TECHNISCHE UNIVERSITÄT WIEN






Informationssicherheits-organisation der TU Wien

(online 09.07.2020)

Richtlinie des Rektorates, Beschluss vom 30.06.2020

Verlautbarung im Mitteilungsblatt Nr. 27/2020 vom 09.07.2020 (lfd. Nr.268)

GZ: 30002.04/008/2020

INHALT

PRÄAMBEL

Dieses Dokument beschreibt die Organisation der TU Wien in Bezug auf Informationssicherheit und definiert entsprechende Rollen und Aufgaben innerhalb der Informationssicherheitsorganisation der TU Wien. Die Rollen und Aufgaben stellen in der beschriebenen Form Mindestanforderungen dar und werden bei Bedarf angepasst oder erweitert.

Dieses Dokument adressiert alle Angehörigen der TU Wien gem. § 94 UG. Darüber hinaus gelten die enthaltenen organisatorischen Regelungen ohne zeitliche und örtliche Einschränkungen.

1 AUFBAU DER INFORMATIONSSICHERHEITS-ORGANISATION DER TU WIEN

Die Informationssicherheitsorganisation stellt sicher, dass zur Erfüllung der Anforderung eines Informationssicherheitsmanagementsystems (ISMS) entsprechende Verantwortlichkeiten, Dokumentationsgrundlagen sowie Rollen, Aufgaben und Kompetenzen festgelegt werden (Anmerkung: analog zur Datenschutzorganisation der TU Wien). Eine Person kann dabei mehrere Rollen innehaben, wie auch eine Rolle gegebenenfalls auf mehrere Personen aufgeteilt werden kann. Die Informationssicherheitsorganisation umfasst alle Rektoratsressorts und Fakultäten.

