellt wird, sind die jeweiligen Daten und Informationen im Hinblick auf den jeweiligen Bereich als hoch schutzbedürftig zu klassifizieren. Aufgrund des ermittelten Schutzbedarfs ergeben sich die entsprechend einzuhaltenden Handlungsanweisungen.

5.2.1. Vertraulichkeit

Daten und Informationen der TU Graz sind vor unberechtigtem Zugriff, unbefugter Kenntnisnahme und Preisgabe zu schützen. Daten und Informationen sind im Bereich der Vertraulichkeit als *öffentlich*, *niedrig, mittel* oder *hoch* zu klassifizieren. Wurde durch den oder die *Data-Owner* keine Klassifizierung vorgenommen, werden die Daten und Informationen standardmäßig als *Vertraulichkeit mittel* klassifiziert. Das trifft auch auf Daten zu, die der FAIR-Data-Policy unterliegen.
Die Klassifizierung im Bereich der Vertraulichkeit entspricht dem TLP (*Traffic Light Protocol*)[12].

Öffentlich

Als öffentlich gelten Daten und Informationen, deren Vertraulichkeit für den Regelbetrieb der TU Graz nicht ausschlaggebend ist oder die durch Dritte oder die TU Graz zur Veröffentlichung vorgesehen sind oder bereits veröffentlicht wurden. Diese Daten und Informationen dürfen ohne Einschränkung weitergegeben werden, auch an die Presse.
Als öffentlich gelten jedenfalls Daten und Informationen, die im Webauftritt der TU Graz oder in *Social Media* frei zugänglich bereits publiziert wurden oder dafür freigegeben wurden; beispielsweise die Satzung, der Organisationsplan, das Mitteilungsblatt, Studienpläne, Ausschreibungen, Marketingmaterial, Broschüren, Interview-Inhalte, Texte für Zeitschriften und (Presse-)Aussendungen und andere Informationen, die aus öffentlich und frei zugänglichen Quellen stammen.
Im Sinne von *Open Access* gelten auch alle Forschungsdaten der TU Graz als öffentlich, solange das nicht durch Verträge, Gesetze oder andere verbindliche Bestimmungen anders definiert ist.
Daten und Informationen der TU Graz, deren Vertraulichkeit zunächst als *niedrig*, *mittel* oder *hoch* klassifiziert worden ist, können vom *Data-Owner* zu einem späteren Zeitpunkt als *öffentlich* klassifiziert werden, z.B. Finanzdaten.
Die Klassifizierung *öffentlich* entspricht TLP: WHITE.

Vertraulichkeit Niedrig

Daten und Informationen mit der Klassifizierung *Vertraulichkeit niedrig* dürfen innerhalb der TU Graz weitergegeben aber nicht veröffentlicht werden. Dazu zählen Daten und Informationen die z.B. auf der Intranetplattform der TU Graz bekanntgegeben werden.
Die Klassifizierung *Vertraulichkeit Niedrig* entspricht TLP: GREEN

Vertraulichkeit Mittel

Daten und Informationen, die innerhalb bestimmter Organisationseinheiten weitergegeben werden dürfen, und weder als *niedrig*, noch als *hoch* klassifiziert sind, z.B. Daten und Informationen im Zuge von Dienstreiseabrechnungen. Diese Daten und Informationen gelten als eingeschränkt schutzbedürftig.
Die Klassifizierung *Vertraulichkeit Mittel* entspricht TLP: AMBER

[12] Nähere Informationen zum TLP unter: https://security.tugraz.at/TLP

Vertraulichkeit Hoch

Daten und Informationen, die nur für einen eng definierten Personenkreis bestimmt sind, der eine interne, rechtliche (gesetzliche, vertragliche) oder gesellschaftliche Notwendigkeit für deren Verwendung hat. Diese gelten als *hoch* schutzbedürftig. Die Weitergabe der Daten und Informationen an Personen außerhalb des definierten Personenkreises ist verboten.
Besondere Kategorien personenbezogener Daten gemäß Artikel 9 DSGVO wie Gesundheitsdaten und hoch schutzbedürftige Daten und Informationen, z.B. als vertraulich gekennzeichnete Daten und Informationen aus Forschungskooperationen mit Dritten, vertrauliche Arbeitsunterlagen des Rektorats, werden standardmäßig als *hoch* klassifiziert.
Die Klassifizierung *Vertraulichkeit Hoch* entspricht TLP: RED

5.2.2. Verfügbarkeit

Daten und Informationen der TU Graz sind vor Verlust und Zerstörung zu schützen. Daten und Informationen sind im Bereich der Verfügbarkeit als *niedrig, mittel* oder *hoch* zu klassifizieren. Als Standard wird für alle Daten und Informationen *Verfügbarkeit niedrig* definiert.

Verfügbarkeit Niedrig

Die Wahrnehmung der Aufgaben in einer Organisationseinheit kann weiterhin aufrechterhalten werden, wenn das IT-System oder physisch aufbewahrte Daten und Informationen für **ca. 3 Tage pro Jahr** nicht verfügbar sind (ca. 99,00 %).

Verfügbarkeit Mittel

Die Wahrnehmung der Aufgaben in einer Organisationseinheit kann weiterhin aufrechterhalten werden, wenn das IT-System oder physisch aufbewahrte Daten und Informationen für **ca. 8 Stunden pro Jahr** nicht verfügbar sind (ca. 99,90 %).

Verfügbarkeit Hoch

Die Wahrnehmung der Aufgaben in einer Organisationseinheit kann weiterhin aufrechterhalten werden, wenn das IT-System oder physisch aufbewahrte Daten und Informationen für **ca. 1 Stunde pro Jahr** nicht verfügbar sind (ca. 99,99 %).

5.2.3. Integrität

Daten und Informationen sind vor ungewollter und manipulativer Veränderung zu schützen. Daten und Informationen sind im Bereich der Integrität als *niedrig, mittel* oder *hoch* zu klassifizieren. Wurde durch den oder die *Data-Owner* keine Klassifizierung vorgenommen, werden die Daten und Informationen generell als *Integrität mittel* klassifiziert.

Integrität Niedrig

Die Integrität der Daten und Informationen ist für den Regelbetrieb der TU Graz und/oder die Einhaltung gesetzlicher, vertraglicher oder selbstauferlegter Pflichten nicht bzw. nicht mehr erforderlich, z.B. nach Abhaltung der Prüfung und dem Verstreichen der gesetzlichen Aufbewahrungsfrist ist die Integrität der Prüfungsfragen für den Regelbetrieb nicht mehr erforderlich.

Integrität Mittel
Die Integrität der Daten und Informationen muss für den Regelbetrieb der TU Graz und/oder die Einhaltung gesetzlicher, vertraglicher oder selbstauferlegter Pflichten zu einem definierten Zeitpunkt, z.B. Bankdaten zum Zeitpunkt der Überweisung, gegeben sein.

Integrität Hoch
Die Integrität der Daten und Informationen muss für den Regelbetrieb der TU Graz und/oder die Einhaltung gesetzlicher, vertraglicher oder selbstauferlegter Pflichten zu jedem Zeitpunkt gegeben sein (z.B. müssen Studierendendaten für den Regelbetrieb zu jedem Zeitpunkt integer sein, um eine LV-Anmeldung, Prüfung oder Zeugnisausstellung vor nehmen zu können).

6. Nutzung von IT-Endgeräten durch Bedienstete

6.1. Zweck
Zweck dieses Abschnittes ist es, Regelungen für die Nutzung von IT-Endgeräten an der TU Graz zu treffen, die die Informationssicherheit gewährleisten und die Einhaltung datenschutzrechtlicher Vorgaben sicherstellen sollen.
Zur Erreichung der Geschäftsziele und zur Erfüllung der Aufgaben der TU Graz sind Informationen, und damit verbunden der Einsatz von Informationstechnologien, unerlässlich.

6.2. Benutzungsregelungen für IT-Endgeräte der TU Graz

6.2.1. Allgemeine Regelungen
IT-Endgeräte, die im Besitz oder Eigentum der TU Graz stehen, dürfen nur von der berechtigten Benutzerin oder dem berechtigten Benutzer verwendet werden.
Auf IT-Endgeräten, die auch von anderen als der berechtigten Benutzerin oder dem berechtigten Benutzer verwendet werden, müssen zur Datentrennung geeignete Maßnahmen ergriffen werden. IT-Endgeräte, auf denen keine Datentrennung möglich ist, dürfen nur durch die berechtigte Benutzerin oder den berechtigten Benutzer verwendet werden.
Urheberrechte sind zu wahren und Lizenzbestimmungen sind einzuhalten.
Jegliche Handlungen, die die Sicherheit von dienstlichen Daten und Informationen gefährden, sind zu unterlassen.

Ausdrücklich untersagt ist Folgendes:

- Die Arbeit mit *Sysadmin/SysOp*- oder *root*-Rechten auf IT-Endgeräten der TU Graz mit Rechtetrennung, außer zu dienstlich notwendigen Arbeits- und Wartungszwecken.
- Das Verschleiern der eigenen Identität im Rahmen der dienstlichen Internet-Nutzung, außer zu Forschungszwecken.
- Der Einsatz von *Soft*- und *Hardware* und sonstigen Mitteln, deren Zweck es ist, Informationen auszuspähen, außer zu dienstlich notwendigen Zwecken.

- Das Starten (*Booten*) von öffentlich zugänglichen IT-Endgeräten über externe, nicht autorisierte Datenträger.
- Die Installation sicherheitsgefährdender Programme.
- Die Veränderung von erkennbar sicherheitsrelevanten Einstellungen[13].
- Die bewusste Inkaufnahme IT-bezogener Sicherheitsrisiken (in begründeten Einzelfällen ist eine Abstimmung mit dem ISKT zu suchen).
- Die Verwendung von IT-Endgeräten[14], die nicht dem Sicherheitsniveau nach Stand der Technik entsprechen.

6.2.2. Gerätesperre und Kennwortschutz

Der kennwortgeschützte Sperrbildschirm auf Arbeitsplatz-/Kleinrechner (PC) und Notebooks ist so einzustellen, dass er spätestens nach 15 Minuten Nutzerinaktivität aktiviert wird und ist bei Verlassen des Arbeitsplatzes manuell zu aktivieren. Die Gerätesperre auf Smartphones und Tablet-PCs ist so einzustellen, dass sie spätestens nach 5 Minuten Nutzerinaktivität aktiviert wird.
Das Deaktivieren der voreingestellten Gerätesperre bzw. des kennwortgeschützten Sperrbildschirms ist untersagt.
Für Demo-/Präsentationsrechner, Laborrechner und Anzeigetafeln etc. ist eine automatische Aktivierung des kennwortgeschützten Sperrbildschirms nach 15 Minuten Inaktivität nicht erforderlich.

6.2.3. Sicherheitsupdates und Schadsoftwarescanner

Das Betriebssystem und die installierten Anwendungen auf Arbeitsplatz-/Kleinrechner (PC), Notebooks und Tablet-PCs sind in Bezug auf Sicherheitsupdates aktuell zu halten und es ist ein aktueller Schadsoftwarescanner zu installieren und zu aktivieren; bei Bedarf unterstützt der ZID bei Auswahl und Installation.
Stehen keine dem Stand der Technik entsprechenden Schadsoftwarescanner zur Verfügung, sind andere geeignete Maßnahmen zu ergreifen und zu dokumentieren, um ein entsprechendes Sicherheitsniveau zu erreichen. Die Schadsoftwaresignaturen auf Arbeitsplatz-/Kleinrechner (PC), Notebooks und Tablet-PCs sind bei signaturbasierten Schadsoftwarescannern aktuell zu halten und bei Aufbau einer Netzwerkverbindung zur TU Graz vor deren weiteren Nutzung zu aktualisieren, entsprechendes gilt für die technischen Grundlagen der Schadsoftwareerkennung bei der Nutzung anderer Technologien. Eine aktuelle lokale Firewall, die ein- und ausgehenden Datenverkehr überwacht, muss installiert und aktiviert sein, sofern eine solche standardmäßig im Betriebssystem integriert ist.
Das Deaktivieren des Schadsoftwarescanners und das Einschränken oder Verhindern der automatischen Installation von Sicherheitsupdates ist untersagt.
Für Demorechner, Präsentationsrechner, Laborrechner, Anzeigetafeln etc. kann von dieser Verpflichtung mit entsprechender Dokumentation abgewichen werden.

[13] z.B. das Deaktivieren des kennwortgeschützten Sperrbildschirms, das Deaktivieren des Schadsoftwarescanners.
[14] Dazu zählen auch Funkmäuse, Presenter etc., die die Datenübertragung nicht nach Stand der Technik verschlüsseln.

