TUBAF

Die Ressourcenuniversität.
Seit 1765.

INFORMATIONSSICHERHEITS-LEITLINIE

DER TU BERGAKADEMIE FREIBERG

Inhaltsverzeichnis

Präambel

Die TU Bergakademie Freiberg ist die deutsche Ressourcenuniversität. Forschung, Lehre und Transfer widmen sich der nachhaltigen, sicheren und verantwortungsvollen Nutzung natürlicher Ressourcen sowie den globalen Herausforderungen des 21. Jahrhunderts. Als Universität übernehmen wir Verantwortung für eine nachhaltige Entwicklung und für den Schutz der Werte, die unser Leitbild prägen.

Eine verlässliche, sichere und verfügbare Informations- und Kommunikationstechnik ist heute Grundvoraussetzung für wissenschaftliche Arbeit, innovative Lehrformate und effiziente Verwaltungsprozesse. Informationssicherheit schützt Forschungsdaten, Lehrmaterialien, personenbezogene Informationen und die technischen Systeme, die den universitären Betrieb ermöglichen. Sie besitzt daher einen hohen strategischen Stellenwert und trägt wesentlich zur Leistungsfähigkeit und Zukunftsfähigkeit der Universität bei. Ihre erfolgreiche Umsetzung erfordert die Mitwirkung aller Mitglieder und Angehörigen der Universität.

I. Zielsetzung der Leitlinie

Diese Leitlinie definiert die grundlegenden Prinzipien und die strategische Ausrichtung der Informationssicherheit an der TU Bergakademie Freiberg. Sie schafft ein gemeinsames Verständnis über Bedeutung und Ziele der Informationssicherheit und bildet die verbindliche Grundlage für den Aufbau und Betrieb des Informationssicherheitsmanagementsystems (ISMS).

II. Geltungsbereich

Diese Leitlinie ist verbindlich für

- alle Organisationseinheiten, Mitglieder und Angehörigen der Universität,
- die gesamte von der Universität verantwortete IT-Infrastruktur, einschließlich zentral und dezentral betriebener IT-Systeme,
- alle extern betriebenen oder beauftragten Systeme, soweit sie Informationen oder IT-Dienste der Universität verarbeiten oder bereitstellen,
- sämtliche Informationen, unabhängig von Form, Medium oder Speicherort, sowie die Prozesse, in denen diese Informationen verarbeitet werden.

Die Festlegungen dieser Leitlinie und der daraus abgeleiteten Richtlinien sind weiterhin bei Vereinbarungen und Verträgen mit An-Instituten, außeruniversitären Einrichtungen und weiteren Dritten, die Informationen oder IT-Systeme der Universität nutzen oder verarbeiten, verbindlich einzuhalten.

III. Sicherheitsziele

Die Universität stellt sicher, dass Vertraulichkeit, Integrität und Verfügbarkeit aller Informationen, IT-Systeme und Dienste jederzeit angemessen gewährleistet sind. Auf dieser Grundlage gelten die folgenden Sicherheitsziele:

- Schutz der Informations- und IT-Infrastruktur sowie aller verarbeiteten Daten vor unbefugtem Zugriff, Missbrauch, Manipulation und Sabotage.
- Aufrechterhaltung eines robusten und verlässlichen Informationssicherheitsniveaus für Lehr-, Forschungs- und Verwaltungsprozesse.
- Bereitstellung sicherer, zuverlässiger und vertrauenswürdiger Online-Dienste für interne und externe Nutzergruppen.

- Einhaltung aller gesetzlichen und regulatorischen Anforderungen, insbesondere im Bereich Datenschutz, sowie angemessener Schutz personenbezogener Daten in allen universitären Abläufen.
- Reduzierung von Informationssicherheitsvorfällen und Begrenzung möglicher Schäden für die Universität, ihre Mitglieder, Angehörigen und ihre Partner.

IV. Sicherheitsstrategie

Das Ziel der Informationssicherheitsstrategie der Universität ist ein systematisches, nachhaltiges und risikoorientiertes Vorgehen, das ein angemessenes Schutzniveau für alle Informationen, IT-Systeme und Prozesse gewährleistet und zugleich die besonderen Anforderungen von Forschung, Lehre und Verwaltung berücksichtigt.

Zur Umsetzung dieser Strategie gelten folgende Grundsätze:

- Die Universität etabliert und betreibt ein ISMS in Anlehnung an die IT-Grundschutz-Methodik des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Es bildet den organisatorischen Rahmen für Planung, Umsetzung, Überwachung und kontinuierliche Verbesserung der Informationssicherheit.
- Sicherheitsmaßnahmen werden auf Grundlage systematischer Risikoanalysen ausgewählt und umgesetzt. Dabei wird ein angemessenes Verhältnis zwischen Schutzbedarf, wissenschaftlicher Freiheit, Innovationsfähigkeit und wirtschaftlicher Vertretbarkeit gewahrt.
- Die Universität gestaltet Sicherheitsmaßnahmen so, dass sie Forschung und Lehre unterstützen und nicht unverhältnismäßig einschränken. Offene Forschungsumgebungen, internationale Kooperationen und experimentelle IT-Infrastrukturen werden durch risikoorientierte und flexible Schutzmechanismen abgesichert.
- Informationssicherheit ist integraler Bestandteil aller Abläufe der Universität. Sicherheitsanforderungen werden frühzeitig berücksichtigt und in Forschung, Lehre, Verwaltung und technische Betriebsprozesse eingebettet.
- Informationssicherheit wird als fortlaufender Prozess verstanden. Das ISMS wird regelmäßig überprüft, bewertet und weiterentwickelt, um auf neue Bedrohungen, technologische Entwicklungen und organisatorische Veränderungen reagieren zu können.
- Alle Mitglieder und Angehörigen der Universität werden regelmäßig über Risiken, Verhaltensregeln und Sicherheitsmaßnahmen informiert und geschult.
- Die Universität fördert den Austausch zwischen Fachbereichen, zentralen Einrichtungen und externen Partnern, um Sicherheitsanforderungen, Risiken und Maßnahmen transparent und koordiniert zu behandeln.

V. Organisationsstruktur und Verantwortlichkeiten

Die Gesamtverantwortung für die Informationssicherheit an der Universität liegt bei der Universitätsleitung. Sie nimmt die Rolle der Leitungsebene im Sinne der BSI-Standards wahr und stellt die erforderlichen organisatorischen und personellen Ressourcen für den Betrieb, die Weiterentwicklung und kontinuierliche Verbesserung des ISMS bereit.

Die nachfolgend beschriebenen Gremien und Funktionstragenden wirken arbeitsteilig zusammen, um ein angemessenes Schutzniveau für Informationen, IT-Systeme und Prozesse der Universität sicherzustellen.

Der **Informationssicherheitsbeauftragte (ISB)** ist die zentrale Ansprechperson für Informationssicherheit und in seiner Funktion nicht weisungsgebunden. Er koordiniert den Sicherheitsprozess, berät die Universitätsleitung und Organisationseinheiten, überwacht die Umsetzung von Sicherheitsmaßnahmen und bewertet sicherheitsrelevante Vorfälle. Der ISB hat das Recht auf Auskunft und erhält Zugang zu allen für die Erfüllung seiner Aufgaben erforderlichen Informationen in sämtlichen Bereichen der Universität. Er kann Maßnahmen und Anordnungen treffen, die zur Gefahrenabwehr oder Wahrung der Informationssicherheit notwendig sind.

Die **Stabsstelle Informationssicherheit** steuert das ISMS der Universität und unterstützt die Universitätsleitung bei der strategischen Weiterentwicklung der Informationssicherheit. Unter der Leitung des ISB koordiniert sie zentrale Maßnahmen und Schulungen, erstellt und pflegt Richtlinien und sorgt für einen geregelten Informationsfluss zwischen den beteiligten Einheiten.

Das **Universitätsrechenzentrum (URZ)** verantwortet den sicheren Betrieb der zentralen IT-Infrastruktur und setzt technische Sicherheitsmaßnahmen um. Es bindet den ISB frühzeitig in IT-Projekte ein und unterstützt gemeinsam mit den für die **dezentrale Administration** verantwortlichen Personen die Stabsstelle Informationssicherheit bei der Umsetzung des ISMS.

Die **Rektoratskommission Forschung** ist das strategische Entscheidungsgremium für Informationssicherheit. Sie verabschiedet grundlegende Richtlinien zur Informationssicherheit und unterstützt die Universitätsleitung bei der Priorisierung sicherheitsrelevanter Maßnahmen. Sie lädt zu Themen der Informationssicherheit und zur Verabschiedung entsprechender Richtlinien den ISB als stimmberechtigtes Mitglied und Moderator des betreffenden Tagesordnungspunkts zur Sitzung ein.

Der **Datenschutzbeauftragte** überwacht die Einhaltung datenschutzrechtlicher Vorgaben und arbeitet eng mit dem ISB zusammen, insbesondere bei Maßnahmen, die sowohl Datenschutz als auch Informationssicherheit betreffen.

Mitglieder und Angehörige der Universität tragen Verantwortung für den bestimmungsgemäßen und sachgerechten Umgang mit den von ihnen genutzten Daten und IT-Systemen. Sie sind im Rahmen der ihnen übertragenen Aufgaben für die Umsetzung der Maßnahmen zur Informationssicherheit verantwortlich. Bei der Einführung neuer und Änderung bestehender Verfahren sind der ISB und DSB frühzeitig zu beteiligen.

Die genannten Einheiten wirken koordiniert zusammen, um die Informationssicherheitsstandards der Universität einzuhalten und weiterzuentwickeln.

VI. Inkrafttreten

Die Informationssicherheitsleitlinie tritt am Tag nach ihrer Veröffentlichung in Kraft.

Freiberg, den 27.04.2026

Prof. Dr. Jutta Emes
Rektorin

Jens Then
Kanzler