IT-Sicherheits-Richtlinie

Arbeitsgruppe IT-Sicherheit
der TU Clausthal

2017-07-18

Vorbemerkung

Das Sicherheitskonzept wendet sich an alle Mitarbeiter und Mitarbeiterinnen sowie die Studierenden, die übrigen Mitglieder und Angehörigen der Technischen Universität Clausthal.
In dieser Richtlinie haben die Rollen folgende Bedeutung:

Universitätsleitung Der Präsident und das Präsidium

IT-Sicherheitsbeauftragter Die vom Präsidium mit der Wahrnehmung der Aufgaben betraute Person. Der derzeitige IT-Sicherheitsbeauftragte findet sich auf der IT-Sicherheits-Webseite der TU Clausthal: `https://tu-c.de/itsec`

Bereichsleitung Diejenige Person, die der fraglichen Einrichtung, Abteilung, usw. vorsteht.

Verfahrensverantwortlicher Diejenige Person, die für ein bestimmtes Verfahren oder einen Prozess verantwortlich ist.

IT-Beauftragter Diejenige Person eines Instituts, Einrichtung oder Abteilung, die von der Einrichtung ermächtigt wurde, die Richtlinien zur IT-Nutzung vorzugeben.

IT-Personal zentrale oder dezentrale Administratoren, die für die Wartung, Installation, Konfiguration usw. von Hard- und Software zuständig sind.

IT-Anwender eine Person, die IT nutzt.

A Allgemeines

A.1 Anwenderqualifizierung

Verantwortlich für die Initiierung: IT-Beauftragter
Verantwortlich für die Umsetzung: IT-Beauftragter
Die Mitarbeiter sind aufgabenspezifisch zu schulen und dürfen erst dann mit IT-Verfahren arbeiten. Dabei sind sie insbesondere auch mit den für sie geltenden Sicherheitsmaßnahmen und den Erfordernissen des Datenschutzes vertraut zu machen.

Die Schulung hat prinzipiell auch das allgemeine Sicherheitsbewusstsein und die Einsicht in die Notwendigkeit von IT-Sicherheitsmaßnahmen zu entwickeln. Die Schulung sollte auch eine realistische Selbsteinschätzung fördern. Die Anwender sollten erkennen, wann Experten hinzugezogen werden sollten.
Eine entsprechende Schulung wird in der Regel in jedem Semester durch das Rechenzentrum angeboten. Zusätzliche Informationen werden an zentraler Stelle bereitgestellt.

A.2 Meldung von Sicherheitsproblemen

Verantwortlich für die Initiierung: IT-Beauftragter
Verantwortlich für die Umsetzung: IT-Beauftragter
Auftretende Sicherheitsprobleme aller Art (Systemabstürze, fehlerhaftes Verhalten von bisher fehlerfrei laufenden Anwendungen, Hardwareausfälle, Eindringen Unbefugter, Manipulationen, Virenbefall u. a.) sind dem zuständigen IT-Personal mitzuteilen. Jeder schwerwiegende Vorfall ist zu dokumentieren und der Arbeitsgruppe IT-Sicherheit zu melden. Die AG IT-Sicherheit berichtet an den IT-Sicherheitsbeauftragten.

A.3 Konsequenzen und Sanktionen bei Sicherheitsverstößen

Verantwortlich für die Initiierung: IT-Sicherheitsbeauftragter
Verantwortlich für die Umsetzung: Universitätsleitung
Verstöße werden nach den geltenden rechtlichen Bestimmungen geahndet.
Als Verstoß gilt die vorsätzliche oder grob fahrlässige Nichtbeachtung der IT-Sicherheitrichtlinie, insbesondere, wenn sie

- die Sicherheit der Mitarbeiter, Nutzer, Vertragspartner, Berater und des Vermögens der TU Clausthal in erheblichem Umfang beeinträchtigt,
- der TU Clausthal erheblichen finanziellen Verlust durch Kompromittierung der Sicherheit von Daten oder Geschäftsinformationen einbringt,
- den unberechtigten Zugriff auf Systeme und Informationen, deren Preisgabe und/oder Änderung beinhaltet,
- die Nutzung von Informationen der TU Clausthal für illegale Zwecke beinhaltet und
- den unbefugten Zugriff auf personenbezogene Daten ermöglicht.

Beurteilung und Ahndung eines Verstoßes erfolgen für Mitarbeiter der Universität in jedem Einzelfall unter Beteiligung des Personalrates.
Zur Gefahrenintervention können zur IT-Sicherheit von den IT-Beauftragten oder dem Rechenzentrum Netzzugänge oder Benutzerkonten vorübergehend deaktiviert werden.