6.2.4. Verlust und Diebstahl

IT-Endgeräte der TU Graz verbleiben auch bei Verwendung durch Angehörige der TU Graz und Dritte im Eigentum der TU Graz. Die IT-Endgeräte sind sorgfältig aufzubewahren und vor Verlust und Diebstahl zu schützen.

Bei Verlust oder Diebstahl von IT-Endgeräten oder mobilen Datenträgern, die im Eigentum der TU Graz stehen oder auf denen sich dienstliche Daten befinden, ist von der betroffenen Person der Prozess zur Meldung von Datenschutzvorfällen gemäß dem *Data-Breach*-Prozess der DSGVO einzuhalten.

6.2.5. Beendigung des Dienstverhältnisses/Vertragsverhältnisses

Bei Beendigung des Dienstverhältnisses bzw. eines Vertragsverhältnisses zur TU Graz sind im Eigentum der TU Graz stehende IT-Arbeitsmittel an die jeweilige Dienstvorgesetzte oder den jeweiligen Dienstvorgesetzten bzw. die jeweilige Ansprechperson zu übergeben.

Auf IT-Endgeräten abgelegte dienstliche Daten sind vor dem Austritt, sofern diese nicht bereits auf zentralen Speicherorten abgelegt sind, an die jeweilige Dienstvorgesetzte oder den jeweiligen Dienstvorgesetzten bzw. die jeweilige Ansprechperson vollständig zu übergeben.

6.2.6. Private Daten

Das Speichern von privaten Daten auf IT-Endgeräten und mobilen Datenträgern, die sich im Eigentum der TU Graz befinden, ist im Umfang des Punktes „Nutzung der Ressourcen der TU Graz“ des Verhaltenskodex gestattet.

Bei einer dem Verhaltenskodex widersprechenden privaten Nutzung von IT-Endgeräten und mobilen Datenträgern sind auf Aufforderung durch die jeweilige Dienstvorgesetzte oder den jeweiligen Dienstvorgesetzten von der Person, die diese Daten dort gespeichert hat, zu löschen. Die TU Graz übernimmt keine Haftung für den Verlust von privaten Daten.

6.2.7. Leihgeräte

Bei Leihgeräten liegt die Verantwortung für die genutzten IT-Endgeräte während der Entlehndauer bei der ausleihenden Person. Für die Sicherung jeglicher Daten und Informationen auf den Leihgeräten im Sinne dieses Abschnitts ist die ausleihende Person verantwortlich.

6.3. Benutzungsregelung für private Endgeräte (*Bring/Use Your Own Device*)

Die oben genannten Punkte gelten mit Ausnahme der Punkte 6.2.5. und 6.2.6. auch für private IT-Endgeräte. Punkt 6.2.4. kommt sinngemäß zur Anwendung.

IT-Endgeräte, die nicht von der TU Graz verwaltet werden, werden auf eigene Gefahr und eigenes Risiko der Benutzerin oder des Benutzers betrieben. Wird für dienstliche Daten ein privates IT-Endgerät verwendet, ist ein aktueller und aktivierter Echtzeit-Schadsoftwarescanner zu installieren, ebenso müssen aktuelle Schadsoftwaresignaturen nach dem Verbindungsaufbau vorhanden sein, entsprechendes gilt für die technischen Grundlagen der Schadsoftwareerkennung bei der Nutzung anderer Technologien. Das Betriebssystem und die Anwendungen sind in Bezug auf Sicherheitsupdates aktuell zu halten. Eine aktuelle lokale Firewall, die ein- und ausgehenden Datenverkehr überwacht, muss installiert und aktiviert sein, sofern eine solche standardmäßig im Betriebssystem integriert ist. Bei Beendigung des Dienstverhältnisses bzw. eines Vertragsverhältnisses sind Kopien von dienstlichen Daten auf privaten IT-Endgeräten, nach Übergabe

an die jeweilige Vorgesetzte oder den jeweiligen Vorgesetzten oder Ablage auf einem zentralen Speicherort, vollständig zu löschen.

7. Nutzung von IT-Endgeräten durch Studierende

7.1. Regelungen

- IT-Endgeräte, die nicht von der TU Graz verwaltet werden, werden auf eigene Gefahr und eigenes Risiko der Benutzerin oder des Benutzers betrieben.
- Das Betriebssystem und die installierten Anwendungen auf Arbeitsplatz-/Kleinrechner (PC), Notebooks und Tablet-PCs sind in Bezug auf Sicherheitsupdates aktuell zu halten, ein aktueller Schadsoftwarescanner ist zu installieren und zu aktivieren. Stehen keine, dem Stand der Technik entsprechenden Schadsoftwarescanner zur Verfügung, sind andere geeignete Maßnahmen zu ergreifen, um ein entsprechendes Sicherheitsniveau zu erreichen. Die Schadsoftwaresignaturen auf Arbeitsplatz-/Kleinrechner, Notebooks und Tablet-PCs sind bei signaturbasierten Schadsoftwarescannern aktuell zu halten, entsprechendes gilt für die technischen Grundlagen der Schadsoftwareerkennung bei der Nutzung anderer Technologien.
- Urheberrechte sind zu wahren und Lizenzbestimmungen sind einzuhalten.

7.2. Ausdrücklich untersagt ist Folgendes

- Das Starten (*Booten*) von öffentlich zugänglichen IT-Endgeräten der TU Graz über externe, nicht autorisierte Datenträger.
- Die Installation sicherheitsgefährdender Programme.
- Das bewusste in Kauf nehmen IT-bezogener Sicherheitsrisiken – in begründeten Einzelfällen ist eine Abstimmung mit dem ISKT zu suchen.

8. Kennwörter

8.1. Zweck

Zweck dieses Abschnittes ist es, geeignete Regelungen für den Einsatz von Kennwörtern zu treffen, um Systeme und die darauf laufenden Anwendungen der TU Graz vor unberechtigten Zugriffen zu schützen.
Die TU Graz stellt technische Informations- und Kommunikationssysteme (IKT-Systeme) zur Erfüllung universitärer Aufgaben zur Verfügung. Diese Systeme und die darauf laufenden Anwendungen sind vor unberechtigten Zugriffen zu schützen.
Kennwörter sind in der TU Graz das überwiegend eingesetzte Mittel, um Zugriffsschutz zu gewährleisten. Wo es technisch möglich ist, ist eine Mehrfaktorauthentifizierung einzusetzen.
Bei der Verwendung von Kennwörtern kommt die Eigenverantwortung der Nutzer in besonderem Maße zum Tragen. Gleichzeitig muss auch durch organisatorische sowie technische Maßnahmen die wirtschaftliche, sichere und gesetzeskonforme Verwendung der Systeme gewährleistet werden.

8.2. Regelungen für den Gebrauch von Kennwörtern zur Verwendung in TU Graz Systemen

- Kennwörter sind von der vorgesehenen Benutzerin oder vom vorgesehenen Benutzer geheim zu halten und dürfen nicht weitergegeben werden[15]. Auf eine unbeobachtete Eingabe des Kennworts ist zu achten.
- Kennwörter dürfen nicht ungesichert über das Netzwerk der TU Graz übertragen werden.
- Kennwörter müssen so gewählt werden, dass sie sich signifikant von anderen eigenen Kennwörtern unterscheiden.
- Kennwörter, von denen angenommen werden muss, dass sie Unberechtigten bekannt geworden sein könnten oder sind, müssen von der berechtigten Benutzerin oder vom berechtigten Benutzer umgehend geändert werden bzw. muss von dieser oder diesem eine Kennwortrücksetzung veranlasst werden.
- Wenn ein Kennwort zurückgesetzt werden soll, ist sicherzustellen, dass die Antragstellerin oder der Antragsteller auch die rechtmäßige Account-Inhaberin oder der rechtmäßige Account-Inhaber ist.
- Die Weitergabe von Kennwörtern für Funktionsbenutzer-IDs darf nur durch die für die jeweilige Funktionsbenutzer-ID verantwortliche Person erfolgen und nur an Personen, die das Kennwort für die Erfüllung ihrer Aufgaben an der TU Graz benötigen.
- Kennwörter für Funktionsbenutzer-IDs dürfen nur von der für die jeweilige ID verantwortlichen Person geändert werden. Bei Ausscheiden einer Person aus der von der ID umfassten Gruppe, ist das Kennwort umgehend zu ändern.
- Initial-Kennwörter sind bei der ersten Anmeldung entsprechend den Minimalanforderungen (siehe Homepage des ZID) zu ändern.
- Werkseitig voreingestellte Kennwörter sind umgehend entsprechend den Mindest-anforderungen zu ändern.
- Zusätzliche Regelungen können, abhängig von der jeweiligen Situation, dann getroffen werden, wenn dies aus Risikogesichtspunkten notwendig erscheint.

8.3. Regelungen für die Vergabe von Initial-Kennwörtern

Initial-Kennwörter müssen nach dem Zufallsprinzip individuell vergeben werden und müssen eine begrenzte Gültigkeitsdauer haben.

8.4. Regelungen für die Verwendung von Kennwörtern in TU externen Systemen

Ist aus dienstlichen Gründen die Anmeldung mit einem Kennwort in externen Systemen notwendig, darf das Kennwort, das für TU Graz Systeme verwendet wird, nicht auch für externe Systeme verwendet werden.

Ist die Sicherheit der Übertragung der Zugangsdaten in das externe System nicht gegeben und ist nur eine einmalige Anmeldung erforderlich, wird die Verwendung von Einmal-Kennwörtern empfohlen.

[15] Auch nicht z.B. an Dienstvorgesetzte, Vertretungen oder Assistentinnen und Assistenten.

9. Löschung und physische Zerstörung von Datenträgern

9.1. Zweck

Zweck dieses Abschnittes ist es, die Vertraulichkeit von schützenswerten bzw. zu schützenden Informationen durch geeignete Regelungen für die Löschung und physische Zerstörung von Datenträgern (inkl. z.B. Papier) sicherzustellen, wenn diese dauerhaft außer Betrieb genommen oder ausgesondert werden.

9.2. Regelungen

Der Datenträgerverantwortliche ist für die sichere Löschung bzw. Zerstörung seiner Datenträger und erforderlichenfalls Geräte zuständig, sobald die tatsächliche Verfügungsgewalt, d.h. die Kontrolle über den Datenträger bzw. das Gerät aufgegeben wird[16].

Die Datenträgerlöschung bzw. -zerstörung ist durch den Datenträgerverantwortlichen selbst oder auf seine Veranlassung durch eine dafür geeignete und dazu beauftragte Stelle durchzuführen[17]. Dazu können diese auch qualifizierte Entsorgungsbetriebe heranziehen. In jedem Fall ist sicherzustellen, dass die Datenträger bis zu ihrer Löschung bzw. Zerstörung zugriffgeschützt bleiben. Falls gefordert sind von der beauftragten Stelle bzw. dem Entsorgungsbetrieb Übernahmebestätigungen auszustellen. Verschlüsselte Datenträger sind genauso zu behandeln wie unverschlüsselte.

10. Nutzung IT-Services Dritter

10.1. Zweck

Die TU Graz regelt die Nutzung von IT-Services Dritter und zielt dabei primär auf unter allen Umständen einzuhaltende rechtliche Anforderungen, wie z.B. Datenschutz und Datensicherheitserfordernisse ab, gefolgt von den Anforderungen hinsichtlich Funktionalität, Leistungsfähigkeit, Wirtschaftlichkeit und Bedienkomfort.

IT-Services Dritter können eine Ergänzung zu den von der TU Graz selbst betriebenen IT-Services sein.

10.2. Regelungen

10.2.1. Bereitstellungsmodelle (*deployment models*)

Im Rahmen dieser Richtlinie wird zwischen den folgenden zwei Bereitstellungsmodellen von IT-Services unterschieden:

- **Interne IT-Services:** Das IT-Service wird von einer Institution, z.B. TU Graz, nur für eigene Zwecke betrieben. Umfang und Art der Nutzung kann in zusätzlichen IT-Nutzungsvereinbarungen definiert werden. An der TU Graz sind das vor allem Services, die vom ZID betrieben werden aber auch IT-Infrastruktur, die durch Bundesbehörden und deren nachgeordnete Dienststellen und Einrichtungen (z.B. BRZ, ACOnet) betrieben werden.

[16] Beispielsweise in folgenden Fällen: Ende der dienstlichen Nutzung eines Notebooks/PCs; Übergabe eines defekten Gerätes an den Hersteller; Entsorgen von Papier, DVDs, USB-Sticks etc.

[17] Es besteht die Möglichkeit, nach Voranmeldung, Datenträger am ZID abzugeben. Dieser übernimmt die richtlinienkonforme Zerstörung.

- **Externe IT-Services:** Darunter versteht man IT-Services, die von der Allgemeinheit oder einer großen Gruppe genutzt werden können und evtl. auch kommerziell angeboten werden. Im konkreten Kontext bedeutet dies, dass das IT-Service nicht durch die TU Graz oder eine Organisation im akademischen Umfeld betrieben wird.