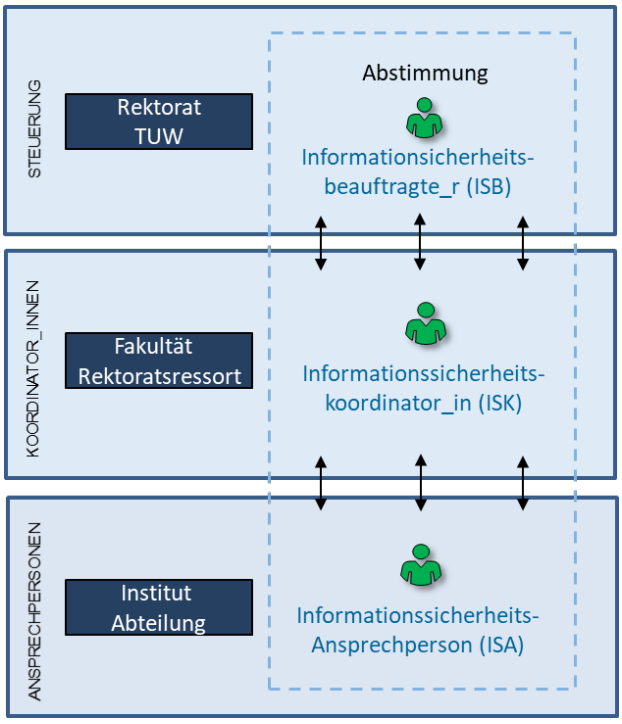

Abb. 1 Informationssicherheitsorganisation der TU Wien

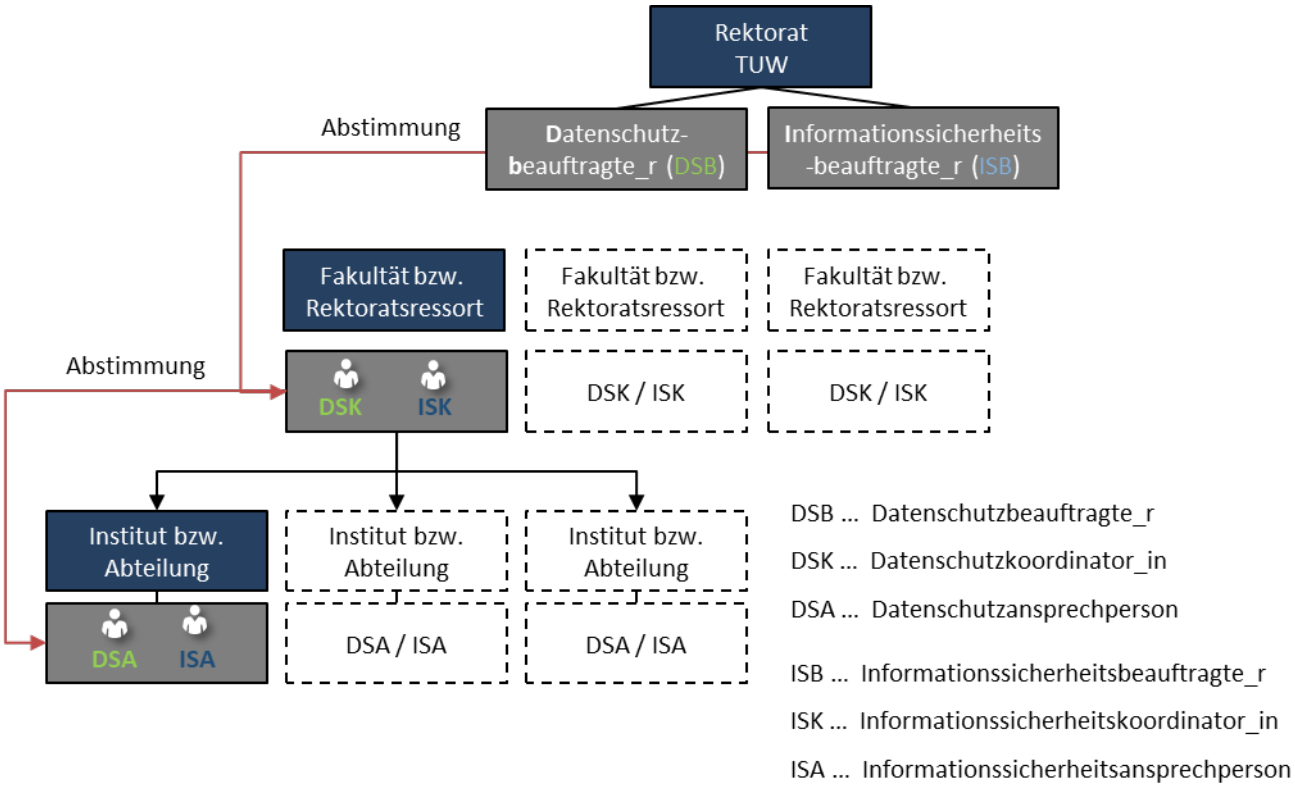

Abb. 2 Informations- und Datenschutzorganisation der TU Wien

2 ROLLEN IN DER INFORMATIONSSICHERHEITS-ORGANISATION DER TU WIEN

2.1 REKTORAT

Die Verantwortung für die Einhaltung der universitätsinternen Informationssicherheitsvorschriften liegt beim Rektorat der TU Wien. Die Informationssicherheitsorganisation unterstützt das Rektorat in der Wahrnehmung seiner Verantwortung und übernimmt die operative Abwicklung der informationssicherheitsrelevanten Aufgaben.

Aufgaben:

- Strategische Entwicklung der Informationssicherheit an der TU Wien;
- Bestellung des_der Informationssicherheitsbeauftragten durch das lt. Geschäftsordnung zuständige Rektoratsmitglied;
- Bestellung der Informationssicherheitskoordinator_innen (ISK) durch das lt. Geschäftsordnung zuständige Rektoratsmitglied;
- Sicherstellung personeller und finanzieller Ressourcen für Informationssicherheit;
- Verabschiedung von Informationssicherheitsrichtlinien und anderen einschlägigen Dokumenten;

- Beschluss und Umsetzung von Maßnahmen auf Universitätsebene (z.B. resultierend aus Überprüfungen / Audits);
- Förderung des Bewusstseins für Informationssicherheit bei allen Angehörigen der TU Wien;
- Behandlung der von dem_der Informationssicherheitsbeauftragten eingebrachten informationssicherheitsrelevanten Themen.