B Sicherung der Infrastruktur

B.1 Räumlicher Zugangsschutz

Verantwortlich für die Initiierung: IT-Beauftragter
Verantwortlich für die Umsetzung: IT-Personal, IT-Anwender
Der unbefugte Zugang zur IT-Infrastruktur der TU Clausthal und die unbefugte Nutzung der Informationstechnik muss verhindert werden. Bei Abwesenheit sind Mitarbeiterräume mit Informationstechnologie verschlossen zu halten. Bei der Anordnung und baulichen Einrichtung der Geräte ist darauf zu achten, dass schützenswerte Daten nicht von Unbefugten eingesehen werden können. Beim Ausdrucken derartiger Daten muss das Entnehmen der Ausdrucke durch Unbefugte verhindert werden.

B.2 Registrierung und Sicherung mobiler Geräte

Verantwortlich für die Initiierung: IT-Beauftragter
Verantwortlich für die Umsetzung: IT-Anwender
Dienstliche mobile Geräte (Smartphones, Tabletts, Notebooks, usw.) sind in einer Liste zu erfassen und zu registrieren. Der Benutzer ist durch ein entsprechendes Informationsblatt über den Umgang mit dem mobilen Gerät zu informieren. Bei der Übergabe des mobilen Gerätes an den Nutzer hat der Nutzer die Kenntnisnahme und Einhaltung der Regeln durch Unterschrift anzuerkennen. Die mobilen Geräte sind durch geeignete Maßnahmen (Kennwort-Schutz, keine private Software, regelmäßige Updates, keine Verwendung von externen Cloud-Diensten, etc.) entsprechend zu schützen. Die hier genannten Regelungen (insbesondere zum Schutz durch Kennwörter, Verschlüsselung, usw.) sind entsprechend anzuwenden. Sofern die jeweilige Applikation eigene Schutzmechanismen anbietet (Verschlüsselung, Kennwörter, etc.) sind diese ebenfalls zu verwenden.
Bei der Speicherung von schützenswerten Daten auf mobilen Geräten (Smartphones, Tablets, Notebooks, usw.) sind besondere Vorkehrungen zum Schutz der Daten zu treffen. Schützenswerte Dateien müssen verschlüsselt werden.
Mobile Geräte sind möglichst verschlossen aufzubewahren. Auf Datensicherung ist besonders Wert zu legen.

C Hard- und Software

C.1 Kontrollierter Softwareeinsatz

Verantwortlich für die Initiierung: IT-Beauftragter
Verantwortlich für die Umsetzung: IT-Anwender
Auf Rechnersystemen der TU Clausthal darf zum Zweck des Schutzes von universitätseigener Hardware und dem Universitätsnetz nur Software installiert werden, die zur Erfüllung der dienstlichen Aufgaben erforderlich ist. Das eigenmächtige Einspielen ist nicht gestattet. Im Zweifelsfall ist die Zustimmung der Leitung der betreffenden Organisationseinheit und des Rechenzentrums einzuholen.

C.2 Keine private Hard- und Software

Verantwortlich für die Initiierung: IT-Beauftragter
Verantwortlich für die Umsetzung: IT-Anwender
Die Benutzung von privater Hard- und Software (Bring Your Own Device, BYOD) in Verbindung mit technischen Einrichtungen der TU Clausthal und deren Netzen ist grundsätzlich nicht gestattet. Die Leitung der betreffenden Organisationseinheit kann Ausnahmen in Abstimmung mit dem Rechenzentrum gestatten.
Allgemeine Ausnahmen gelten für den Einsatz von privaten Computern für Lehrveranstaltungen und Vorträge sowie in speziell gekennzeichneten Bereichen, wie zum Beispiel in Bibliotheken oder in Studierendenarbeitsbereichen, und im Funknetz eduroam.

C.3 Virenschutz

Verantwortlich für die Initiierung: IT-Beauftragter
Verantwortlich für die Umsetzung: IT-Personal, IT-Anwender
Auf allen Arbeitsplatzrechnern ist, soweit technisch möglich, ein aktueller Virenscanner einzurichten, der automatisch alle eingehenden und zu öffnenden Dateien überprüft. Damit soll bereits das Eindringen von schädlichen Programmen erkannt und verhindert werden.
Per E-Mail erhaltene Anhänge sind nur dann zu öffnen, wenn ihre Herkunft bekannt und Ungefährlichkeit wahrscheinlich ist.
Bei Verdacht auf Vireninfektion ist das zuständige IT-Personal zu informieren.