10.2.2. Wahl der IT-Services

Bei der Überlegung interne IT-Services oder IT-Services Dritter zu nutzen, ist der Schutzbedarf der zugrundeliegenden Daten entscheidend.
Personenbezogene Daten dürfen nur im Einklang mit den geltenden Datenschutzbestimmungen verarbeitet und übermittelt werden.
Bei der Auslagerung von personenbezogenen Daten und Anwendungen in IT-Services Dritter sind insbesondere die datenschutzrechtlichen Grundprinzipien (Zweckbindungsgrundsatz, Wesentlichkeitsgrundsatz, Verhältnismäßigkeitsgebot, Datensparsamkeit) zu beachten und dürfen Daten u.a. nur solange in personenbezogener Form gespeichert werden, als dies für die Erreichung der Zwecke, zu denen die Daten verarbeitet werden, erforderlich ist.
Bei urheberrechtlich geschützten Inhalten sind ferner die Bestimmungen des Urheberrechts einzuhalten.
Darüber hinaus sind die von der TU Graz formulierten Grundsätze und Regelungen zu beachten.
Strengere Informationssicherheitsvorgaben aus Kooperationsverträgen oder anderen Verträgen mit Dritten, z.B. Verbot der Nutzung von IT-Services Dritter, haben Vorrang vor den Richtlinienvorgaben.
Die Entscheidung, ob interne IT-Services oder IT-Services Dritter genutzt werden soll, erfolgt aufgrund technischer, wirtschaftlicher, rechtlicher und strategischer Überlegungen.
Bei technischen Fragen kann eine Unterstützung durch das ISKT und bei Fragen in Bezug auf den Datenschutz durch die Datenschutzkoordination erfolgen.

	Nutzung interner IT-Services	***Nutzung IT-Services Dritter***
Besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO	Ja	Nein*
Daten in Prozessen mit einer hohen Anforderung an Integrität, Vertraulichkeit oder Verfügbarkeit	Ja	Ja**
Daten in Prozessen mit einer mittleren bis geringen Anforderung an Integrität, Vertraulichkeit und Verfügbarkeit	Ja	Ja***

* Für personenbezogene Daten besonderer Kategorien im Sinne des Art. 9 DSGVO sollen in erster Linie interne IT-Services genutzt werden. Sollte der Bedarf durch die interne IT-Services nicht gedeckt werden können, kann eine Ausnahme durch einen Rektoratsbeschluss gewährt werden.

** Werden Daten aus Prozessen mit einer hohen Anforderung an Integrität, Vertraulichkeit oder Verfügbarkeit in IT-Services Dritter verarbeitet, müssen folgende Voraussetzungen eingehalten werden:

- Zertifizierung nach ISO 27001, ISO 27018, BSI Grundschutz oder vergleichbaren international gültigen Standards.
- Die Anforderungen aus dem Datenschutz sind einzuhalten.
- Das Vorliegen der Voraussetzungen ist in regelmäßigen Abständen zu überprüfen und zu dokumentieren.

*** Werden Daten aus Prozessen mit einer mittleren bis geringen Anforderung an Integrität, Vertraulichkeit und Verfügbarkeit in IT-Services Dritter verarbeitet, müssen folgende Voraussetzungen eingehalten werden:

- Die Anforderungen aus dem Datenschutz sind einzuhalten.
- Das Vorliegen der Voraussetzungen ist in regelmäßigen Abständen zu überprüfen und zu dokumentieren.

Sofern die zur Verwendung von IT-Services Dritter vorgesehenen Daten jedoch anonym, verschlüsselt, allgemein verfügbar oder bereits legal veröffentlicht sind, besteht an ihnen kein schutzwürdiges Geheimhaltungsinteresse, womit eine Prüfung der obigen Voraussetzungen nicht notwendig ist.

TEIL C Regelungen für Angehörige der TU Graz mit besonderen technische Aufgaben

In diesem Teil der Richtlinie werden Regelungen aufgestellt, die ausschließlich Angehörige der TU Graz, die spezielle technische Aufgaben übernommen haben, wie z.B. EDV-Beauftragter, IT-Auskunftsperson, Sysadmin bzw. Serveroperator, betreffen.

11. Identity & Access Management

11.1. Zweck

Zweck dieses Abschnittes ist es, die Prozesse von der Anlage bis zum Entzug von Benutzungsberechtigungen für IT-Dienstleistungen der TU Graz zu regeln.
Aufgabe von Identity & Access Management (IAM) im Sinne dieser Richtlinie ist es, digitale Identitäten mit all ihren Rollen zu verwalten und die an das IAM angeschlossenen IT-Systeme mit verlässlichen und aktuellen Daten zu versorgen. Eine zentrale IAM-Infrastruktur inkl. Rechtemanagement wird durch den ZID betrieben. Es soll bevorzugt dieses zentrale IAM für die gesamte TU Graz zum Einsatz kommen. Werden in einzelnen Organisationseinheiten eigene IAM-Systeme betrieben, gelten die unten aufgestellten Regelungen sinngemäß auch für diese. Der Betrieb eines eigenen IAM an einzelnen Organisationseinheiten ist schriftlich zu begründen.

11.2. Regelungen

Angebotene IT-Dienstleistungen sind vom ZID in einem Servicekatalog zu erfassen. Rollen sind vom Rektorat festzulegen. Aus Rollen und dem Servicekatalog ist vom Rektorat eine Berechtigungsmatrix freizugeben. Hierbei ist festzulegen, welche Berechtigungen standardmäßig vergeben werden und welche erweiterten Berechtigungen in begründeten Fällen befristet vergeben werden können. Erweiterte Berechtigungen können von Inhabern von dazu autorisierten Rollen[18] erteilt werden. Diese Fälle sind zu dokumentieren.

12. Druckerbetrieb

12.1. Zweck

Zweck dieses Abschnittes ist es, Regelungen für den sicheren Betrieb von Druckersystemen und Druckern an der TU Graz zu treffen. Für Arbeitsplatzdrucker sind nur die Punkte 12.2.2. und 12.2.3. anwendbar.

12.2. Regelungen

12.2.1. Verantwortlichkeiten und Betriebsprozesse

Verantwortlichkeiten für die IT-Administration der Druckersysteme und Drucker sind festzulegen und zu dokumentieren.
Konfigurationen sind zu dokumentieren, zu sichern und zugriffbereit zu halten.

[18] z.B. Leiter von Organisationseinheiten, Projektverantwortliche, Service-Verantwortliche.

Die Betriebsprozesse und -prozeduren sind zu definieren und zu dokumentieren. Die Uhren der Druckersysteme sind, wenn technisch möglich, mit einem zentralen Zeitserver zu synchronisieren.

12.2.2. Physische Aspekte

Aufstellungsort

Drucker und Druckersysteme sind so zu platzieren, dass diese innerhalb der Betriebsspezifikationen der Hersteller betrieben werden können. Dies betrifft insbesondere Stromversorgung und Kühlung. Schutz vor Flüssigkeiten, insbesondere Wasser, sowie Brandschutz und Brandlöscheinrichtungen sind vorzusehen. Die dafür zu treffenden Maßnahmen sind dabei an den jeweiligen Erfordernissen an die Verfügbarkeit auszurichten.

Zutrittskontrolle

Drucker und Druckersysteme sind so zu platzieren, dass diese entsprechend den Regelungen des Abschnitts zur *Klassifizierung von Daten und Informationen* zutrittgeschützt sind.

12.2.3. Netzwerkanschluss

Zu beachten sind die Regelungen des Abschnitts Netzwerkanschluss und -verbindung. Geplante Neuanschaffungen von Druckern und Druckersystemen sind mit dem ZID abzustimmen. Druckeranschlüsse sind netzwerktechnisch so abzusichern, dass die Drucker nur aus autorisierten Netzwerkbereichen erreichbar sind. Bei Druckern, die integrierte WLAN-Access-Point-Funktionalität aufweisen, ist diese zu deaktivieren. Schnittstellen wie z.B. USB-Anschlüsse, Speicherkarteneinschübe und Bluetooth sind nach Möglichkeit zu deaktivieren.

12.2.4. Kennwörter

Werkseitig voreingestellte Kennwörter (z.B. SNMP- und Webserver-Kennwörter) sind umgehend, spätestens aber bei Produktivstellung entsprechend dem Abschnitt *Kennwort* zu ändern.

12.2.5. Verschlüsselung von Speichermedien

Auf Druckern und Druckersystemen, die eine Verschlüsselung ihrer nichtflüchtigen Speicher (z.B. Festplatten, *Flash*-Speicher) erlauben, ist diese Funktion zu aktivieren. Bei Neukäufen muss diese Funktion standardmäßig vorhanden sein, Druckern ohne nichtflüchtige Speichermedien ist bei der Neuanschaffung der Vorzug zu geben.

12.2.6. Verschlüsselung im Zuge der Datenübertragung

Sofern Druckersysteme Datentransferprotokolle mit *End-to-End*-Verschlüsselung unterstützen, ist die Verschlüsselung zu aktivieren. Bei Neukäufen muss diese Funktion standardmäßig vorhanden sein.

12.2.7. Secure Print

Auf Druckern, die *Secure Print* erlauben, ist diese Funktion zu aktivieren, wenn nicht durch entsprechende Zutrittskontrollmaßnahmen angemessener Schutz gewährleistet werden kann.

12.2.8. Logging

In Bezug auf die Verwendung personenbezogener Daten ist die Datenschutzrichtlinie zu berücksichtigen.

12.2.9. Sichere Löschung und physische Zerstörung von Speichermedien

Nichtflüchtige Speichermedien in Druckern und Druckersystemen sind entsprechend dem Abschnitt *Löschungs- und physische Zerstörung von Datenträgern* zu löschen bzw. zu zerstören.

13. Serverbetrieb

13.1. Zweck

Zweck dieses Abschnittes ist es, Regelungen für die TU Graz und den sicheren Betrieb von *Servern* zu treffen. Die Regelungen in diesem Dokument verstehen sich als Maßnahme zur Schaffung eines verlässlichen Rahmens.

13.2. Verantwortlichkeiten und Betriebsprozesse

Verantwortlichkeiten für die Server- und die Serviceadministration sind festzulegen und zu dokumentieren.
Konfigurationen sind zu dokumentieren, zu sichern und zugriffbereit zu halten.
Produktivumgebungen sind bei technischer und wirtschaftlicher Möglichkeit von Test-, Installations-, Qualitätssicherungs- und Entwicklungsumgebungen zu trennen. Der *Software*-Freigabeprozess ist zu definieren.

13.3. Konfigurations- und Änderungsmanagement

- Konfigurationen sind laufend so anzupassen, dass ein angemessenes Sicherheitsniveau gewährleistet ist.
- Serveruhren sind mit einem zentralen Zeitserver zu synchronisieren.
- Standardmeldungen von Servern sind nach technischer und wirtschaftlicher Möglichkeit so anzupassen, dass Rückschlüsse auf die verwendete Hard- und Software weitestgehend verhindert werden.
- Meldungen für Benutzer sind verständlich zu formulieren und geeignete Kontaktdaten zur Meldung von Problemen oder Sicherheitsvorfällen anzugeben.

13.4. Physische Aspekte

Aufstellungsort

Server sind so zu platzieren, dass diese innerhalb der Betriebsspezifikationen der Hersteller betrieben werden können. Dies betrifft insbesondere Stromversorgung und Kühlung. Schutz vor Flüssigkeiten, insbesondere Wasser, sowie Brandschutz und Brandlöscheinrichtungen sind vorzusehen. Die dafür zu treffenden Maßnahmen sind dabei an den jeweiligen Erfordernissen der Verfügbarkeit entsprechend auszurichten.

Zutrittskontrolle

Server, auf denen zumindest als intern klassifizierte Daten verarbeitet oder gespeichert werden, sind so zu platzieren, dass diese zutrittgeschützt sind.

Der Zutritt zu Serverräumen darf für externe Personen nur in Ausnahmefällen, z.B. Zugang zur Haustechnikanlage zu Wartungs- und Reparaturzwecken, und nur nach vorheriger Anmeldung erfolgen. Externen Personen sind klare Verhaltensweisen vorzugeben und deren Kenntnisnahme ist schriftlich zu bestätigen.

Zu beachten sind die Regelungen des Abschnittes zur *Klassifizierung von Daten und Informationen*.

Netzwerkanschluss

Zu beachten sind die Regelungen des Abschnittes *Netzwerkanschluss und -verbindung*.

13.5. Zugriffskontrolle

Regelungen für die Serverdienstanmeldung sind zu treffen. Zu beachten sind insbesondere die Regelungen des Abschnittes *Kennwörter*.