2.2 INFORMATIONSSICHERHEITSBEAUFTRAGTE_R

Im Rahmen der Informationssicherheitsorganisation der TU Wien ist die Bestellung eines_einer Informationssicherheitsbeauftragten (ISB) vorgesehen. Diese_r ist organisatorisch dem lt. Geschäftsordnung zuständigen Rektoratsmitglied zugeordnet und berichtet diesem direkt.

Aufgaben

- Strategische Planung und Entwicklung von Konzepten, Standards und Richtlinien für die Informationssicherheit an der TU Wien;
- Etablierung und Betrieb eines Managementsystems für Informationssicherheit (ISMS);
- Identifizierung aller sicherheitsrelevanten Prozesse der gesamten TU Wien und Festlegung des Geltungsbereiches der sicherheitsrelevanten Maßnahmen;
- Unmittelbare Berichterstattung an das lt. Geschäftsordnung zuständige Rektoratsmitglied (direkter Berichtsweg); in diesem Zusammenhang mindestens einmal jährlich Erstellung eines zusammenfassenden Berichts für das Rektorat betreffend des Themas Informationssicherheit aus dem vorhergehenden Geschäftsjahr sowie der geplanten Aktivitäten zur Informationssicherheit in Abstimmung mit den jeweiligen Informationssicherheitskoordinator_innen;
- Etablierung eines operationellen Risikomanagements innerhalb der TU Wien;
- Unterstützung der Informationssicherheitskoordinator_innen bei der Wahrnehmung ihrer Rolle und bei der Einhaltung der Informationssicherheitsrichtlinien der TU Wien;
- Durchführung von regelmäßigen Schulungen zum Thema Informationssicherheit an der TU Wien entsprechend der Anforderungen der jeweiligen Mitarbeiter_innengruppe;
- Verantwortliche Erstellung, Aktualisierung und Kommunikation von Regelungen im Bereich Informationssicherheit, die verpflichtend von allen Angehörigen der TU Wien gem. § 94 UG anzuwenden sind (zB Informationssicherheits-Governance, Informationssicherheits-Organisationshandbuch, Informationssicherheits-Richtlinie(n), Informationssicherheits-Prozessbeschreibungen, etc.);
- Durchführung von Überprüfungen (Supervision);
- Im Bedarfsfall Einbringen von informationssicherheitsrelevanten Themen als Tagesordnungspunkt in die wöchentlichen Sitzungen des Rektorats im Wege des lt. Geschäftsordnung zuständigen Rektoratsmitglieds;

- Identifikation von Verbesserungsmaßnahmen auf Basis der Informationssicherheits-audits;
- Abhaltung regelmäßiger Jour fixe mit den Informationssicherheitskoordinator_innen, v.a. zur Sicherstellung, dass Informationssicherheits-Aktivitäten, -Prozesse, -Richtlinien und -Methoden in allgemeiner Übereinstimmung akzeptiert werden;
- Sensibilisierung und Bewusstseinsbildung;
- Bekanntmachung der Inhalte der Informationssicherheitsrichtlinie(n) und -regelungen.

Der_die Informationssicherheitsbeauftragte ist bei allen größeren Projekten sowie bei der Einführung neuer Anwendungen und IT-Systeme zu informieren.

2.3 INFORMATIONSSICHERHEITSKOORDINATOR_IN

Die Informationssicherheitskoordinator_innen (ISK) sind Kontaktpersonen für alle informationssicherheitsbezogenen Themen der zugeordneten Fakultäten und der zugeordneten Rektoratsressorts.

Aufgaben

- Erste_r Ansprechpartner_in im zugeordneten Bereich für Informationssicherheitsfragestellungen;
- Beratung und Unterstützung der Mitarbeiter_innen in den Fakultäten bzw. Rektoratsressorts;
- Verantwortlich für die Verbreitung und Unterstützung bei der Umsetzung der Informationssicherheitsvorgaben in ihren Fakultäten bzw. Rektoratsressorts sowie teamübergreifende Forcierung der jeweiligen Informationssicherheitsprozesse zur Erhöhung der Effektivität;
- Anlassbezogene Berichterstattung direkt an den_die jeweils zuständige_n Dekan_in bzw. das jeweils zuständige Rektoratsmitglied (direkter Berichtsweg) und zusätzlich im Rahmen der Informationssicherheitsorganisation an den_die Informationssicherheits-beauftragte_n;
- Sensibilisierung der in ihrer Fakultät bzw. ihrem Rektoratsressort tätigen Mitarbeiter_innen;
- Bekanntmachung der Inhalte der Informationssicherheitsrichtlinie(n) und -regelungen;
- Unterstützung des_der Informationssicherheitsbeauftragten bei der Erfüllung seiner_ihrer Tätigkeiten;
- Erfüllung und Überwachung der Vorgaben in Bezug auf Informationssicherheit im zugeordneten Bereich.

2.4 INFORMATIONSSICHERHEITSANSPRECHPERSON

Die Informationssicherheitsansprechpersonen sind erste Anlaufstelle für Fragen in Zusammenhang mit Informationssicherheit an einem Institut bzw. in einer Abteilung. Die Einrichtung dieser Rolle an Instituten ist nicht verpflichtend, wird aber empfohlen. In den

Abteilungen ist diese Rolle jedenfalls einzurichten. Eine Informationssicherheitsansprechperson kann dabei mehrere Abteilungen betreuen. Der_die Instituts- bzw. Abteilungsleiter_in kann diese Aufgabe selbst übernehmen oder seine_ihre diesbezüglichen Aufgaben an eine andere Person des Instituts bzw. der Abteilung übertragen, sofern diese Person der Übertragung zustimmt. Die Informationssicherheitsansprechpersonen unterstützen den_die Informationssicherheitsbeauftragte_n und den_die Informationssicherheitskoordinator_in bei der Umsetzung und Einhaltung der Informationssicherheitsrichtlinien der TU Wien und sind dazu angehalten, auf Verstöße gegen die Informationssicherheit hinzuweisen.

Aufgaben

- Verantwortlich für die Verbreitung und Unterstützung bei der Umsetzung der Informationssicherheitsvorgaben in ihren Instituten bzw. Abteilungen sowie teamübergreifende Forcierung der jeweiligen Informationssicherheitsprozesse zur Erhöhung der Effektivität;
- Anlassbezogene Berichterstattung direkt an den_die jeweils zuständige_n Instituts- bzw. Abteilungsleiter_in (direkter Berichtsweg) und zusätzlich im Rahmen der Informationssicherheitsorganisation an den_die zuständige_n Informationssicherheitskoordinator_in;
- Sensibilisierung der in ihrem Institut bzw. ihrer Abteilung tätigen Mitarbeiter_innen;
- Bekanntmachung der Inhalte der Informationssicherheitsrichtlinie(n) und -regelungen, insbesondere den mit vertrauenswürdigen Informationen arbeitenden Mitarbeiter_innen;
- Unterstützung des_der zuständige_n Informationssicherheitskoordinator_in und des_der Informationssicherheitsbeauftragten bei der Erfüllung seiner_ihrer Tätigkeiten;
- Erfüllung und Überwachung der Vorgaben hinsichtlich Informationssicherheit im zugeordneten Institut bzw. Abteilung.

3 FACHLICHE SCHNITTSTELLEN

3.1 INFORMATIONSEIGENTÜMER_INNEN

Die Informationseigentümer_innen sind für die ordnungsgemäße Umsetzung der Informationssicherheitsanforderungen verantwortlich. Informationseigentümer_innen sind jene Personen, die über die Verarbeitung von Informationen entscheiden.

Aufgaben

- Autorisierung von Zugriffsrechten und regelmäßige Überprüfung der Zugriffsrechte, Definition von Benutzungsregeln in Abstimmung mit dem_der Informationssicherheitsbeauftragten;

- Klassifizierung der in ihrem_seinem Verantwortungsbereich liegenden Daten und Informationen (z.B. in Bezug auf Vertraulichkeit, Verfügbarkeit, Integrität, Nachvollziehbarkeit);
- Identifizierung und Behandlung von Informationssicherheitsrisiken;
- Spezifizierung von Sicherheitsanforderungen zum Schutz von Informationen;
- Überwachung der Maßnahmenumsetzung;
- Unterstützung des_der Informationssicherheitsbeauftragten bei der Erfüllung seiner_ihrer Tätigkeiten.
- Unverzügliches Melden von kritischen Schwachstellen und Informationssicherheitsvorfällen an den_die Informationssicherheitsbeauftragte_n.

3.2 IT UND IT-SICHERHEIT

Die TU.it ist in der Rolle des Fachexperten operativer Hauptkontakt für den_die Informationssicherheitsbeauftragte_n für fachliche Themen der IT-Sicherheit und die Gewährleistung der Sicherheitsanforderungen aus der Informationssicherheit. Aus diesem Grund muss ein regelmäßiger Informationsaustausch stattfinden.

Aufgaben der TU.it

- Koordination der erforderlichen IT-Sicherheitsmaßnahmen für alle von der TU.it angebotenen IT-Services;
- Entwicklung von TU.it-internen Prozessen und Konzepten bezüglich Informationssicherheit auf Basis von Informationssicherheitsanforderungen;
- Entwicklung, Implementierung, Dokumentation und Überwachung von detaillierten Realisierungsplänen für Informationssicherheitsmaßnahmen;
- Unterstützung der TU-Mitarbeiter_innen durch technische Hilfestellungen, Aufklärungen und Empfehlungen bei den von der TU.it angebotenen IT-Services;
- Unterstützung des_der Informationssicherheitsbeauftragte_n bei der Durchführung seiner_ihrer Tätigkeiten, insbesondere bei Informationssicherheitsvorfällen, Supervision und Audits;
- Unverzügliches Melden von kritischen Schwachstellen und Informationssicherheitsvorfällen an den_die Informationssicherheitsbeauftragte_n.

Dezentrale IT-Kontaktpersonen[1] haben in ihrem unmittelbaren Wirkungskreis folgende Aufgaben:

- Umsetzung und Kontrolle der Effektivität der (vorgesehenen) IT-Sicherheitsmaßnahmen im laufenden Betrieb;

[1] Die Personengruppe der IT-Kontaktpersonen (Rolle in TISS) ist seit vielen Jahren Hauptansprechpartner der TU.it in den Instituten und Abteilungen.

- Umsetzung und Kontrolle der Effektivität von (vorgesehenen) Informationssicherheitsmaßnahmen im laufenden Betrieb;
- Sensibilisierung und Bewusstseinsbildung;
- Unverzügliches Melden von kritischen Schwachstellen und Informationssicherheitsvorfällen an den_die Informationssicherheitsbeauftragte_n;
- Einbringen von Praxisanregungen.

3.3 PERSONALADMINISTRATION

Die Personaladministration ist in der Rolle der Fachexpertin verantwortlich für die Implementierung und das Management von mitarbeiter_innenbezogenen Informationssicherheitsrichtlinien und -maßnahmen.

Aufgaben

- Dokumentation von Informationspflichten bzw. Zustimmungserklärungen betreffend Mitarbeiter_innen der TU Wien;
- Adaptierung von Betriebsvereinbarungen im Hinblick auf die geltenden Informationssicherheitsbestimmungen;
- Unterstützung des_der Informationssicherheitsbeauftragte_n bei der Durchführung seiner_ihrer Tätigkeiten.

3.4 STUDIENABTEILUNG, CONTINUING EDUCATION CENTER, DEKANATE

Die Studienabteilung, das Continuing Education Center sowie die Dekanate sind in der Rolle der Fachexpert_innen verantwortlich für die Implementierung und das Management von studierendenbezogenen Informationssicherheitsrichtlinien und -maßnahmen.