D Zugriffsschutz

D.1 Abmelden und ausschalten

Verantwortlich für die Initiierung: IT-Beauftragter
Verantwortlich für die Umsetzung: IT-Personal, IT-Anwender
Bei kürzerem Verlassen des Zimmers muss der Arbeitsplatzrechner und mobile Geräte (Notebooks, Tabletts, Smartphones, usw.) durch einen Kennwortschutz gesperrt werden. Grundsätzlich sind die Systeme nach Dienstschluss auszuschalten. Von diesen Regelungen kann nur abgewichen werden, soweit es die Arbeitsorganisation dringend erfordert und/oder andere Sicherheitsmaßnahmen es ermöglichen.

D.2 Personenbezogene Kennungen

Verantwortlich für die Initiierung: Bereichsleitung
Verantwortlich für die Umsetzung: Bereichsleitung
Alle Rechnersysteme sind so einzurichten, dass nur berechtigte Benutzer die Möglichkeit haben, mit ihnen zu arbeiten. Infolgedessen ist zunächst eine Anmeldung mit Benutzerkennung und einem Kennwort oder anderen eindeutigen Merkmalen erforderlich.
Die Vergabe von Benutzerkennungen für die Arbeit an IT-Systemen soll in der Regel personenbezogen erfolgen. In den Fällen, in denen kein personenbezogener Account möglich ist, ist ein

Funktions-Account einzurichten. Der Kreis der Nutzer solcher Funktions-Accounts ist unbedingt auf das Notwendigste zu beschränken und regelmäßig zu überprüfen.
Die Arbeit unter der Kennung einer anderen Person ist unzulässig. Dem Benutzer ist untersagt, Kennungen und Passwörter weiterzugeben.
Ausgenommen von dieser Regelung sind Systeme, die für allgemeine öffentliche Zugänge bestimmt sind (z. B. Kiosksysteme, Abfragestationen für Bibliothekskataloge).

D.3 Gebrauch von Passwörtern

Verantwortlich für die Initiierung: IT-Beauftragter
Verantwortlich für die Umsetzung: IT-Personal, IT-Anwender
Der Benutzer hat sein Passwort geheim zu halten. Idealerweise sollte das Passwort nicht notiert werden.
Empfehlungen zur Gestaltung der Passwörter sind in `https://tu-c.de/itsec` genannt und sollen in der Schulung intensiv behandelt werden.
Erhält ein Benutzer beim Anmelden mit seinem Passwort keinen Zugriff auf das System, besteht die Gefahr, dass sein Passwort durch Ausprobieren ermittelt werden sollte, um illegal Zugang zum System zu erhalten. Solche Vorfälle sind dem zuständigen Vorgesetzten und dem IT-Personal zu melden (Siehe A.2).
Vergisst ein Benutzer sein Passwort, hat er beim Administrator ohne vorheriges Ausprobieren das Zurücksetzen zu veranlassen. Diese Festlegung soll verhindern, dass der Vorgang als Eindringversuch protokolliert und behandelt wird.
Spezielle Regelungen und Hinweise für Zertifikate und Zertifikatsticks findet man auf der Seite `https://tu-c.de/itsec`.

D.4 Zugriffsrechte

Verantwortlich für die Initiierung: IT-Beauftragter
Verantwortlich für die Umsetzung: IT-Personal
Der Benutzer darf nur mit den Zugriffsrechten ausgestattet werden, die unmittelbar für die Erledigung seiner Aufgaben vorgesehen sind. Insbesondere sind alltägliche Arbeiten nicht mit privilegierten Benutzerkonten (Administrator, root o. a.) vorzunehmen.
Bei allen administrativen Anwendungen, die gesetzlichen Anforderungen genügen müssen (Datenschutz, Handelsgesetzbuch, u. a.) erfolgt die Vergabe bzw. Änderung der Zugriffsrechte für die einzelnen Benutzer auf schriftlichen Antrag.
In allen anderen Bereichen sind die dort geltenden Regelungen zu beachten.
Bei der Vergabe von Zugriffsrechten ist die Funktionstrennung zu beachten.

D.5 Netzzugänge

Verantwortlich für die Initiierung: IT-Beauftragter
Verantwortlich für die Umsetzung: IT-Personal, IT-Anwender
Der Anschluss von Systemen an das Datennetz der TU Clausthal hat ausschließlich über die dafür vorgesehene Infrastruktur zu erfolgen. Die eigenmächtige Einrichtung oder Benutzung von

zusätzlichen Verbindungen (Switches, Modems o. ä.) sowie die eigenmächtige Einbringung aktiver und passiver Netzwerkkomponenten ist unzulässig. Ausnahmen darf nur das Rechenzentrum in Absprache mit dem IT-Beauftragten des Bereichs und ggf. mit dem Datenschutzbeauftragten einrichten. Das Netz wird durch geeignete Maßnahmen geschützt, die nicht umgangen werden dürfen.