Bei der Einrichtung von Zugriffsberechtigungen ist darauf zu achten, dass diese nach dem *Need-to-Know*-Prinzip und dem *Least-Privilege*-Prinzip vergeben werden. Bei Kenntnis über den Wegfall der Nutzungsgrundlagen sind Berechtigungen zu entziehen.

Regelungen zum Schlüssel- und Zertifikatsmanagement sind zu treffen. Insbesondere ist bei Zertifikaten auf Gültigkeitsdatum, Validierbarkeit und Sicherheitsniveau sowie den Schutz privater Schlüssel zu achten.

13.6. Monitoring des Serverbetriebs

Im Betrieb ist durch den Server- bzw. den Serviceverantwortlichen sicherzustellen, dass die Komponentenverfügbarkeit[21] vorbeugend und die definierten Leistungsparameter laufend überwacht werden.

Liefert die vorbeugende Komponentenprüfung oder die Prüfung der Leistungsparameter drohende Fehlerzustände, sind entsprechende Abhilfemaßnahmen zu setzen. Besteht Unklarheit über mögliche Abhilfemaßnahmen oder über deren Auswirkungen bzw. sind Abweichungen vom Normalbetrieb zu erwarten, sind derartige Situationen umgehend an den/die zuständigen *Sysadmin/s* bzw. den/die verantwortlichen *Service-Owner* zu melden.

13.7. Vermeidung von Sicherheitsschwachstellen und Schadsoftware

- Aktuelle Schadsoftwarescanner sind auf den Servern zu installieren. Sollte dies aus technischen Gründen nicht möglich sein, ist dies zu dokumentieren.
- Einsatz einer Host-basierten Firewall. Erlaubt ist nur die Nutzung eines vom Hersteller gewarteten Betriebssystems.
- Das Betriebssystem und die installierten Anwendungen auf Servern sind durch den Verantwortlichen in Bezug auf Sicherheitsupdates aktuell zu halten.
- Aktuelle Schadsoftwarescanner

[21] Beispiele: SMART-Parameter, Festplattenauslastungstrends

- Deaktivierung nicht benötigter Dienste (*Hardening*).
- Löschen von für den Betrieb nicht benötigten Dateien (Installations-, Konfigurations-, Logdateien etc.).
- An administrativen Workstations ist der Abschnitt über die *Nutzung von IT-Endgeräten* einzuhalten.
- Zu beachten sind insbesondere die Regelungen des Abschnittes *Netzwerkanschluss und -verbindung*.

13.8. Datensicherung

Zu beachten sind die Regelungen des Abschnittes über die *Sicherung betriebsrelevanter Daten und Informationen*.
Es ist sicherzustellen, dass kompromittierte Server Datensicherungen nicht unbrauchbar machen oder löschen können.

13.9. Logging

Alle für den sicheren, zuverlässigen Serverbetrieb und die Analyse von Vorfällen und Abweichungen erwartungsgemäß relevanten Ereignisse sind zu protokollieren[22].

13.10. Virtuelle Server

Für virtuelle Server, die dazugehörige Managementschicht und die darunterliegende Hardware gelten dieselben Regelungen wie für physische Server, wobei insbesondere auf die spezifischen Sicherheitsanforderungen der Managementschicht einzugehen ist.
Diese Vorgaben sind insbesondere bei der Verlagerung von virtuellen Systemen zu berücksichtigen, sodass das vorgesehene Schutzniveau aufrechterhalten bleibt. Beispielsweise ist darauf zu achten, dass Standortredundanzen erhalten bleiben, dass es nicht zu einer unzulässigen Vermischung unterschiedlicher Sicherheitsniveaus kommt und die netzwerktechnischen Voraussetzungen erfüllt bleiben.

13.11. Speichersysteme

Zugriffsschutz

Die Vertraulichkeit der auf mobilen oder aus dem Internet erreichbaren Speichersystemen abgelegten Daten ist so sicherzustellen, dass das vorgesehene Schutzniveau aufrechterhalten bleibt. Dazu sind die Daten gegebenenfalls zu verschlüsseln oder durchgehend physisch vor unbefugtem Zugriff zu schützen und entsprechend dem Abschnitt über *Löschung und physische Zerstörung von Datenträgern* zu löschen bzw. zu zerstören.

Monitoring

Die Verfügbarkeit der auf Speichersystemen abgelegten Daten ist dadurch zu gewährleisten, dass der Status der Speichersysteme laufend überwacht wird und rechtzeitig Maßnahmen zur Aufrechterhaltung des Betriebs gesetzt werden.

[22] Siehe Abschnitt 15.

14. Netzwerkanschluss und -verbindung

14.1. Zweck

Eine moderne IT-Infrastruktur gliedert sich in unterschiedliche Sicherheitsbereiche. Zweck dieses Abschnittes ist es, diese Bereiche zu definieren und festzulegen, unter welchen technischen und organisatorischen Voraussetzungen Geräte an die IT-Infrastruktur der TU Graz angeschlossen oder mit ihr fernverbunden werden dürfen. Darüber hinaus regelt dieser Abschnitt die erlaubten und verbotenen Verbindungen in und aus diesen Bereichen.
Erlaubte und verbotene Verbindungen: Siehe Informationen auf der Homepage des ZID.

14.2. Allgemeine Regeln, gültig für alle Netzwerkbereiche

- Die Zuordnung von Organisationseinheiten zu Sicherheitsbereichen und die damit verbundene Vergabe von IP-Adressen (privat und öffentlich) und logischen Netzwerken wird gemeinschaftlich von den Organisationseinheiten der TU Graz und der ZID vorgenommen, dokumentiert und gewartet.
- Die den jeweiligen Organisationseinheiten zugeordneten Netzanschlüsse ergeben sich aus der baulichen Lage der Räume sowie allfälliger von einer Organisationseinheit zusätzlich beim ZID beantragter Netzanschlüsse in anderen Bereichen. Diese Zuordnung wird vom ZID periodisch sowie bei Bedarf geprüft.
- Nicht benötigte Anschlüsse sind dem ZID bekanntzugeben und bis zu einer Neuzuordnung zu deaktivieren.
- Der mehrfache, gleichzeitige aktive Netzwerkanschluss eines IT-Endgerätes an unterschiedliche Netzwerkbereiche ist prinzipiell verboten, notwendige Mehrfachverbindungen sind mit dem ZID abzustimmen (z.B. in System-Managementbereichen, HA-Lösungen, VM-Lösungen usw.).
- *Bridging* oder *Routing* zwischen Netzen oder Netzbereichen darf nur über Netzwerk-komponenten erfolgen. Der Anschluss und Betrieb von Netzwerkkomponenten ist grundsätzlich dem ZID vorbehalten. Ist der Anschluss und Betrieb eigener Netzwerkkomponenten durch einzelne Organisationseinheiten beabsichtigt, ist dies im Vorhinein mit dem ZID anzustimmen.
- Der Betrieb von Servern im WLAN ist nicht zulässig.
- Der Einsatz von aus Sicherheitsgründen nicht genehmigten Diensten oder Protokollen für Forschungszwecke bedarf gegebenenfalls der Errichtung eines eigens dafür vorgesehenen Internet-Anschlusses sowie der Isolation der betroffenen Systeme vom Netzwerk der TU Graz. Eine diesbezügliche Lösung ist im Einvernehmen mit dem ZID zu erarbeiten.
- Darüber hinaus sind die speziellen Regelungen zur Sperre einzelner ein- und ausgehender Verbindungen (Ports und Protokolle) zu beachten. Diese Liste der erlaubten und verbotenen Dienste wird getrennt von dieser Richtlinie auf der Homepage des ZID verwaltet.

Jedenfalls unzulässig ist:

- Der Betrieb einer Authentifizierungsstruktur, bei denen der Benutzername einer Person der vom ZID vergebenen Benutzerkennung gleicht, ohne dass die Authentifizierung gegen Server vom ZID stattfindet.
- Verwendung einer SSID, die den Eindruck erweckt, sie sei ein offizielle SSID der TU Graz, wie „eduroam“ oder „TUGraz“ (Bedrohung: z.B. Phishing).
- Verwendung der Hotspot-Funktion von IT-Endgeräten in Bereichen, die durch das WLAN der TU Graz abgedeckt sind (Bedrohung: z.B. Funkstörung, Bandbreitenbedarf).
- Lagerung insbesondere von brennbarem Material (z.B. Dekorationsutensilien) in Räumlichkeiten, in denen Verteiler mit aktiven Netzwerkkomponenten (Netzwerkschränke) oder Verteilerknotenpunkte untergebracht sind und als Technikraum, Haustechnik oder Raum vom Typ “EDV” bzw. „IT“ ausgewiesen sind.

14.3. Regelungen für die einzelnen Netzwerkbereiche

14.3.1. Öffentlicher Bereich

- Alle öffentlich zugänglichen Anschlüsse (LAN und WLAN) an den Standorten der TU Graz (z.B. Hörsäle, Seminarräume, Selbststudienzonen, Aulen, Schulungsräume, Gangbereiche, Freiflächen).
- Erlaubte Systeme: Im Besitz oder Eigentum der Universität stehende, von ihr freigegebene und sonstige IT-Endgeräte.
- Netzzuordnung: Öffentlich zugängliche Anschlüsse, als öffentlich definiertes Netzwerk mit Authentifizierungsmechanismen zur Zuordnung einer von der TU Graz zur Verfügung gestellten IP-Adresse.

Die Sicherheit jedes an diesen Bereich angeschlossenen Systems obliegt der Eigenverantwortung des Benutzers.
Der Betrieb von Servern in diesem Bereich ist unzulässig.
Vom öffentlichen Bereich sind folgende Dienste ohne Authentisierung erreichbar:

- Öffentlicher Teil des TU Graz Intranet-Angebotes
- Systeme zur Authentifizierung (z.B. VPN)

Nach erfolgter Autorisierung ist die Kommunikation aus diesem Bereich hinaus auf Protokolle und Applikationen, die durch den ZID freigegeben sind, beschränkt.

14.3.2. Forschung und Lehre

- Alle Anschlüsse (LAN, WLAN, Telefonie etc.), die Einrichtungen für Forschung und Lehre der TU Graz zugeordnet und nicht öffentlich zugänglich sind. Zu den Einrichtungen in diesem Bereich zählen auch Organisationen an der TU Graz wie z.B. assoziierte Vereine, Beteiligungen, Kooperationen in Kompetenzzentren, K-Projekte und akademische Einmietungen.
- Erlaubte Systeme: Im Besitz oder Eigentum der Universität stehende, von ihr freigegebene und sonstige IT-Endgeräte.

- Netzzuordnung: Nicht öffentlich zugängliche Anschlüsse, die Forschungs- und Lehreinrichtungen der TU Graz oder universitätsnahen Organisationen zugeordnet sind.

Die Sicherheit jedes an diesen Bereich angeschlossenen Systems obliegt der Verantwortung der Leitung der Organisationseinheit. Die Zuständigkeit für die Umsetzung von Regelungen kann von dieser innerhalb der Organisationseinheit delegiert werden.
Der Betrieb von Servern in diesem Bereich ist unzulässig. Dafür sind die vorgesehenen Serverbereiche (intern und extern) zu verwenden.
Die Kommunikation aus diesem Bereich hinaus ist grundsätzlich nicht eingeschränkt.
Kommunikation in diesen Bereich hinein ist nicht gestattet, ausgenommen aus einem zugewiesenen Fernzugangsbereich.
Zum Schutz von in dieser Zone angeschlossenen Geräten gelten die Vorgaben des Abschnittes über die *Nutzung von IT-Endgeräten*.

14.3.3. Dienstleistungsbereich

- Alle Anschlüsse (LAN, WLAN, Telefonie etc.), die bestimmten Dienstleistungseinrichtungen der TU Graz zugeordnet und nicht öffentlich zugänglich sind. Zu den Einrichtungen in diesem Bereich zählen auch Organisationen an der TU Graz wie z.B. assoziierte Vereine, die nicht dem Bereich Forschung und Lehre zugeordnet sind, die österreichische Hochschülerschaft (ÖH), Alumnivereine.
- Erlaubte Systeme: Im Besitz oder Eigentum der Universität stehende, von ihr freigegebene und sonstige IT-Endgeräte.
- Netzzuordnung: Nicht öffentlich zugängliche Anschlüsse, die Dienstleistungseinrichtungen der TU Graz oder universitätsnahen Organisationen zugeordnet sind.