Aufgaben

- Dokumentation von informationssicherheitsrelevanten Informationspflichten bzw. Zustimmungserklärungen betreffend Studierende der TU Wien;
- Adaptierung von studienrechtlichen Informationen im Hinblick auf die geltenden Informationssicherheitsrichtlinien;
- Unterstützung des_der Informationssicherheitsbeauftragte_n bei der Durchführung seiner_ihrer Tätigkeiten.

3.5 SECURITY

Der Fachgruppe Objektschutz und Brandschutz der Abteilung Gebäude und Technik ist in der Rolle als Fachexperte verantwortlich für die Implementierung und das Management von Informationssicherheitsrichtlinien und -maßnahmen bezogen auf die Infrastrukturbereiche der TU Wien.

Aufgaben

- Entwicklung, Implementierung, Dokumentation und Überwachung der informationssicherheitsrelevanten Maßnahmen zu Gebäudeschutz und Zutrittssystemen, Arbeitnehmer_innenschutz inkl. Arbeitsmedizin, Reinigung, Veranstaltungen, Wartung und Instandhaltung, Immobilienmanagement sowie Vergabe;
- Unterstützung des_der Informationssicherheitsbeauftragte_n bei der Durchführung seiner_ihrer Tätigkeiten.

3.6 INTERNE REVISION

Die Abteilung Interne Revision hat die Verantwortung, die Informationssicherheitsprozesse und -maßnahmen auf Einhaltung gemäß den Regelungen in internen Richtlinien, externen Anforderungen und Industriestandards zu prüfen. Des Weiteren müssen Effizienz und Effektivität dieser Prozesse durch Prüfungen sichergestellt werden.

4 INFORMATIONSSICHERHEIT DURCH DIE ANGEHÖRIGEN DER TU WIEN

4.1 UNMITTELBARE_R VORGESETZTE_R

Der_die unmittelbare Vorgesetzte wirkt als Vorbild und Multiplikator_in in Informationssicherheitsthemen der TU Wien.

Aufgaben

- Unterstützung seiner_ihrer Mitarbeiter_innen in Themen der Informationssicherheit;
- Sensibilisierung und Bewusstseinsbildung;
- Vorbildwirkung für seine_ihre Mitarbeiter_innen.

4.2 PROJEKTLEITER_IN

Der_die Projektleiter_in ist für die Einhaltung der Informationssicherheit in jenen Projekten verantwortlich, die von ihm_ihr geleitet werden. Dies gilt für sämtliche Projekte an der TU Wien, nicht ausschließlich für Forschungsprojekte.

Aufgaben

- Identifizierung von Informationssicherheitsrelevanz in Projekten;
- Identifizierung von Informationssicherheitsrisiken in Projekten;
- Information des_der zuständigen Informationssicherheitskoordinator_in über Angelegenheiten betreffend Informationssicherheit in Projekten;
- Planung von Informationssicherheitsmaßnahmen und Risikobehandlung für Projekte, in denen vertrauliche Informationen verarbeitet werden;

- Abstimmung zu identifizierten Risiken, notwendigen Maßnahmen und benötigten Ressourcen mit den Dateneigentümer_innen oder mit dem_der zuständigen Informationssicherheitskoordinator_in;
- Unverzügliches Melden von Schwachstellen und Informationssicherheitsvorfällen in Projekten an den_die zuständige_n Informationssicherheitskoordinator_in;
- Überwachung der Einhaltung von Informationssicherheitsrichtlinien und -verfahren im Projektumfeld;
- Sicherstellung der Berücksichtigung informationssicherheitsbezogener Aspekte in Projekten.

4.3 ALLE ANGEHÖRIGEN DER TU WIEN

Aufgaben

- Einhaltung und Umsetzung der Informationssicherheitsrichtlinien und -maßnahmen;
- Bekanntgabe von möglichen Risiken;
- Einbringen von Verbesserungsvorschlägen;
- Meldung von sicherheitsrelevanten Vorkommnissen und Sicherheitsmängeln.