D.6 Telearbeit

Verantwortlich für die Initiierung: Bereichsleitung
Verantwortlich für die Umsetzung: IT-Personal, IT-Anwender
Bei der Telearbeit verlassen Daten den räumlich eingegrenzten Bereich der Datenverarbeitenden Stelle. Zur Einrichtung und zum Betrieb von Telearbeitsplätzen ist eine Dienstvereinbarung erforderlich. Dabei sind die Rahmenbedingungen jedes Einzelfalls zu berücksichtigen.

Der telearbeitende IT-Anwender hat die entsprechenden Vereinbarungen zum Schutz der bearbeiteten Daten und verwendeten System einzuhalten.

E Kommunikationssicherheit

E.1 Sichere Netzwerknutzung

Verantwortlich für die Initiierung: IT-Beauftragter
Verantwortlich für die Umsetzung: IT-Personal, IT-Anwender
Der Einsatz von verschlüsselten Kommunikationsdiensten ist, nach Möglichkeit, den unverschlüsselten Diensten vorzuziehen. Die Übertragung schützenswerter Daten muss verschlüsselt erfolgen oder durch andere geeignete Maßnahmen (z. B. isolierter eigener Netze) gesichert werden.

F Datensicherung

F.1 Datensicherung

Verantwortlich für die Initiierung: Verfahrensverantwortlicher
Verantwortlich für die Umsetzung: IT-Personal
Regelmäßig durchgeführte Datensicherungen sollen vor Verlust durch Fehlbedienung, technische Störungen o. ä. schützen. Grundsätzlich sind Daten auf zentralen Servern zu speichern. Ist die Speicherung auf zentralen Servern nicht möglich, ist der Benutzer für die Sicherung seiner Daten selbst verantwortlich.

Bei zentraler Datensicherung sollte sich der Nutzer über die in den jeweiligen Bereichen geltenden Regelungen zu Rhythmus und Verfahrensweise für die Datensicherung informieren.

G Datenträger

G.1 Umgang mit Datenträgern

Verantwortlich für die Initiierung: Verfahrensverantwortlicher
Verantwortlich für die Umsetzung: IT-Personal
Datenträger sind an gesicherten Orten aufzubewahren. Ggf. sind Datenträgertresore zu beschaffen. Weiterhin sind Datenträger zu kennzeichnen, falls die Identifikation des Datenträgers nicht durch ein anderes technisches Verfahren erfolgt. Datenträger müssen beim Transport vor Beschädigungen geschützt sein. Bei schützenswerten Daten ist eine Verschlüsselung erforderlich.

G.2 Physisches Löschen von Datenträgern

Verantwortlich für die Initiierung: Verfahrensverantwortlicher
Verantwortlich für die Umsetzung: IT-Personal, IT-Anwender
Datenträger mit schützenswerten Daten müssen vor einer Weitergabe an nicht autorisierte Personen physisch gelöscht werden. Das kann mit geeigneten Programmen oder mit einem Gerät zum magnetischen Durchflutungslöschen erfolgen.
Auszusondernde oder defekte Datenträger müssen, sofern sie schützenswerte Daten enthalten (oder enthalten haben), vollständig unlesbar gemacht werden. Weitere Informationen und Auskünfte zum Löschen von Datenträgern geben: RZ (Helpdesk), die Universitätsverwaltung sowie die Datenschutzbeauftragten der Universität.

H Schützenswerte Daten

H.1 Schützenswerte Daten auf dem Arbeitsplatzrechner

Verantwortlich für die Initiierung: Verfahrensverantwortlicher
Verantwortlich für die Umsetzung: IT-Personal, IT-Anwender
Das Speichern schützenswerter Daten auf der Festplatte des Arbeitsplatzrechners oder anderer lokaler Speicher- oder Übertragungsmedien und deren Übertragung ist nur zulässig, wenn die für den jeweiligen Schutzbedarf (die für die jeweilige Schutzstufe) erforderlichen Sicherheitsmaßnahmen getroffen wurden (s. z. B. § 9 Bundesdatenschutzgesetz, Grundschutzhandbuch des BSI, Hinweise des/der Datenschutzbeauftragten).

H.2 Speicherung in einer Cloud

Verantwortlich für die Initiierung: Verfahrensverantwortlicher
Verantwortlich für die Umsetzung: IT-Personal, IT-Anwender
Für die Speicherung, insbesondere von schützenswerten Daten, in der Cloud sind besondere Regelungen zu beachten, die auf der Webseite `https://tu-c.de/itsec` detailliert beschrieben sind. Ebenso sind dort die Fristen und Regelungen für die Löschung der Daten hinterlegt.