Die Sicherheit jedes an diesen Bereich angeschlossenen Systems obliegt der Verantwortung der Leitung der Organisationseinheit. Die Zuständigkeit für die Umsetzung von Regelungen kann von dieser innerhalb der Organisationseinheit delegiert werden.
Der Betrieb von Servern in diesem Bereich ist unzulässig. Dafür sind die vorgesehenen Serverbereiche zu verwenden.
Die Kommunikation aus diesem Bereich hinaus ist grundsätzlich nicht eingeschränkt.
Kommunikation in diesen Bereich hinein ist nicht gestattet, ausgenommen aus einem zugewiesenen Fernzugangsbereich.
Zum Schutz von in dieser Zone angeschlossenen Geräten gelten die Vorgaben des Abschnittes über die *Nutzung von IT-Endgeräten*.

14.3.4. Verwaltungsbereich

- Alle Anschlüsse (LAN und WLAN), die ausschließlich verwaltenden Organisationseinheiten der TU Graz zugeordnet sind, die entweder personenbezogene oder direkt finanzwirksame Daten verarbeiten. Diese Bereiche sind z.B. das Rektorat, Assistenzen des Rektorats und der Vizerektorinnen und Vizerektoren, Organisationseinheiten Recht und Versicherungsmanagement, Interne Revision, Finanzen und Rechnungswesen, Controlling, Studienservice und Prüfungsangelegenheiten, Qualitätswesen etc.[23].
- Erlaubte Systeme: Im Besitzt oder Eigentum der Universität stehende, von ihr freigegebene IT-Endgeräte.
- Netzzuordnung: Nicht öffentlich zugängliche Anschlüsse, die Verwaltungseinrichtungen der TU Graz zugeordnet sind.

Die Leitung der Organisationseinheit ist für die Einhaltung der Regelungen innerhalb der jeweiligen Organisationseinheit und in Zusammenarbeit mit dem ZID für die Sicherheit jedes an diesen Bereich angeschlossenen Systems verantwortlich.
Der Betrieb von Servern in diesem Bereich ist unzulässig.
Die Kommunikation aus diesem Bereich in das Internet wird im Anlassfall eingeschränkt.
Direkte Verbindungen zu IT-Endgeräten im Verwaltungsbereich von außerhalb der jeweiligen Organisationseinheit sind nur aus System-Managementbereichen gestattet.
Zum Schutz von in dieser Zone angeschlossenen Geräten gelten die Vorgaben des Abschnittes über die *Nutzung von IT-Endgeräten*.
Für die interne elektronische Kommunikation (Dateiaustausch, Messaging, E-Mail, Kalender-abstimmung etc.) dürfen nur vom ZID bereitgestellte Systeme verwendet werden.

14.3.5. Fernzugangsbereich

- Alle Verbindungen von außen an das Netzwerk der TU Graz, die auf den dafür vorgesehenen und genehmigten Wegen hergestellt werden (z.B. VPN, SSH, RDS).
- Erlaubte Systeme: Im Besitz oder Eigentum der Universität stehende, von ihr freigegebene und sonstige IT-Endgeräte.
- Netzzuordnung: Öffentlich zugängliche Anschlüsse, als öffentlich definiertes Netzwerk mit Authentifizierungsmechanismen zur Zuordnung einer von der TU Graz zur Verfügung gestellten IP-Adresse.

Mit der Bereitstellung der technischen Infrastruktur durch den ZID ist im Falle der Fernverbindung über das Internet der Einsatz von VPN-*Software* oder gleichartiger *Software* in Verbindung mit von der TU Graz zentral verwalteten Accounts vorgeschrieben.

14.3.6. Fernwartungsbereich

- Alle Verbindungen von außen an das Netzwerk der TU Graz, die auf den dafür vorgesehenen und genehmigten Wegen zu Wartungszwecken hergestellt werden (z.B. VPN, Modem).

[23] vgl. Organigramm der TU Graz

- Erlaubte Systeme: Im Besitz oder Eigentum der Universität stehende, von ihr freigegebene und sonstige IT-Endgeräte.
- Netzzuordnung: Öffentlich zugängliche Anschlüsse, als intern definiertes Netzwerk mit Authentifizierungsmechanismen zur Zuordnung einer von der TU Graz zur Verfügung gestellten IP-Adresse, die für Wartungszwecke verwendet wird.

Mit der Bereitstellung der technischen Infrastruktur durch den ZID ist im Falle der Fernverbindung über das Internet der Einsatz von VPN-Software oder gleichartiger Software in Verbindung mit von der TU Graz zentral verwalteten Accounts vorgeschrieben.
Alternative Zugänge sind mit dem ZID abzustimmen, beim ZID zu dokumentieren, von ihm zentral zu verwalten und periodisch auf deren Notwendigkeit zu überprüfen.

14.3.7. Externer Serverbereich

- Server, die aus dem Internet und dem TU-Netz erreichbar sind.
- Erlaubte Systeme: Serversysteme und Serverperipherie, die die Vorgaben des Abschnittes über den *Serverbetrieb* erfüllen.
- Netzzuordnung: Nicht öffentlich zugängliche Anschlüsse, die Dienstleistungs- und Verwaltungseinrichtungen sowie Einrichtungen für Forschung und Lehre der TU Graz oder universitätsnahen Organisationen zugeordnet sind.

Die Sicherheit jedes an diesen Bereich angeschlossenen Systems obliegt der Verantwortung der Leitung der Organisationseinheit. Für jedes System sind von der betreibenden Organisationseinheit zumindest ein System-Administrator oder eine IT-Auskunftsperson und eine Kontaktperson für Abwesenheiten des System-Administrators oder der IT-Auskunftsperson zu benennen. Die Zuordnung eines Systems zum externen Serverbereich sowie die Zuständigkeit der *Sysadmins* werden vom ZID periodisch und im Anlassfall überprüft.
Die räumliche Zuordnung eines Systems im externen Serverbereich ist grundsätzlich ein vom ZID zugewiesener Serverraum.
In den externen Serverbereich sind nur die für den jeweiligen Serverdienst notwendigen Protokolle zuzulassen.
Wartungszugänge zu Systemen im externen Serverbereich sind nur aus Systemmanagement-bereichen und bei Servern, die durch Institute selbst betrieben werden, aus dem Fernwartungsbereich gestattet.

14.3.8. Interner Serverbereich

- Server, die ausschließlich aus dem Netzwerkbereich der TU Graz erreichbar sind.
- Erlaubte Systeme: Serversysteme und Serverperipherie, die die Vorgaben des Abschnittes über den *Serverbetrieb* erfüllen.
- Netzzuordnung: Nicht öffentlich zugängliche Anschlüsse, die Dienstleistungs- und Verwaltungs-einrichtungen der TU Graz zugeordnet sind.

Die Sicherheit jedes an diesen Bereich angeschlossenen Systems obliegt der Verantwortung der Leitung der Organisationseinheit. Für jedes System sind von der betreibenden Organisationseinheit zumindest ein System-Administrator oder eine IT-Auskunftsperson und eine Kontaktperson für Abwesenheiten des System-Administrators oder der IT-Auskunftsperson zu benennen.
Die Zuordnung eines Systems zum internen Serverbereich sowie die Zuständigkeit der *Sysadmins* werden vom ZID periodisch und im Anlassfall überprüft.
Die räumliche Zuordnung eines Systems im internen Serverbereich ist grundsätzlich ein vom ZID zugewiesener Serverraum.
In den und aus dem internen Serverbereich sind nur die für den jeweiligen Serverdienst notwendigen Protokolle aus dem bzw. in das Netzwerk der TU Graz zuzulassen.
Wartungszugänge zu Systemen im internen Serverbereich sind nur aus Systemmanagementbereichen und bei Servern die durch Institute selbst betrieben werden aus dem Fernwartungsbereich gestattet.

14.3.9. Systemmanagementbereich

- IT-Systeme, die dem Betrieb und der Überwachung der zentralen IT-Infrastruktur dienen und ausschließlich aus autorisierten Bereichen des ZID erreichbar sind.
- Erlaubte Systeme: Serversysteme und Serverperipherie, die die Vorgaben des Abschnittes über den *Serverbetrieb* erfüllen.
- Netzzuordnung: Nicht öffentlich zugängliche Anschlüsse, die dem ZID der TU Graz zugeordnet sind.

Die Sicherheit jedes an diesen Bereich angeschlossenen Systems obliegt der Verantwortung des ZID.
Folgende Verbindungen sind zulässig:

- In Systemmanagementbereiche: Abgesicherte Remote-Zugriffe (z.B. SSH) aus den authorisierten Bereichen des ZID heraus von Geräten, die dem Abschnitt über die *Nutzung von IT-Endgeräten entsprechen.*
- Aus Systemmanagementbereichen: Abgesicherte Zugriffe auf die entsprechenden Managementinterfaces (z.B. Konsole, Web-Interface).

Zum Schutz von in dieser Zone angeschlossenen Systemen gelten die Vorgaben des Abschnittes über den *Serverbetrieb*.

14.3.10. Quarantänebereich

- Anschlüsse, zu denen IT-Systeme verbunden werden, die nicht den Sicherheitsanforderungen der anderen Bereiche entsprechen. Jeder Anschluss kann vorübergehend diesem Bereich zugeordnet werden.
- Erlaubte Systeme: Im Besitz oder Eigentum der Universität stehende, von ihr freigegebene Serversysteme und -peripherie oder sonstige IT-Endgeräte.
- Netzzuordnung: Nicht öffentlich zugängliche Anschlüsse, die dem ZID der TU Graz zugeordnet sind.

Die Sicherheit jedes an diesen Bereich angeschlossenen Systems obliegt der Verantwortung der Besitzerin oder des Besitzers (Benutzerin oder Benutzers).

In den und aus dem Quarantänebereich sind nur die für die Erreichung bzw. Umsetzung der geforderten technischen Sicherheitsstandards notwendigen Verbindungen und Protokolle zuzulassen.

14.3.11. Installationsbereich

- Anschlüsse, zu denen IT-Systeme verbunden werden, um mit einer neuen Installation versehen zu werden.
- Erlaubte Systeme: Serversysteme und Serverperipherie, die die Vorgaben des Abschnittes über den *Serverbetrieb* erfüllen und sonstige IT-Endgeräte.
- Netzzuordnung: Nicht öffentlich zugängliche Anschlüsse, die dem ZID der TU Graz zugeordnet sind.

Die Sicherheit jedes an diesen Bereich angeschlossenen Systems obliegt der Verantwortung der Leitung der Organisationseinheit. Für jedes System ist von der betreibenden Organisationseinheit zumindest eine Ansprechperson zu benennen.
In den und aus dem Installationsbereich sind nur die für die Installation notwendigen Verbindungen und Protokolle zuzulassen.

14.3.12. Testbereich

- Anschlüsse, zu denen IT-Systeme ausschließlich für Testzwecke verbunden werden.
- Erlaubte Systeme: Serversysteme und Serverperipherie, die die Vorgaben des Abschnittes über den *Serverbetrieb* erfüllen und sonstige IT-Endgeräte.
- Netzzuordnung: Nicht öffentlich zugängliche Anschlüsse, die dem ZID der TU Graz zugeordnet sind.

Die Sicherheit jedes an diesen Bereich angeschlossenen Systems obliegt der Verantwortung der Leitung der Organisationseinheit. Für jedes System ist von der betreibenden Organisationseinheit zumindest eine Ansprechperson zu benennen.
In den und aus dem Testbereich sind nur die für den Test notwendigen Verbindungen und Protokolle zuzulassen.

14.3.13. Sonderbereiche

- **Techniknetz der Haustechnik**
  Der Zugriff auf das Techniknetz der Haustechnik ist nur über den Fernwartungsbereich zulässig. Zum Schutz von in dieser Zone angeschlossenen Systemen gelten die Vorgaben der Abschnitte über die *Nutzung von IT-Endgeräten* und den *Serverbetrieb*.
- **Telefonie (VoIP)**
  In den und aus dem Bereich der Telefonie sind nur die für die Telefonie notwendigen Verbindungen und Protokolle zuzulassen.
  Erlaubte Systeme: Vom ZID freigegebene IT-Endgeräte (z.B. Telefone).
- **Öffentliches WLAN**
  Protokolle, Dienste etc. in diesem Bereich sind durch den ZID eingehend und ausgehend gefiltert und eingeschränkt.

Die Sicherheit jedes an diesen Bereich angeschlossenen Systems obliegt der Verantwortung der Benutzerin oder des Benutzers.

15. Logging

15.1. Zweck

Zur Erfüllung folgender Aufgaben der TU Graz

- Gewährleistung der Systemsicherheit
- Gewährleistung der Systemfunktionalität
- Analyse und Korrektur von technischen Fehlern im System
- Optimierung der Systemleistung
- Leistungsverrechnung für den Systembetrieb

ist die Erfassung von Protokolldaten auf Informationssystemen erforderlich.

