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	Thomas Riedrich/ Stephanie Pichler	Claudia von der Linden	Rektoratsbeschluss
Datum	25.07.2018	25.07.2018	07.08.2018

Zweck

Diese Richtlinie legt Regelungen fest, um Informationssicherheit an der Technischen Universität Graz (TU Graz) sicherzustellen. Informationssicherheit dient dem Schutz von Daten, Informationen und daraus entstandenem Wissen vor unberechtigtem Zugriff, unbefugter Kenntnisnahme und Preisgabe, vor Verlust, Zerstörung und vor Veränderung, und ermöglicht die Nachvollziehbarkeit von Daten- und Informationsflüssen. 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

EU Datenschutz-Grundverordnung (DSGVO) idgF.

Datenschutzgesetz (DSG) idgF.

Verhaltenskodex (Compliance Richtlinie)

Vollmachten und Richtlinien Handbuch der TU Graz

Richtlinie für Mobile Endgeräte der Technischen Universität Graz

Prozessverantwortung und Kontakt

Prozessverantwortung: Leitung des Zentralen Informatikdienstes

Kontakt für technische Fragen: it-security@tugraz.at

Kontakt für datenschutzrechtliche Fragen: datenschutz@tugraz.at

Inhaltsverzeichnis

1. Begriffserklärungen

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 Administratoren 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.

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.

Data Beach

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[1], 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 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.

[1] z.B. werden personenbezogene Daten von Studierenden oder Sponsoren in großem Umfang auf öffentlich zugänglichen Webseiten publiziert; ein Notebook mit Daten der OE 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.

Freigegebene Hardware und Software

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

Funktionsbenutzer-ID

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

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.

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 Gehalt 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-Endbenutzer

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

IT-Endgerät

Standgeräte (Desktops), tragbare Geräte (Notebooks, Tablet-PCs, Tablets etc.), netzwerkfähige Kleingeräte (Smartphones, Mobiltelefone, Navigationsgeräte, Datenerfassungsgeräte, VoIP-Telefone etc.), Endgeräte bei Medizintechnikgeräten sowie Multifunktionsgeräte (Kombifaxe, Druck(Fax)stationen etc.)

Kennwort

Als Kennwort 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.

Mobiler Datenträger

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

Privacy-by-design/Privacy-by-default

Die DSGVO und das DSG definieren in Bezug auf die datenschutzgerechte Beschaffung und Implementierung von Informationssystemen Folgendes:

- Privacy-by-design – Datenschutz durch Technikgestaltung siehe Art. 25 Abs. 1 DSGVO
- Privacy-by-default – datenschutzfreundliche Voreinstellungen siehe Art. 25 Abs. 2 DSGVO

Rolle

Unter einer Rolle wird ein Bündel von Benutzungsberechtigungen verstanden.

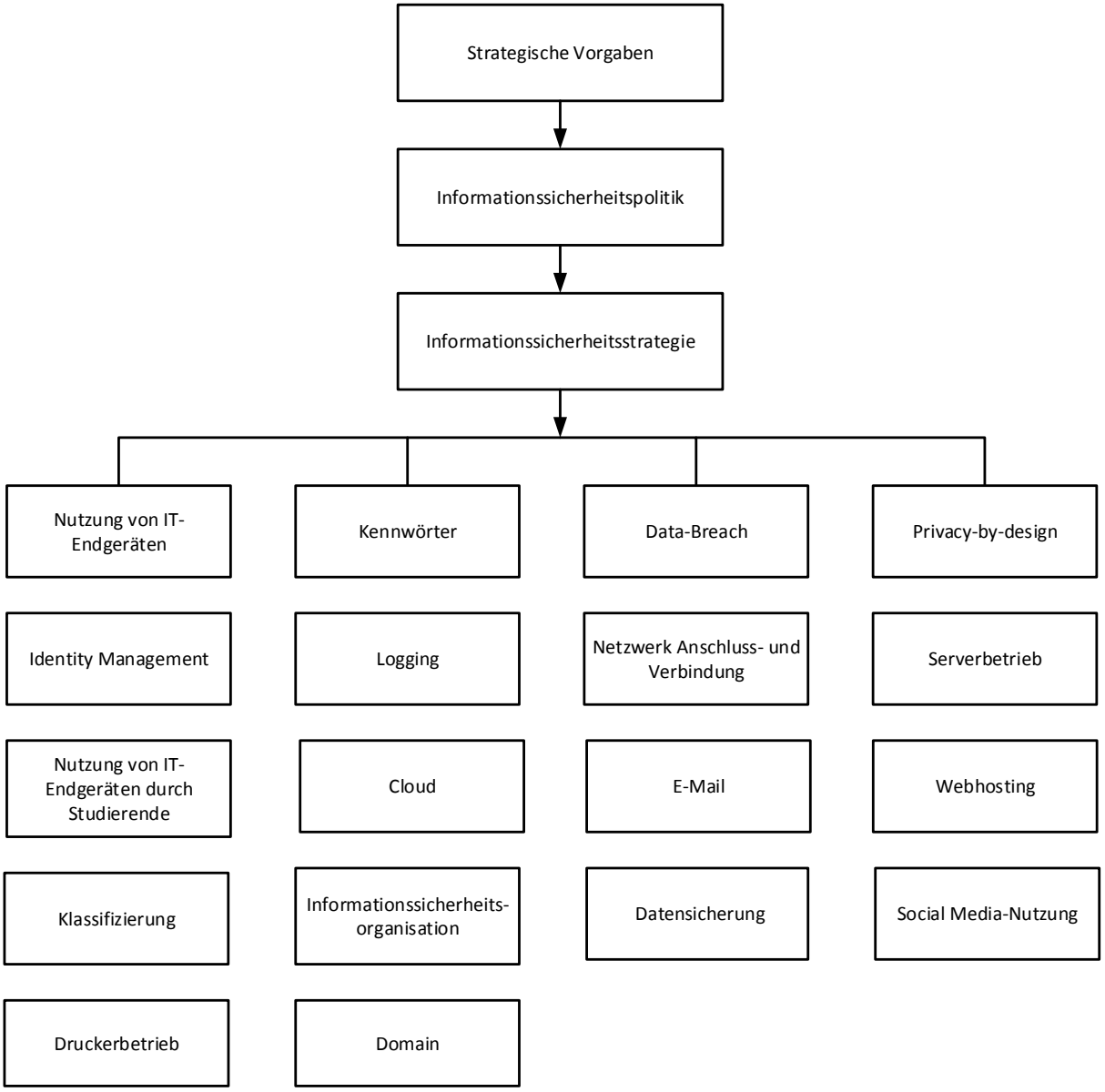
Verarbeitung

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.“ Der Begriff ist somit sehr weit gefasst.

2. Die Regelungshierarchie zu Informationssicherheit

2.1 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.



2.2. Ebenen der Regelungshierarchie

2.2.1. Strategische Vorgaben

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

2.2.2. Sicherheitspolitik inklusive –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.“

2.2.3. Sicherheitsrichtlinienabschnitte (Prozessstandards)

Prozessstandards 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.“

2.2.4. 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*. Für die Verschlüsselung von ruhenden Daten auf Windows-Endgeräten ist Bitlocker zu verwenden und folgendermaßen zu konfigurieren: *xyz*."

2.2.5. 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: „Bei der Ausgabe von Smartphones sind folgende Checklisten-Punkte mit der Empfängerin oder dem Empfänger abzuarbeiten: a, b, c. Die Liste ist binnen 72h per E-Mail an *xyz* zu übermitteln."

Unterstützende Dokumente und Materialien

Z.B. Sensibilisierungsunterlagen wie Schulungspräsentationen, Poster, E-Mails etc.

3. Informationssicherheitspolitik

3.1. Zweck:

Die Informationssicherheitspolitik der TU Graz drückt die Ziele und die Verantwortungshaltung der Universitätsleitung aus und schafft damit den Rahmen für nachhaltiges Informationssicherheitsmanagement.

Neben den gesetzlichen Verpflichtungen sind es die Ansprüche und Erwartungen der TU Graz, ihrer Angehörigen, Partnerinnen und Partner und Lieferantinnen und Lieferanten sowie der Öffentlichkeit, die Informationssicherheit zu einem wichtigen Thema machen.

Die Abhängigkeit von Information und Informationssystemen, deren zunehmende Vernetzung, verschärfte gesetzliche Rahmenbedingungen, und die damit verbundenen internen und externen Risiken machen es notwendig, Anforderungen an die Informationssicherheit zu regeln. Informationssicherheit, und damit verwandt, Daten- und IT-Sicherheit, sind daher nicht Selbstzweck, sondern ein wesentlicher Aspekt unserer Arbeitsweise.

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.

3.2. 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, für uns gleichwertigen Ziele wirksam unterstützen:

- Einhaltung gesetzlicher Vorgaben und vertraglicher Vereinbarungen.
- Positionierung der TU Graz als vertrauensvolle, zuverlässige Partnerin.

- 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

3.3. 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.

3.4. 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.

4. Informationssicherheitsstrategie

4.1. 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.

4.2. 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[2].

Aus den ermittelten Schutzbedürfnissen sind folglich entsprechende Maßnahmen[3] abzuleiten, wobei „Good Practices“[4] und „der Stand der Technik“ als Grundlage angesehen werden.

4.3. Themenkreise

Um ein angemessenes Schutzniveau erreichen zu können, müssen zumindest folgende Themenkreise behandelt werden:

- Personenbezogene Sicherheit – Human Resources Security
- Umgang mit Ressourcen – Asset Management
- Zugriffskontrolle – Access Control
- Kryptografie – Cryptography
- Physische Sicherheit – Physical And Environmental Security
- Betriebssicherheit – Operations Security
- Kommunikationssicherheit – Communications Security

[2] 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“. Details siehe Punkt 9.2.
[3] Maßnahmen können organisatorischer, technischer und physischer Natur sein.
[4] Darunter wird eine grundsätzliche Normen- und Standardorientierung verstanden, z.B. an ISO/IEC Normen, COBIT und Branchenstandards (z.B. Gesundheitswesen).

- Sicherheit bei Beschaffung, Entwicklung und Betrieb von Informationssystemen
- Lieferantenbeziehungen – Supplier Relationships
- Umgang mit Sicherheitsvorfällen – Information Security Incident Management
- Informationssicherheitsaspekte in Bezug auf die Aufrechterhaltung des Betriebs – Information Security Aspects of Business Continuity
- Einhaltung der Sicherheitsvorschriften, Regelbefolgung – Compliance

4.4. Prinzipien zur Erreichung der angestrebten Informationssicherheitsziele

4.4.1. Berücksichtigung von Informationssicherheit in allen Projekten

Informationssicherheit wird bei Projekten mit Bezug zu informationssicherheitsrelevanten Zielen als ein eigenständiges Projektziel betrachtet.

In Bezug auf Projekte ist Informationssicherheit ein gleichwertiges Ziel neben Funktionalität und Leistungsfähigkeit bei der Entwicklung, der Beschaffung und dem Einsatz von informationsverarbeitenden Systemen.

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

4.4.2. Orientierung an Good Practice-Ansätzen

Informationssicherheit bei der TU Graz orientiert sich an anerkannten Normen sowie Good Practice-Ansätzen – diese sind zumindest folgende:

- ISO/IEC 2700x[5]
- Österreichisches Informationssicherheitshandbuch[6]
- BSI Grundschutz[7]

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.

[5] https://www.iso.org/isoiec-27001-information-security.html (kostenpflichtige Norm)
[6] https://www.sicherheitshandbuch.gv.at/downloads/sicherheitshandbuch.pdf
[7] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

4.4.3. Klassifizierung durch Informationseigentümer

Die Klassifizierung (Schutzbedarfsfeststellung) sowie Autorisierung zur Nutzung der Daten und Informationen erfolgt durch deren Dateneigentümer[8], die Umsetzung der Vorgaben durch deren Custodians[9].

4.4.4. Anwendung des Need-To-Know-Prinzips

Die Autorisierung zur Nutzung von 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).

4.4.5. 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 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).

4.5. Vorgehensweisen zur Erreichung der angestrebten Ziele

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

4.5.1. Erfassung

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

[8] Dieser Begriff ist vergleichbar mit dem des Auftraggebers/Verantwortlichen im Datenschutzrecht. Dateneigentümer (Data Owner) sind z.B. Fachabteilungen, Institute, Tochtergesellschaften, assoziierte Vereine, Kooperationspartner, Projektteams.

[9] Dieser Begriff ist vergleichbar mit der Dienstleisterin oder des Dienstleisters/der Auftragsverarbeiterin oder des Auftragsverarbeiters im Datenschutzrecht.

4.5.2. Zuordnung

Den Daten- und Informationsbeständen, dazugehörigen Prozessen und Ressourcen[10] sind eindeutige Dateneigentümer und Custodians zuzuordnen.

4.5.3. 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[11] zu entwickeln und dokumentieren.

4.5.4. 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.

4.5.5. Übernahme von Restrisiken

Restrisiken sind festzuhalten und zu bewerten. Die Verantwortung für die Restrisiken ist im Innenverhältnis zum Rektorat durch die zuständige Dateneigentümerin und den zuständigen Dateneigentümer zu übernehmen.

4.5.6. Überprüfung der Einhaltung der Sicherheitskonzepte

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

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

[11] 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.

4.5.7. 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.

5. Identity Management

5.1. 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 Management (IDM) im Sinne dieses Dokuments ist es, digitale Identitäten mit all ihren Rollen zu verwalten und die an das IDM angeschlossenen IT-Systeme mit verlässlichen und aktuellen Daten zu versorgen.

5.2. Regelungen

Angebotene IT-Dienstleistungen sind von der OE Zentraler Informatikdienst (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[12] erteilt werden. Diese Fälle sind zu dokumentieren.

- Gruppenzuordnungen sind von den für sie verantwortlichen Stellen[13] zu pflegen, insbesondere ist deren Gültigkeitsdauer festzulegen. Daraus ergeben sich die Rollenzugehörigkeiten.
- Einer Identität ist ausschließlich ein Account zugeordnet (Single-Account-Policy).
- Werden mehrere IDM-Erfassungssysteme verwendet, sind diese konsistent zu halten.
- Alle Systeme, die IT-Dienstleistungen aus dem Servicekatalog erbringen, haben die aktuellen Berechtigungen aus dem IDM zu berücksichtigen.[14]

[12] z.B. Leiter von Organisationseinheiten, Projektverantwortliche, Service-Verantwortliche.
[13] OE Studienservice und Prüfungsangelegenheiten, OE Personalabteilung, Dekanate etc.
[14] z.B. Deaktivieren von SSH-Keys.

- Der ZID (IDM Service und Security Service) sind ermächtigt, Berechtigungen bei Gefahr in Verzug ohne vorherige Warnung vorübergehend zu entziehen.

Bezüglich der Löschung von Berechtigungen und Identitäten sind insbesondere die DSGVO, das DSG und Betriebsvereinbarungen zu beachten.
Geheimhaltungspflichten sind nach Beendigung des Dienst-/Vertragsverhältnisses weiterhin einzuhalten.

6. Nutzung von IT-Endgeräten

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 ist Information, und damit verbunden der Einsatz von Informationstechnologien (IT), unerlässlich.

6.2. Benutzungsregelungen für IT-Endgeräte der TU Graz

6.2.1. Allgemeine Regelungen

IT-Endgeräte, die im 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:

1. Die Arbeit mit Administrator- oder Root-Rechten auf IT-Endgeräten mit Rechtetrennung, außer zu dienstlich notwendigen Arbeits- und Wartungszwecken.
2. Das Verschleiern der eigenen Identität im Rahmen der dienstlichen Internet-Nutzung, außer zu Forschungszwecken.
3. Der Einsatz von Soft- und Hardware und sonstigen Mitteln, deren Zweck es ist, Informationen auszuspähen, außer zu dienstlich notwendigen Zwecken.
4. Das Neustarten (Booten) von öffentlich zugänglichen IT-Endgeräten über externe, nicht autorisierte Datenträger.
5. Die Installation sicherheitsgefährdender Programme.
6. Veränderung von erkennbar sicherheitsrelevanten Einstellungen.[15]
7. Das bewusste Inkaufnehmen IT-bezogener Sicherheitsrisiken - im Zweifelsfall ist eine Abstimmung mit dem ZID zu suchen.

6.2.2. Gerätesperre und Kennwortschutz

Der kennwortgeschützte Sperrbildschirm auf Notebooks, Desktops und Tablet-PCs ist so einzustellen, dass er spätestens nach 15 Minuten Inaktivität aktiviert wird und ist bei Verlassen des Arbeitsplatzes manuell zu aktivieren. Die Gerätesperre auf Smartphones und Tablets ist so einzustellen, dass sie spätestens nach 5 Minuten Inaktivität aktiviert wird.

Das Deaktivieren der voreingestellten Gerätesperre bzw. des kennwortgeschützten Sperrbildschirms ist untersagt.

Für Demorechner, Laborrechner und Anzeigetafeln 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 Notebooks, Desktops und Tablet-PCs sind in Bezug auf Sicherheitsupdates aktuell zu halten. Auf Notebooks, Desktops und Tablet-PCs ist ein aktueller Schadsoftwarescanner 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

[15] z.B. Das Deaktivieren des kennwortgeschützten Sperrbildschirms, das Deaktivieren des Schadsoftwarescanners

Schadsoftwaresignaturen auf Notebooks, Desktops und Tablet-PCs sind bei signaturbasierenden Schadsoftwarescannern aktuell zu halten und bei Aufbau einer Netzwerkverbindung zur TU Graz vor deren weiteren Nutzung zu aktualisieren, analoges gilt für die technischen Grundlagen der Schadsoftwareerkennung bei der Nutzung anderer Technologien.
Das Deaktivieren des Schadsoftwarescanners und das Einschränken oder Verhindern der automatischen Installation von Sicherheitsupdates ist untersagt.
Für Demorechner, Laborrechner und Anzeigetafeln kann von dieser Verpflichtung abgewichen werden.

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 Abschnitt Data-Breach einzuhalten. Darüber hinaus ist bei Verlust oder Diebstahl von IT-Endgeräten oder mobilen Datenträgern, die im Eigentum der TU Graz stehen, umgehend eine polizeiliche Anzeigebestätigung bei der OE Recht und Zentrale Services abzugeben.

6.2.5. Beendigung des Dienstverhältnisses/Vertragsverhältnisses

Bei Beendigung des Dienstverhältnisses bzw. eines Vertragsverhältnisses 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 Verleihdauer bei der ausleihenden Person. Für die Sicherung jeglicher Daten und Informationen auf den Leihgeräten im Sinne dieser Richtlinie ist die ausleihende Person verantwortlich.

6.3. Benutzungsregelungen für private IT-Endgeräte/ bring your own device (BYOD)

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. Anspruch auf Unterstützung durch den ZID besteht in diesen Fällen nicht. 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, analoges 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. Kennwörter

7.1. 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 Informations- und Kommunikationssysteme 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.

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.

7.2. Regelungen betreffend die Struktur von Kennwörtern

Kennwörter müssen zumindest den folgenden Anforderungen („MINIMALANFORDERUNGEN“) entsprechen:

Eigenschaft	*Standard-Account (Standardbenutzer)*	*Account (Benutzer) mit erweiterten Rechten*
Minimale Kennwortlänge	8	12
Komplexitätserfordernisse (mindestens drei der vier angeführten müssen erfüllt sein)	• Mindestens ein Großbuchstabe (A bis Z) • Mindestens ein Kleinbuchstabe (a bis z) • Mindestens eine Ziffer (0 bis 9) • Mindestens ein Sonderzeichen (!“#$%&'()*+,-./:;<=>?@[\]^_`{|}~)	
Unzulässige Phrasen	• Vor-, Nach- und Username, Sozialversicherungsnummer und Matrikelnummer dürfen nicht Teil des Kennwortes sein. • „Standardfragmente“ (abcd, qwert, 1234, asdf, passwort) sind nicht erlaubt. • Ein neues Kennwort muss sich von allen Kennwörtern der letzten 18 Monate an mindestens 3 Stellen unterscheiden.	

Maximales Kennwortalter: legt fest, wie lange ein einmal gewähltes Kennwort längstens verwendet werden darf.	maximale Gültigkeit von 450 Tagen
Kennwort-Historie: Zeit, innerhalb derer ein Kennwort nicht wiederverwendet werden darf.	Ein neues Kennwort muss sich von allen Kennwörtern der letzten 18 Monate an mindestens 3 Stellen unterscheiden.
Anzahl von erlaubten Fehlversuchen, bis das Konto gesperrt wird	Keine Sperre, bei Falscheingabe zeitliche Verzögerung
Zeit, die nach einer Falscheingabe gewartet werden muss, bis eine neue Eingabe angenommen wird;.	Nach 3 Fehlversuchen eine Verzögerung von 30 Sekunden, danach bei Falscheingabe jedes Mal eine Verzögerung von 30 Sekunden; die Zeit ist nicht ansteigend
Zweifaktor-Authentifizierung erforderlich	Nein

7.3. Regelungen für den Gebrauch von Kennwörtern

- Kennwörter sind von der vorgesehenen Benutzerin oder vom vorgesehenen Benutzer geheim zu halten und dürfen nicht weitergegeben werden[16]. Auf eine unbeobachtete Eingabe des Kennworts ist zu achten.
- Kennwörter dürfen nicht ungesichert über das Netzwerk 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.

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

- 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 zu ändern.
- Werkseitig voreingestellte Kennwörter sind umgehend entsprechend den Minimalanforderungen zu ändern.
- Zusätzliche Regelungen können, abhängig von der jeweiligen Situation, dann getroffen werden, wenn dies aus Risikogesichtspunkten notwendig erscheint.

7.4. Regelungen für die Vergabe von Initial-Kennwörtern

Die Struktur von Initial-Kennwörtern muss zumindest den Minimalanforderungen des Punkts 7.2. entsprechen.

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

8. Privacy-by-design

8.1. Zweck:

Zweck dieses Abschnittes ist es, Rahmenbedingungen für die datenschutzgerechte Beschaffung, Entwicklung und Implementierung von Informationssystemen zu formulieren. An der TU Graz ist deren Einhaltung eine Grundlage für einen datenschutzrechtskonformen Betrieb.

8.2. Grundsätze

Vorrangiges Ziel von Privacy-by-design ist die Datenminimierung und Verhinderung unbeabsichtigter oder zweckentfremdender Verwendung eines Informationssystems. Die Anforderung Privacy-by-design ist bei Beschaffung, Entwicklung und Implementierung eines Informationssystems daher von Beginn an zu berücksichtigen.

Privacy-by-design verpflichtet die im Geltungsbereich dieser Richtlinie umfassten Personen, bei der Beschaffung, Entwicklung und Implementierung von Informationssystemen die folgenden Grundsätze zu beachten:

8.2.1. Minimise

- Das Informationssystem verarbeitet nur jene personenbezogenen Daten, die zur Zweckerfüllung notwendig sind. Darüberhinausgehend erhobene personenbezogene Daten werden anonymisiert verarbeitet.
- Die für die jeweiligen personenbezogenen Daten geltenden Löschfristen, unter Beachtung der anwendbaren Aufbewahrungspflichten, werden eingehalten.

8.2.2. Hide

- Personenbezogene Daten werden über angemessen abgesicherte Übertragungswege übermittelt[17] und auf angemessen geschützten Datenträgern gespeichert[18].
- Personenbezogene Daten werden nur den zur Zweckerfüllung notwendigen Personen zugänglich gemacht.

[17] z.B. TLS-verschlüsselt
[18] z.B. AES-verschlüsselt

8.2.3. Seperate

- Von unterschiedlichen Informationssystemen erhobene und verarbeitete personenbezogene Daten werden unabhängig bzw. getrennt voneinander gespeichert und verarbeitet.

8.2.4. Aggregate

- Personenbezogene Daten werden auf dem höchsten Aggregationsniveau und gleichzeitig dem geringstmöglichen Detailgrad verarbeitet, in dem sie ihren Zweck noch erfüllen.

8.2.5. Inform

- Eine den rechtlichen Anforderungen entsprechende Datenschutzleitlinie ist für das Informationssystem vorhanden und den betroffenen Personen zugänglich.
- Das Informationssystem bietet den betroffenen Personen die Möglichkeit zu erkennen, welche personenbezogenen Daten zu welchem Zweck auf welcher Rechtsgrundlage und wie verarbeitet und mit Dritten geteilt werden.

8.2.6. Control

- Die betroffenen Personen können auf die sie betreffenden Datenschutzeinstellungen zugreifen und über die Verarbeitung und insbesondere auch die Veröffentlichung ihrer Daten bestimmen, diese im Zuge der Beauskunftung einsehen, berichtigen und ggf. löschen lassen.
- Die Nutzbarkeit des Informationssystems durch die dazu berechtigten betroffenen Personen ist auch dann gewährleistet, wenn zur Zweckerbringung nicht notwendige personenbezogene Daten nicht zur Verfügung gestellt werden.

8.2.7. Enforce

- Die den rechtlichen Anforderungen entsprechende Datenschutzleitlinie für das Informationssystem ist umgesetzt.
- Es ist sichergestellt, dass im Falle eines Sicherheitsvorfalls die betroffenen Personen unverzüglich und auf rechtskonforme Weise über den Vorfall und mögliche Auswirkungen informiert werden können.

8.2.8. Demonstrate

- Die Einhaltung der Datenschutzleitlinie und der anwendbaren gesetzlichen Bestimmungen kann nachgewiesen werden.

8.3. Maßnahmen

Privacy-by-design verpflichtet die im Geltungsbereich dieser Richtlinie umfassten Personen, bei der Beschaffung und Implementierung von Informationssystemen die folgenden Maßnahmen zu beachten:

8.3.1. Technische Maßnahmen

- Es werden so wenig personenbezogene Daten wie möglich und nur die für den jeweiligen Zweck notwendigen Daten verarbeitet („so wenig wie möglich und so viel wie nötig“).
- Es wird sichergestellt, dass durch die Voreinstellungen Informationssysteme so konfiguriert sind, dass personenbezogene Daten ohne Eingreifen der Person nicht einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden, außer der Verarbeitungszweck erfordert die Zugänglichmachung eben dieser personenbezogenen Daten (Privacy-by-default).
- Personenbezogene Daten einer Person werden so weit wie möglich verteilt und von anderen sie betreffenden personenbezogenen Daten abgegrenzt verarbeitet.
- Personenbezogene Daten werden auf dem höchsten Aggregationsniveau und mit dem gleichzeitig geringstmöglichen Detailgrad verarbeitet, in dem sie ihre Zwecke noch erfüllen („so verdichtet wie möglich und so fein granular wie gerade noch nötig“).
- Personenbezogene Daten und ihre Zusammenhänge sind nicht offen einsehbar, sondern vor unberechtigter Einsichtnahme geschützt, außer der Verarbeitungszweck erfordert die Veröffentlichung eben dieser personenbezogenen Daten.

8.3.2. Organisatorische Maßnahmen

- Betroffene sind angemessen informiert, wenn personenbezogene Daten über sie verarbeitet werden.
- Betroffene verfügen über die Kontrolle über die Verarbeitung ihrer personenbezogenen Daten.

- Eine mit den rechtlichen Anforderungen in Einklang stehende Datenschutzleitlinie ist vorhanden, umgesetzt und wird durchgesetzt.
- Die Einhaltung der Datenschutzleitlinien der TU Graz und aller anwendbaren gesetzlichen Bestimmungen ist entsprechend nachweisbar.

8.4. Nichterfüllen der Grundsätze oder Maßnahmen

Erfüllt ein Informationssystem die in diesem Abschnitt aufgezählten Grundsätze voraussichtlich nicht oder können die in diesem Abschnitt aufgezählten Maßnahmen voraussichtlich nicht umgesetzt werden, so ist die Datenschutzkoordination der TU Graz zu kontaktieren. Diese oder dieser prüft im Einzelfall, ob das Informationssystem den gesetzlichen Bestimmungen entspricht.

9. Data Breach

9.1. Zweck:

Dieser Abschnitt beschreibt den erforderlichen Umgang mit einem erfolgten, vermuteten oder möglichen „Data Breach“ (Datenmissbrauch, Datenverlust) im Sinne der DSGVO an der TU Graz.

9.2. Allgemeine Vorgaben der DSGVO

9.2.1. Vorgehen bei einem Data Breach

Gemäß DSGVO sind bei einem erfolgten oder möglichen unberechtigten Zugriff auf personenbezogene Daten unter bestimmten Umständen unverzüglich die Datenschutzbehörde (DSB) bzw. alle betroffenen Personen zu informieren. Datenlecks sind unverzüglich zu schließen. Diese Meldepflichten können auch Situationen betreffen, in den es zu einer unbeabsichtigten oder unerwünschten Löschung von personenbezogenen Daten (Datenverlust) kommt.

Um diese Situation gar nicht entstehen zu lassen, ist der unter Punkt 9.3. dargestellte Prozess zum Umgang mit Datenschutz- und Datensicherheitsverletzungen an der TU Graz auch dann in Gang zu setzen, wenn lediglich der Verdacht auf derartige Sachverhalte besteht.

9.2.2. Informationspflichten an die DSB und an die betroffenen Personen

Laut Art. 33 DSGVO tritt eine Informationspflicht dann ein, wenn der TU Graz bekannt wird, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem Risiko oder zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen[19] führt.
Was ein „hohes Risiko“ im Vergleich zu einem „Risiko“ darstellt, ist im Einzelfall festzustellen.

Die DSGVO sieht für den Fall einer solchen Verletzung des Schutzes personenbezogener Daten folgende Melde- und Benachrichtigungspflichten vor:

- Unverzügliche Meldung an die DSB, möglichst binnen 72 Stunden, ansonsten mit Begründung, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
- Unverzügliche Benachrichtigung der betroffenen Person in klarer und einfacher Sprache, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.

Die Benachrichtigung der betroffenen Person darf jedoch unterbleiben, wenn eine der folgenden Bedingungen erfüllt ist:

- Die Verantwortliche oder der Verantwortliche hat geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und hat diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt, insbesondere solche Maßnahmen, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung.
- Die Verantwortliche oder der Verantwortliche hat durch nachfolgende Maßnahmen sichergestellt, dass das hohe Risiko für die Rechte und

[19] Vorfälle können beispielsweise folgende Auswirkungen hervorrufen: Verlust der Kontrolle über die personenbezogenen Daten der betroffenen Person, z.B. durch Veröffentlichung sensibler Daten; Identitätsdiebstahl; finanzielle Verluste; Rufschädigung; Verlust von wichtigen Unterlagen; Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile; Diskriminierung.

Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht.

- Die Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

9.3. Vorgehen bei Verdacht/ Eintritt des Data Breach

9.3.1. Erste Schritte für alle Angehörigen der TU Graz

1. Die Person, die vom Vorfall erfahren hat, kontaktiert unverzüglich die jeweilige Dienstvorgesetzte oder den jeweiligen Dienstvorgesetzten oder direkt die Datenschutzkoordination der TU Graz unter databreach@tugraz.at und übermittelt alle vorliegenden sachdienlichen Informationen.
2. Die Dienstvorgesetzte oder der Dienstvorgesetzte kontaktiert unverzüglich die Datenschutzkoordination der TU Graz unter databreach@tugraz.at.

9.3.2. Weiteres Vorgehen der Datenschutzkoordination, des Rektorats und des Datenschutzbeauftragten

3. Die Datenschutzkoordination der TU Graz initiiert eine technische und rechtliche Prüfung des Vorfalls, gegebenenfalls gemeinsam mit den Daten- bzw. IT-Verantwortlichen und bei Bedarf weiteren Personen:
    a. Erheben des Sachverhalts und prüfen, ob die Voraussetzungen für eine Meldepflicht bestehen, insbesondere:
        - Wann und wo kam es zu dem Vorfall?
        - Um was für eine Art von Vorfall handelt es sich?
        - Sind personenbezogene Daten von dem Vorfall betroffen?
        - Welche Daten sind betroffen?
        - Wie viele Personen bzw. Datensätze sind von dem Vorfall betroffen?
        - Welcher Klassifizierung unterliegen diese Daten? (z.B. interne oder vertrauliche Daten)
        - Welche IT-Systeme und/oder Datenträger, inkl. Papier, sind betroffen?
        - Mit welchen Folgen des Vorfalls müssen die betroffenen Personen wahrscheinlich rechnen?

- Welche Maßnahmen zur Behebung des Vorfalls wurden ergriffen oder werden vorgeschlagen?
- Welche Maßnahmen zur Abmilderung der Auswirkungen des Vorfalls auf die betroffenen Personen wurden gesetzt oder werden vorgeschlagen?

b. Setzen von technischen und organisatorischen Maßnahmen zur Verhinderung eines allfällig weiteren Datenmissbrauchs[20].

4. Das Rektorat entscheidet nach Beratung mit dem Datenschutzbeauftragten, ob und in welcher Form die Datenschutzbehörde und gegebenenfalls auch die betroffenen Personen zu informieren sind und setzt allfällige weitere Schritte, z.B. Abgabe einer Sachverhaltsdarstellung an die Staatsanwaltschaft oder eine Prüfung arbeitsrechtlicher Schritte.
5. Der Datenschutzbeauftragte setzt gegebenenfalls alle im Zuge der Meldungen notwendigen Schritte gegenüber der Datenschutzbehörde und gegebenenfalls informiert das Rektorat die betroffenen Personen.
6. Nach Abschluss der Bearbeitung des Vorfalls ist zum Zwecke der kontinuierlichen Verbesserung der Abläufe eine Nachbesprechung durchzuführen.
7. Alle an der Bearbeitung eines erfolgten, vermuteten oder möglichen Vorfalls Beteiligten sind angehalten, gegenüber Dritten Stillschweigen zu bewahren.
8. Bei Kontaktversuchen durch Medien sind diese an das involvierte Rektoratsmitglied bzw. die Pressesprecherin oder den Pressesprecher zu verweisen.
9. Behördenkontakte sind ebenfalls nur nach Rücksprache mit einem Rektoratsmitglied zu pflegen oder herzustellen.

[20] z.B. Anzeige bei der Staatsanwaltschaft oder Polizei, Unterbrechen der Verbindung zu einem Server, Einspielen eines Software-Patches, Entziehen von Zugriffsberechtigungen einer verdächtigen Person.

10. Folgen der Nichteinhaltung

Die Einhaltung der in dieser Richtlinie enthaltenen Regelungen und Sicherheitsmaßnahmen wird regelmäßig, aber auch anlassbezogen überprüft.
Ihre Missachtung kann neben entsprechenden disziplinären und dienstrechtlichen auch zivil- und strafrechtliche Folgen nach sich ziehen.

11. Ausnahmen von dieser Richtlinie

Es ist generell zunächst eine Vorgehensweise zu wählen, die den geltenden Richtlinien 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 ZID zu stellen.
Die aktuell gewährten Ausnahmen werden getrennt von dieser Richtlinie im Dokument „Ausnahmen von IT-Sicherheitsrichtlinien TU Graz“ vom ZID verwaltet. Das Ausnahmenregister ist nicht öffentlich einsehbar.