15.2. Regelungen

Betrifft die Protokollierung personenbezogene Daten, die weder anonymisiert noch pseudonymisiert wurden, unterliegen diese der Datenschutzgrundverordnung (DSGVO) und dem Datenschutzgesetz (DSG). Das Logging (auch indirekt) personenbezogener Daten hat nach dem Prinzip der Datensparsamkeit zu erfolgen, für alle anderen Protokolldaten gilt: der Umfang sollte dem jeweiligen Zweck angepasst sein.

15.2.1. Aufbewahrungsdauer von Logdaten

Solange keine (indirekt) personenbezogenen Daten verarbeitet werden, können Logdaten unbegrenzt gespeichert werden, zumindest aber so lange, wie es zur Erreichung der o.g. Zwecke notwendig ist.
Für nicht ano- bzw. pseudonymisierte (indirekt) personenbezogene Daten gelten die Regelungen, die die TU Graz für personenbezogene Daten getroffen hat.

15.2.2. Schutz der Logdaten

Um Logdaten gegen Manipulation zu schützen, sind sie auf einem zentralen, besonders geschützten Log-Server („Loghost“) abzulegen, die Zeitstempel in Logdateien sind mit einem zentralen Zeitserver zu synchronisieren.

16. Sicherung betriebsrelevanter Daten und Informationen

16.1. Zweck

Zweck dieses Abschnittes ist es, die Sicherung von betriebsrelevanten Daten und Informationen der TU Graz zu regeln.
Dieser Abschnitt legt fest, welche Maßnahmen zumindest getroffen werden müssen, um die Sicherung und Wiederherstellung dieser Daten gewährleisten zu können.

16.2. Regelungen

16.2.1. Datenbestände im Sicherungsumfang

Betriebsrelevante Daten, die zur Wiederherstellung von Geschäftsprozessen notwendig sind, sind zu sichern.

16.2.2. Umfang und Frequenz der durchzuführenden Sicherungen

Die Mindest- und Maximalaufbewahrungsfristen sowie Sicherungszyklen (Umfang und Frequenz) sind von dem jeweiligen *Data-Owner* schriftlich festzulegen.
Die Datensicherungen müssen zumindest den folgenden Anforderungen entsprechen:

- Sicherungen erfolgen zumindest einmal täglich.
- *Backup-Sysadmins* können bei Bedarf weitere Sicherungen anstoßen.

16.2.3. Kennzeichnung und Inventarisierung der Sicherungsmedien

Die eingesetzten Sicherungsmedien sind zu inventarisieren, zu kennzeichnen und so zu verwalten, dass deren gesicherte physische Zerstörung am Ende ihres Lebenszyklus gewährleistet ist.
Die physische Zerstörung ist schriftlich zu dokumentieren.

16.2.4. Physische Schutzmaßnahmen für Sicherungen

Im Rahmen ihres Einsatzes sind Sicherungsmedien so zu schützen, dass ein unberechtigter Zugriff auf sie verhindert wird. Dies betrifft sowohl die Orte und Räume, in denen sie eingesetzt und gelagert werden, als auch Transportwege zwischen diesen Orten und Räumen.
Aufbewahrungsorte für Sicherungen sind räumlich weit genug vom Aufstellungsort der zu sichernden Systeme entfernt zu wählen und hinreichend gegen Feuer, Wasser, unzulässige Temperatur und Luftfeuchtigkeit, gegen Stromausfall, unberechtigten Zutritt etc. zu schützen.

16.2.5. Logische Schutzmaßnahmen für Daten und Sicherungsmedien

Gesicherte Daten sind so zu schützen, dass ein unberechtigter Zugriff auf sie verhindert wird. Dies betrifft sowohl Daten auf Sicherungsmedien, als auch elektronisch übertragene Daten.
Die zu ergreifenden logischen Schutzmaßnahmen sind je nach Schutzbedürftigkeit der Daten festzulegen.

16.2.6. Wiederherstellung von Daten

Die Datenwiederherstellung muss zumindest den folgenden Anforderungen entsprechen:

- Die zuständigen *Backup-Sysadmins* können Wiederherstellungen jederzeit anstoßen.
- *Data-Owner* und autorisierte Personen können Wiederherstellungen jederzeit veranlassen. Die Wiederherstellung erfolgt zeitnah im Rahmen der Betriebszeiten.
- Die Verantwortlichkeit für die Nutzbarkeit der wiederhergestellten Daten (Bereitstellung notwendiger Systemumgebung) für die Geschäftsprozesse liegt beim jeweiligen *Data-Owner*.

16.2.7. Maßnahmen zur Prüfung der Integrität der Sicherungsmedien

Zur Sicherstellung der Integrität der gesicherten Daten müssen zumindest die folgenden Maßnahmen gesetzt werden:

- Das *Backup*-System prüft die Medien auf Schreib- und Lesefehler und verweigert defekte Medien.
- Die Funktionsfähigkeit des *Backup*-Systems muss regelmäßig überprüft und dokumentiert werden.

16.2.8. Maßnahmen zur Langzeitsicherung von Daten

Wenn vom Rektorat gefordert, sind Daten in Absprache mit dem jeweiligen *Data-Owner* in ein Langzeitarchiv zu überführen.

16.2.9. Protokollierung

Wiederherstellungsvorgänge sind zu dokumentieren und die entsprechenden Protokolldaten den *Data-Ownern* über einen vorab vereinbarten Zeitraum auf Anfrage zur Verfügung zu stellen. Die Protokollierung von Sicherungen und Wiederherstellungen erfolgen automatisch in den Systemlogdateien.

17. Domain

17.1. Zweck

Seitens der TU Graz werden als Domaininhaber Pflichten gegenüber ACOnet und Dritten übernommen. Dabei trägt die TU Graz die volle Verantwortung, übernimmt beträchtliche Haftungsrisiken und muss Name und Ruf der TU Graz in der Öffentlichkeit entsprechend wahren. Zweck dieses Abschnittes ist es den rechtmäßigen Betrieb der Domains an der TU Graz sicherzustellen.
Inhaber der Domains „tu-graz.ac.at“ und „tugraz.at“ ist die TU Graz. Die Domain „tu-graz.ac.at“ wird aus historischen Gründen noch für ausgewählte Services weiterverwendet, die offizielle Domain der TU Graz lautet aber „tugraz.at“. Im Rahmen der Verwendung dieser Domain betreibt die TU Graz für eine Reihe von Organisationen bzw. Organisationseinheiten sowohl Sub-Domains von „tugraz.at“ bzw. „tu-graz.ac.at“, als auch anderslautende, d.h. nicht mit „tugraz.at“ oder „tu-graz.ac.at“ endende Domains, zugehörigen DNS-Zonen, sowie die den IP-Adressen zugeordneten Reverse-Zonen.
Zu diesem Zweck wird vom ZID der TU Graz die zentrale IT-Infrastruktur (Netzwerk, IT-Systeme, Anwendungen etc.) bereitgestellt.
Bei Verwendung von Diensten jeglicher Provider sind die entsprechenden Allgemeinen Geschäftsbedingungen und Vertragsbedingungen einzuhalten, betreffend das ACOnet insbesondere „die Grundsätze für die Teilnahme an ACOnet“. Zusätzliche Informationen werden in der Homepage vom ZID bereitgestellt.

17.2. Regelungen für den Domainbetrieb

17.2.1. Betrieb der DNS-Server

DNS-Server (*Authoritative Domain Name Server* für die Domain „tu-graz.ac.at" und „tugraz.at") werden ausschließlich durch den ZID betrieben und für den zulässigen Domainbetrieb bereitgestellt. Der Betrieb von Authoritative DNS-Servern durch einzelne Organisationseinheiten ist grundsätzlich untersagt. Im Einzelfall kann durch Gewährung einer Ausnahme (siehe Abschnitt *Ausnahmen von der Richtlinie*) unter Sicherstellung aller Sicherheitsanforderungen im Sinn dieser Richtlinie der Betrieb von DNS-Servern durch einzelne Organisationseinheiten erfolgen.

17.2.2. Zulässiger Domainbetrieb

Grundsätzlich zulässig ist der Betrieb

- einer Sub-Domain der Domains „tu-graz.ac.at" bzw. „tugraz.at" oder wenn der Inhaber der Sub-Domain oder der anderslautenden Domain die TU Graz ist oder
- eine TU Graz nahe Organisation im Sinne der „Grundsätze für die Teilnahme an ACOnet" ist und die TU Graz ihr ausdrückliches Interesse an deren Unterstützung bekundet hat.

17.2.3. Unzulässiger Domainbetrieb

Jedenfalls unzulässig ist der Betrieb

- einer Sub-Domain der Domains „tu-graz.ac.at" bzw. „tugraz.at" außerhalb des TUGnet und den darin vorgesehenen IP-Bereichen oder
- einer Sub-Domain der Domains „tu-graz.ac.at" bzw. „tugraz.at" innerhalb der IT-Infrastruktur der TU Graz zu kommerziellen oder gewerblichen Zwecken im Sinne der „Grundsätze für die Teilnahme an ACOnet" oder
- einer anderslautenden Domain (nicht auf „tugraz.at" oder „tu-graz.ac.at" endend) innerhalb der IT-Infrastruktur der TU Graz, die keinen Bezug zur TU Graz aufweist oder
- einer Domain außerhalb der IT-Infrastruktur der TU Graz, die aufgrund ihrer Gestaltung (z.B. „abctugraz.at") zu einer Verwechslungsgefahr und damit einer Zurechnung zur TU Graz und der Domain „tugraz.at" führt oder
- einer Domain mit Personenbezug zu aktiven Angehörigen der TU Graz oder
- einer Domain mit TU Graz Bezug, deren Inhaber nicht die TU Graz ist, vgl. Punkt 17.2.5., oder
- einer Fremddomain unter Einbinden von Webseiten der TU Graz in ein Frameset (iframe)[24] oder
- einer Fremddomain, mit der Ausnahme für zeitlich begrenzte nationale und internationale Kooperationen und Projekte der TU Graz. Der ZID übernimmt weder die Registrierung noch jegliche Kosten, die mit dem Betrieb der Fremddomain verbunden sind[25].

[24] anders ausgedrückt: Inhalte, die an der TU Graz bereitgestellt werden, müssen auch in der Location-Zeile als solche erkennbar sein.
[25] Für nationale und internationale Kooperationen ist eine Umschaltung in die Domäne tugraz.at nicht erforderlich, für Projekte die innerhalb der TU Graz unter einer Fremddomain laufen, hat eine Umschaltung in die Domäne tugraz.at zu erfolgen.

17.2.4. Nationale und internationale Kooperationen

Für nationale und internationale Kooperationen ist es zulässig, Domains oder Sub-Domains im Ganzen oder teilweise, ein- oder wechselseitig zu betreiben. Im Impressum ist der Hinweis "*System hosted at Graz University of Technology*" zu führen.

17.2.5. Domaininhaber

Grundsätzlich sind offizielle Inhalte der TU Graz unter„tugraz.at" bereitzustellen. In begründeten Einzelfällen kann eine Ausnahme (siehe Abschnitt *Ausnahmen von der Richtlinie*) gewährt werden. In diesen Ausnahmefällen ist die TU Graz als Domaininhaber einzutragen. Die Kosten für die Registrierung sind durch die beantragende Organisationseinheit selbst zu tragen.
Werden für Kooperationen „Fremddomänen" registriert, kann an Stelle der TU Graz der Kooperationspartner als Domaininhaber eingetragen werden. Die Kosten sind durch die beteiligte Organisationseinheit oder den Kooperationspartner zu tragen.

17.2.6. Zertifikate

Für folgende Domains werden Gratis-Zertifikate im Rahmen der ACOnet-Teilnehmerschaft vergeben:

- tugraz.at
- tu-graz.ac.at
- vc-graz.ac.at

Für Seiten, auf denen offizielle Inhalte der TU Graz bereitgestellt werden, sind solche Zertifikate zu verwenden.
Für „Weiterschaltungsdomains" können auch andere Zertifikate (z.B. von *Lets-Encrypt*) verwenden werden. Die Verwendung von Zertifikaten wird auch bei Fremddomains empfohlen. Die beteiligte Organisationseinheit bzw. der Kooperationspartner hat selbst für die Kosten und die Verwendung der Zertifikate Sorge zu tragen. Für Fremddomains erfolgt keine Vergabe von Zertifikaten durch den ZID.

17.3. Antragstellung

Durch Einbringung des formlosen E-Mail-Antrags auf Freigabe und Einrichtung einer Domain bzw. Subdomain erklärt die Antragstellerin oder der Antragsteller, die einschlägigen gesetzlichen Bestimmungen zu beachten und insbesondere niemanden in seinen Kennzeichenrechten und Wettbewerbsrechten (Namensrecht, Markenrecht, Wettbewerbsrecht etc.) zu verletzen.
Die TU Graz behält es sich vor, sich bei der Antragstellerin oder beim Antragssteller allenfalls schad- und klaglos zu halten, wenn die TU Graz durch in ihren Rechten verletzte Dritte in Anspruch genommen wird und die Rechtsverletzung auf die von der Antragstellerin oder vom Antragsteller beantragte Domain-Delegation zurückzuführen ist.
Im Falle einer anderslautenden Domains (nicht mit „tugraz.at" oder „tu-graz.ac.at" endend), die innerhalb der IT-Infrastruktur der TU Graz betrieben wird, muss als Ansprechperson (in der Regel *Technical Contact* genannt) gegenüber der Registrierungsstelle zumindest eine Bedienstete oder ein Bediensteter des ZID eingetragen sein.

17.4. Entscheidung

In eindeutigen Fällen entscheidet die Leitung des ZID.
In allen anderen Fällen entscheidet die Leitung des ZID in Abstimmung mit der Organisationseinheit Recht und Versicherungsmanagement.

17.5. Nutzungsbedingungen

Berechtigte Nutzer der IT-Infrastruktur der TU Graz sind verpflichtet, folgende Regelungen zu beachten:

1. Einhaltung aller mit der Nutzung in Zusammenhang stehenden Richtlinien und Regelungen.
2. Einhaltung der Regelungen betreffend unzulässige Nutzung von ACOnet an der TU Graz („teilnehmende Institution“) entsprechend der ACOnet *Acceptable Use Policy*.
3. Unzulässig ist ferner die bewusste Inanspruchnahme von ACOnet-Diensten zur Übertragung, Verbreitung oder Speicherung von Daten, welche
    - gegen bestehende Gesetze verstößt oder die öffentliche Ordnung oder die Sittlichkeit gefährdet,
    - Schutzrechte anderer (z.B. Datenschutz, Urheberrecht) verletzt,
    - andere Netzteilnehmer behindert, belästigt oder verängstigt (z.B. Spam),
    - schädliche Komponenten (z.B. Viren, Trojanische Pferde) enthält,
    - zur Erlangung eines unautorisierten Zugriffs dient (z.B. Portscan, Passwort-Scan, Ausnutzung von Systemschwächen, Phishing),
    - eine Beeinträchtigung des Netzbetriebs beabsichtigt (z.B. bewusstes Herbeiführen eines Systemabsturzes, DoS-Attacken).

Verstöße gegen die ACOnet-Richtlinien werden von der TU Graz („teilnehmende Institution“), insbesondere vom ZID der TU Graz, entsprechend der *ACOnet Acceptable Use Policy* unverzüglich abgestellt.

18. Webhosting

18.1. Zweck

Im Rahmen der vom ZID der TU Graz angebotenen Webhosting-Services muss durch organisatorische und technische Maßnahmen die wirtschaftliche, sichere und gesetzeskonforme Verwendung der IT-Infrastruktur gewährleistet werden.
Zweck dieses Abschnittes ist es, Verantwortlichkeiten festzulegen und Regelungen für die Beantragung und Nutzung von Webspace zu treffen.

18.2. Regelungen

18.2.1. Persönlicher Webspace

Verantwortlich für persönlichen Webspace ist jene Person, der dieser zugeteilt wurde.

18.2.2. Beantragung von Webhosting für Organisationseinheiten

Berechtigt, einen Antrag auf Webspace zu stellen, sind Universitätsangehörige, die ein aufrechtes Dienstverhältnis an der TU Graz haben, wobei die Gesamtverantwortung für den Webspace bei der Leitung der Organisationseinheit liegt.

Die Nutzungsdauer des Webspace ist lt. Betriebsordnung ab Einrichtung befristet. Eine gewünschte Verlängerung erfordert ein formfreies Schreiben bis spätestens zwei Wochen vor Ablauf der ursprünglichen Frist. Der Webspace wird nach Ende der Nutzungsdauer deaktiviert und in weiterer Folge nach Ablauf von drei Monaten gelöscht.

Im Antrag sind die Benutzer-Kennungen aller Personen anzugeben, die Zugriffsberechtigungen auf den Webspace benötigen. Voraussetzung dafür ist, dass die betreffenden Personen bereits im zentralen Benutzermanagement erfasst sind. Änderungen bedürfen der Zustimmung des Leiters der Organisationseinheit.

Im Antrag ist ein entsprechend qualifizierter technischer Ansprechpartner anzugeben. Änderungen sind vom Leiter der Organisationseinheit bekanntzugeben. Die Stellvertretung des technischen Ansprechpartners ist der Leiter der Organisationseinheit.

18.2.3. Nutzung des Webspace

- Der *Webspace* darf ausschließlich für dienstliche Zwecke oder strategische Ziele der TU Graz genutzt werden. Ausdrücklich nicht zulässig ist die Nutzung zu kommerziellen oder gewerblichen Zwecken sowie eine Weitergabe an fremde Einrichtungen.
- Die Leitung der Organisationseinheit sorgt dafür, dass die *Webspace*-Inhalte den jeweils aktuellen gesetzlichen und universitätsinternen Bestimmungen entsprechen. Insbesondere sind das Urheberrecht und die Offenlegungspflichten zu beachten.
- Es obliegt der Leitung der Organisationseinheit, für die laufende Datensicherung und die Archivierung der Daten vor Ende der Nutzungsdauer zu sorgen.
- Die von den *Webspace*-Zugriffsberechtigten installierten Anwendungen und Konfigurationen sind in Bezug auf Sicherheitsupdates aktuell zu halten, sodass ein angemessenes Sicherheitsniveau gewährleistet ist.
- Ist ein angemessenes Sicherheitsniveau oder die Einhaltung der gesetzlichen und sonstigen rechtlichen Rahmenbedingungen nicht gewährleistet, so ist der *Webspace* vom ZID zu deaktivieren und sind von der Leitung der Organisationseinheit der erforderliche Sicherheitszustand und entsprechende Rechtskonformität herzustellen.
- Bei Kenntnis von rechtswidrigen Inhalten ist der Zugriff darauf unverzüglich von der verantwortlichen Person zu unterbinden bzw. kann vom ZID unterbunden werden.

TEIL D Schluss- und Begriffsbestimmungen

19. Ausnahmen von der Richtlinie

Es ist generell zunächst eine Vorgehensweise zu wählen, die den geltenden Richtlinienabschnitten entspricht. Erst wenn dies technisch oder organisatorisch nicht möglich oder nicht wirtschaftlich ist, kann über eine Ausnahmeregelung entschieden werden.

Ausnahmen müssen

- zeitlich begrenzt werden,
- auf Zweck und Benutzerkreis eingeschränkt werden,
- hinsichtlich Antrag, Genehmigung/Ablehnung, Änderungen und Auslaufen dokumentiert werden,
- kontrolliert und im Falle des Auslaufens ohne Neuantrag nach entsprechender Frist,
- im Falle der Nichtbeachtung einschlägiger Richtlinien der TU Graz umgehend aufgehoben werden.

Der Antrag zur Erteilung einer Ausnahme ist von Angehörigen der TU Graz bzw. Dritten an den **Informationssicherheitsbeauftragten (ISB)** zu stellen, welcher über die Anträge auf Ausnahmen entscheidet. Die aktuell gewährten Ausnahmen werden getrennt von dieser Richtlinie im Dokument „Ausnahmen von IT-Sicherheitsrichtlinien TU Graz“ vom Informationssicherheitsbeauftragten verwaltet. Das Ausnahmenregister ist nicht öffentlich einsehbar.

20. Umsetzung und Überprüfung der Einhaltung der Richtlinienvorgaben

- Die Einhaltung der in dieser Richtlinie enthaltenen Regelungen und Sicherheitsmaßnahmen wird regelmäßig, aber auch anlassbezogen überprüft.
- Die Datenschutzkoordination ist mit der Umsetzung und Überprüfung der Einhaltung des Datenschutzes an der TU Graz beauftragt.
- Der Informationssicherheitsbeauftragte ist für die Umsetzung und Überprüfung der Informationssicherheit für die gesamte TU Graz verantwortlich.
- Überprüfungen im Rahmen der Informationssicherheit in den zentralen Bereichen erfolgen durch den ZID, soweit die Richtlinie nichts anderes vorsieht.
- In den dezentralen Bereichen ist der Informationssicherheitsbeauftragte für die Überprüfung der Informationssicherheit verantwortlich. Die operative Prüfung erfolgt durch das ISKT.
- Die Leitung der Organisationseinheiten unterstützt den Informationssicherheitsbeauftragten bei dessen Aufgaben.
- Werden bei Überprüfungen Abweichungen bei der Umsetzung festgestellt, sind diese zu dokumentieren.

Ein Verstoß gegen diese Richtlinien kann neben dienst- und disziplinarrechtlichen Folgen auch zivil- und strafrechtliche Konsequenzen nach sich ziehen.

21. Begriffsbestimmungen

Account
Unter einem Account, auch als (Benutzer-)Konto bezeichnet, wird eine Kombination aus einer Benutzer-ID und einem Kennwort verstanden. Diese beiden Elemente bilden die sogenannten Zugangsdaten. Ein Account stellt eine Zugriffsberechtigung zu einem geschützten IT-System dar.
Die Begriffe Konto, Benutzerkonto oder *User Credentials* werden als Synonyme für Account verwendet.

Account mit erweiterten Rechten
Als Account mit erweiterten Rechten werden jene Accounts bezeichnet, die umfassendere Rechte als Standard-Accounts besitzen. In der Regel gehören der *Sysadmin/Systemoperator* (z.B. der Benutzer *root)* zu dieser Benutzergruppe.

Anonymisierung/Pseudonymisierung
Anonymisierung modifiziert Identifikationsmerkmale (z.B. den Namen oder andere personenbezogene Daten) so, dass diese einer bestimmten Person dauerhaft nicht mehr zugeordnet werden können. Anonymisierte Daten gelten nicht als personenbezogene Daten.
Pseudonymisierung ersetzt Identifikationsmerkmale durch ein Pseudonym, meist eine Kombination aus Buchstaben und Zahlen. Anders als bei der Anonymisierung bleiben die Bezüge zwischen Pseudonym und Identifikationsmerkmal jedoch erhalten. Über diesen so genannten „Schlüssel“ können Identifikationsmerkmale einer bestimmten Person wieder zugeordnet werden. Pseudonymisierte Daten gelten daher als personenbezogene Daten.

Autorisierte Person
Autorisierte Personen im Kontext dieses Dokuments besitzen, aufgrund der Ermächtigung durch den *Data-Owner*, die legitimierte Berechtigung Datenwiederherstellungen zu veranlassen. Der *Data-Owner* hat eine Liste über alle von ihm autorisierten Personen zu führen.

Backup-Sysadmin
Personen die mit der Sicherung und Wiederherstellung von Daten betraut sind.

Benutzer-ID
Als Benutzer-ID wird eine Zeichenfolge aus Buchstaben, Ziffern und/oder Sonderzeichen bezeichnet, die eine eindeutige Zuordnung zu einem Berechtigungsprofil darstellt und somit personenbezogen ist.
Die Begriffe Username, Benutzername, TUGRAZonline-Benutzername oder User-ID werden als Synonyme für Benutzer-ID verwendet.

Betroffene/r
Jede natürliche Person, deren Daten verarbeitet werden.

Custodian

Custodian (Verwalter) sind im Kontext dieses Dokuments Organisationen, Organisationseinheiten oder Personen, die im Rahmen ihrer Funktion beauftragt und zuständig sind, Daten und Informationen im Sinne des *Data-Owners* auftragsgemäß zu verwenden, d.h. zu verarbeiten[27].
Entsprechend dem vom *Data-Owner* festgelegten Schutzbedarf und der vom ihm gewählten Klassifikation sind von Custodians sinnvolle Schutzmaßnahmen (insbesondere bei personenbezogenen Daten ggf. TOM lt. DSGVO) zu setzen.

Data Breach

Die DSGVO definiert in Art. 4 Z 12 eine „Verletzung des Schutzes personenbezogener Daten“ (*Data Breach*, Datenleck, Datenpanne, Datenmissbrauch, Datenverlust) als „eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt[28], die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.“

Daten

Daten sind die Grundlage von Information und können sowohl in digitaler Form (z.B. auf IT-Systemen gespeichert, auf mobilen Datenträgern abgelegt) als auch in analoger Form (z.B. gedruckt, handschriftlich) vorliegen. Daten können z.B. Zahlen oder Worte sein. Daten können zu Datenkategorien, wie Prüfungsunterlagen, Forschungsdaten oder Personaldaten zusammengefasst werden.

Daten im Sinne der DSGVO und des DSG

- „Personenbezogene Daten“

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Darunter sind alle personenbezogenen Angaben über Betroffene natürliche Personen zu verstehen, unabhängig von deren technischer Repräsentation, also sowohl elektronische Daten als auch solche auf Papier, Mikrofilm etc. Vollständig anonymisierte und nicht personenbezogene Daten sind von der DSGVO nicht umfasst.

[27] Beispielsweise bedeutet Verarbeitung im Sinne der DSGVO: jede mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
[28] z.B. werden personenbezogene Daten von Studierenden oder Sponsoren in großem Umfang auf öffentlich zugänglichen Webseiten publiziert; ein Notebook mit Daten der Organisationseinheit Personalabteilung geht verloren, wird gestohlen oder geraubt; Mitarbeiterinnen oder Mitarbeiter greifen unbefugt auf Daten zu; Daten werden an falsche Empfängerinnen und Empfänger versandt; es kommt zu einem Hacking-Angriff mit Datendiebstahl oder -verlust durch Löschung.

- „Besondere Kategorien von Daten“ (besonders schutzwürdige Daten; früher: sensible Daten)

Personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Data-Owner

Data-Owner (Dateneigentümer) im Kontext dieses Dokuments besitzen die legitimierte Verfügungsberechtigung über Daten und Informationen und sind für diese verantwortlich.
Diese sind z.B. die Leiter von Dienstleistungseinrichtungen, *Departments*, Fakultäten, Dekanaten und Instituten, die stellvertretend für ihre Organisationseinheit als *Data-Owner* verstanden werden.
Data-Owner kann aber auch die TU Graz sein, repräsentiert durch das Rektorat.
Ebenso können Personen, die Daten in eigener Verantwortung erstellen, als *Data-Owner* verstanden werden, z.B. Bedienstete, die aus freien Stücken Daten generieren, deren Eigentümer nicht, wie z.B. bei Diensterfindungen, automatisch der Dienstgeber wird.
Zuletzt kommen als *Data-Owner* auch Externe in Frage, z.B. Unternehmen oder Personen, die der TU Graz Daten überlassen, darüber jedoch die Verfügungsberechtigung bewahren.

Datenträgerverantwortliche

Datenträgerverantwortliche sind Personen, die im Rahmen ihrer Funktion autorisiert sind, Datenträger bzw. Geräte, in denen elektronische Speichermedien verbaut sind, zu betreiben oder eigenständig zu nutzen.

Domain

Unter einer Domain wird ein zusammenhängender Teilbereich des hierarchischen *Domain Name System* (DNS) verstanden (authoritative – maßgebend).

Druckersystem, Drucker

Unter einem Druck(er)system wird die Gesamtheit aus Hardware und Software verstanden, die die zu druckenden Daten entgegennimmt, verarbeitet und an einen Drucker ausliefert.
Unter einem Drucker wird ein Peripheriegerät verstanden, das zur Ausgabe von Daten auf ein Trägermedium, meist Papier, verwendet wird.
Umfasst sind auch Multifunktionsgeräte (z.B. Kombinationsgeräte Drucker-Fax-Scanner) in ihrer Eigenschaft als Drucksysteme und Drucker.

Druckprotokoll, Protokolldaten, Logdaten

Unter einem Druckprotokoll wird ein automatisch geführtes Ereignisprotokoll von Prozessen auf einem Drucksystem verstanden. Die dadurch entstandenen Daten werden als Protokolldaten oder Logdaten bezeichnet.

Freigegebene Hardware und Software

Darunter werden IT-Endgeräte, IT-Peripheriegeräte, mobile Datenträger, Betriebssysteme, Anwendungen /Softwareprodukte etc. verstanden, die bestimmten, von der TU Graz festgelegten Kriterien entsprechen.

Freigegebene Systeme

Darunter werden Systeme verstanden, die von der TU Graz für den jeweiligen Netzwerkbereich festgelegten Bedingungen entsprechen.

Funktionsbenutzer-ID

Eine Funktionsbenutzer-ID darf im Gegensatz zu personenbezogenen Benutzer-IDs von mehreren Personen verwendet werden.

Geschäftsprozess

Ein Geschäftsprozess besteht aus verknüpften Einzeltätigkeiten (Aufgaben, Aktivitäten), die ausgeführt werden, um ein wesentliches geschäftliches oder betriebliches Ziel zu erreichen.

Gruppe

Unter einer Gruppe wird eine Menge von Personen mit gemeinsamen Eigenschaften verstanden. Beispiele: Studierende, Angestellte, Beamtinnen und Beamte, Gastprofessorinnen und Gastprofessoren, Mitarbeiterinnen und Mitarbeiter von Fremdfirmen, Lektoren, Emeriti, Alumni.

Gültigkeitsdauer

Unter Gültigkeitsdauer wird der Zeitraum (Beginn und Ende) verstanden, in dem eine Zuordnung zu einer Rolle aktiv ist.

Identität, Identity

Unter Identität wird eine Sammlung von Attributen verstanden, die die natürliche Person, die sich dieser Identität bedient, eindeutig identifizierbar macht.

Im Eigentum der Universität stehende Geräte

Darunter werden Geräte verstanden, über die die TU Graz die uneingeschränkte Verfügungsgewalt besitzt.

Information(en)

Information baut auf Daten auf. Im Verständnis dieses Dokuments stellt Information Daten dar, die so aufbereitet wurden, dass sie eine für den Empfänger inhaltlich fassbare, verständliche Form angenommen haben. Daten werden also so verknüpft oder strukturiert, dass sie Bedeutung erlangen, z.B. in Form von E-Mails, Tabellen, Datenbanken oder schriftlichen Dokumenten.

Informationssystem
Ein Informationssystem bezeichnet die Gesamtheit der IT-Infrastruktur, bestehend aus Hardware, Software, Daten, Speichertechnik, Kommunikation und Netzwerk, welche für ein bestimmtes Aufgabengebiet entwickelt wurde.

Initial-Kennwort
Als Initial-Kennwort wird ein Kennwort bezeichnet, das einmalig für den Account gesetzt wird.

IT-Arbeitsmittel
Unter IT-Arbeitsmitteln werden verstanden: Hardware, d.h. IT-Endgeräte, IT-Peripheriegeräte, IT-Zubehör, Datenträger etc. sowie Software auf den IT-Geräten, außerdem Geräte wie Telefonapparate, Funkgeräte, Mobiltelefone, Presenter etc.

IT-Auskunftsperson
Unter IT-Auskunftspersonen werden in diesem Dokument jedenfalls die EDV-Beauftragten lt. Campus-managementsystem und die für die IKT an der jeweiligen Organisationseinheit zuständigen Personen verstanden.

IT-Endbenutzer
Personen, die aus dem in dieser Richtlinie definierten Geltungsbereich stammen und eines der in dieser Richtlinie definierten IT-Endgeräte und damit in Verbindung stehende (mobile) Datenträger oder IT-Peripheriegeräte nutzen.

IT-Endgerät
Kleinrechner (Desktop-Computer, PC), tragbare Geräte (Notebooks, Tablet-PCs, Tablets etc.), netzwerkfähige Kleingeräte (Smartphones, Mobiltelefone, Navigationsgeräte, Datenerfassungsgeräte, VoIP-Telefone etc.), Endgeräte bei Labor-/Messgeräten sowie Multifunktionsgeräte (Kombifaxe, Druck-/Fax-Stationen etc.)

Kennwort
Als Kennwort (*Password*) wird eine Zeichenfolge aus Buchstaben, Ziffern und/oder Sonderzeichen bezeichnet, die die Überprüfung einer Identität möglich macht.
Die Begriffe Passwort, Schlüsselwort, TUGRAZonline-Kennwort oder Password werden als Synonyme für Kennwort verwendet.

Logdatei, Protokolldaten, Logdaten
Unter einer Logdatei wird ein automatisch geführtes Ereignisprotokoll von Prozessen auf einem IT-System verstanden. Die dadurch entstandenen Daten werden als Protokolldaten oder Logdaten bezeichnet.

Logging
Unter Logging wird die Protokollierung von Ereignissen verstanden.

Loghost
Unter einem Loghost wird ein Server verstanden, der für andere Server Logdateien zugriffgeschützt speichert.

Logische Schutzmaßnahmen
Maßnahmen die einen unberechtigten Zugriff auf gesicherte Daten verhindern, z.B. Verwendung von Kennwörtern oder Verschlüsselung von Dateien.

Managementschicht
Unter einer Managementschicht wird ein *Virtual Machine Monitor* (z.B. Hypervisor) einschließlich der IT-Administrationswerkzeuge verstanden. Von dieser Managementschicht werden virtuelle Server bereitgestellt.

Mehrfaktor-Authentifizierung
Die Zwei-Faktor-Authentisierung (2FA) bezeichnet den Identitätsnachweis eines Nutzers mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren).

Mobiler Datenträger
Speichersticks (USB-Sticks), Speicherkarten aller Art (auch in Ausweiskarten, Multimedia-Abspielgeräten, in Kameras etc.), mobile Festplatten (z.B. magnetisch und flashspeicherbasiert), CDs, DVDs, Disketten, Magnetbänder und ähnliche Speichermedien.

Netzwerkkomponente
Physische oder virtuelle Komponenten des Netzwerks mit *Routing-, Bridging-, Switching-* oder ähnlichen Funktionen wie z.B. *Router, Switches, Hubs, Firewalls, Access Points, Modems*, VPN-Konzentratoren, einige Arten von *Load Balancern* etc.

Projekt
Unter einem Projekt versteht man zeitlich befristete Vorhaben, die mittels Projektmanagement geführt werden (z.B. Forschungsprojekte, Infrastrukturprojekte, Softwareprojekte etc.).

Rolle
Unter einer Rolle wird ein Bündel von Benutzungsberechtigungen verstanden.

Secure Print
Mit der Funktion *Secure Print* wird ein Druckauftrag nicht sofort ausgegeben, sondern erst nach Freigabe am Gerät, z.B. der Druckauftrag oder die Druckfreigabe ist mit einem Kennwort, Code oder Chipkarte geschützt.

Server, Serversystem

Unter einem Server wird ein Rechner verstanden, der IT-Dienste für andere IT-Systeme und deren Benutzer zur Verfügung stellt.

Serverdienst, Service

Unter einem Serverdienst wird ein Programm verstanden, das über entsprechende Protokolle Dienste anbietet (z.B. Webserver, E-Mailserver, Druckserver, Cloud-/Dateiserver, Datenbankserver, DHCP-Server, Nameserver, Timeserver).

Service-Owner

Unter einem *Service-Owner* wird die Person, die für den ordentlichen Betrieb einer Anwendung bzw. eines IT-Services zuständig und verantwortlich ist (z.B. der Webmaster, der den Webserver betreut und betreibt) verstanden. Der *Service-Owner* steht zwischen dem *Data-Owner* und dem Sysadmin/SysOp.

Sicherheitsvorfall

Unter einem Sicherheitsvorfall versteht man ein Ereignis, das die Informationssicherheit (die Vertraulichkeit, Integrität und/oder die Verfügbarkeit von Daten, personenbezogenen Daten, Informationen und dem daraus entstandenem Wissen) beeinträchtigen.

Social Networks und Social Media

Social Networks sind Netzgemeinschaften bzw. Web-Anwendungen, die Netzgemeinschaften beherbergen. Handelt es sich um Technologien, bei denen die Benutzer gemeinsam Inhalte erstellen, erzeugen, teilen und konsumieren, bezeichnet man diese als *Social Media*.

Speichersystem

Unter einem Speichersystem wird ein Verbund von Speichermedien verstanden, der große Datenmengen nichtflüchtig speichert. Beispiele sind verteilte Speichersysteme, SAN, NAS, *Backup*systeme, Archivsysteme.

Subdomain

Unter einer Subdomain wird eine Domain verstanden, die in der Hierarchie unterhalb einer anderen liegt.

Sysadmin (SysOp)

Unter einem *Sysadmin/SysOp* wird im Rahmen dieses Dokuments eine Person verstanden, die für den Betrieb der IT-Systemhardware und der Betriebssystem-Software zuständig ist (oft mit erweiterten Benutzerrechten).

Verarbeitung

Unter einer „Verarbeitung“ ist laut Art. 4 Z 2 DSGVO Folgendes zu verstehen: Jeder „mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im

Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung."

Virtuelle Server

Virtuelle Server teilen sich physische Rechner und deren Ressourcen. Die operative Verwaltung der virtuellen Server und Ressourcen erfolgt durch eine Managementschicht.

Webhosting

Unter Webhosting wird die Bereitstellung von im Allgemeinen öffentlich über HTTP/HTTPS erreichbarem Webspace durch den ZID der TU Graz verstanden.
Nicht von diesem Begriff in dieser Richtlinie umfasst sind der Intranet- und Internetauftritt der TU Graz.

Webspace

Unter Webspace wird dediziert zugewiesener Speicherplatz mit damit verbundenen Services (z.B. Datenbanken, Scripting) verstanden.

Zertifikat

Ein (digitales) Zertifikat ist ein digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann.