Weisung «Informationssicherheit an der ETH Zürich» RSETHZ 203.25

vom 17. Dezember 2024

Die Schulleitung der ETH Zürich,

gestützt auf Art. 4 Abs. 1 Bst. b der Verordnung über die Organisation der Eidgenössischen Technischen Hochschule Zürich vom 21. November 2024[1],

v e r o r d n e t:

1. Abschnitt: Allgemeine Bestimmungen

Artikel 1 Gegenstand

[1] Diese Weisung regelt die Ziele und Anforderungen an die Informationssicherheit. Sie definiert die Aufgaben, Verantwortlichkeiten und Kompetenzen sowie die übergeordnete Steuerung der Informationssicherheit.

Artikel 2 Geltungsbereich

[1] Diese Weisung gilt für alle Einheiten der ETH Zürich gemäss Verordnung über die Organisation der Eidgenössischen Technischen Hochschule Zürich vom 21. November 2024 (*Organisationsverordnung ETH Zürich*)[2] und deren Angehörige, namentlich für die

a. Zentralen Organe;

b. Departemente und deren Institute, Zentren, Laboratorien und Professuren und

c. Einheiten ausserhalb der Departemente gemäss Art. 92 Organisationsverordnung ETH Zürich, die allein von der ETH Zürich betrieben werden.

[2] Für Einheiten ausserhalb der Departemente, die gemeinsam mit anderen Hochschulen betrieben werden, sind individuelle Regelungen zu treffen.

[1] RSETHZ 201.021
[2] RSETHZ 201.021

2. Abschnitt: Ziele und Anforderungen

Artikel 3 Ziele

[1] Informationssicherheit gewährleistet die Vertraulichkeit, Integrität (Richtigkeit sowie Vollständigkeit) und Verfügbarkeit von Informationen. Die Informationssicherheitsstrategie unterstützt dabei bestmöglich die Umsetzung der Strategie der ETH Zürich. IT-Sicherheit ist Teil der Informationssicherheit und bedeutet die Gewährleistung der Informationssicherheit beim Einsatz von IT-Mitteln. IT-Mittel sind alle IT-Geräte und IT-Dienste, welche im Eigentum oder im Auftrag der ETH Zürich eingesetzt werden. Dies beinhaltet auch Drucker, Scanner, Software, Telefonie sowie Haustechniksysteme, Gebäudeautomation und ausgelagerte Dienstleistungen wie externe Cloud-Dienste. Ausgenommen ist die Videoüberwachung gemäss Art. 36i ETH-Gesetz.

[2] Der/Die Chief Information Security Officer (CISO) ist zuständig für die Informationssicherheit an der ETH Zürich. Die Organisationseinheiten setzen die Ziele und die Informationssicherheitsstrategie eigenverantwortlich und nach den Vorgaben und Empfehlungen der/des CISO um.

Artikel 4 Anforderungen

[1] Bei der Umsetzung von Informationssicherheit hält die ETH Zürich die rechtlichen Anforderungen ein und orientiert sich an den in der Fachwelt bewährten Standards und Normen.

Sie orientiert sich dabei an den folgenden Anforderungen:

a. Informationssicherheitsrichtlinien sind festgelegt, von der zuständigen Leitung genehmigt, herausgegeben, periodisch überprüft und werden bei Bedarf überarbeitet und den ETH-Angehörigen sowie relevanten externen Parteien bekanntgemacht;

b. Ein Rahmenwerk[3] und Managementsystem, mit welchem die Umsetzung der Informationssicherheit in der ETH Zürich eingeleitet und gesteuert und rapportiert werden kann, ist eingerichtet;

c. ETH Angehörige, Forschungspartnerinnen und -partner und Auftragnehmerinnen und -nehmer verstehen ihre Verantwortlichkeiten bezüglich Informationssicherheit und kommen diesen nach (Awareness). Bei Bedarf werden Sicherheitsüberprüfungen durchgeführt. Der Schutz bezüglich der Interessen der Informationssicherheit der ETH Zürich ist bei Beginn, bei der Änderung oder Beendigung einer Beschäftigung, Forschungskooperation oder eines Studiums zu berücksichtigen;

d. Die ETH Zürich inventarisiert und klassifiziert die in ihrem Auftrag erhobenen und bearbeiteten Informationen. Sie definiert die Zuständigkeiten und Verantwortlichkeiten für die genutzten Arbeitsmittel und unterbindet die unerlaubte Offenlegung, Veränderung, Entfernung oder Zerstörung von Informationen;

e. Der Zugriff auf Informationen und informationsverarbeitende Einrichtungen wird auf Zugriffs- oder Zugangsberechtigte eingeschränkt. Benutzerinnen und Benutzer sind für den Schutz ihrer Authentisierungsinformation verantwortlich;

f. Der angemessene und wirksame Gebrauch von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Informationen ist sichergestellt;

[3] Für eine graphische Darstellung siehe Anhang «Rahmenwerk der Informationssicherheit»

g. Der unbefugte Zutritt zu informationsverarbeitenden Einrichtungen sowie die Beschädigung und Beeinträchtigung von Informationen werden verhindert. Der Verlust, die Beschädigung, der Diebstahl oder die Gefährdung von Werten und die Unterbrechung von Organisationstätigkeiten sind unterbunden;

h. Der ordnungsgemässe und sichere Betrieb von informationsverarbeitenden Einrichtungen ist sichergestellt und vor Schadsoftware geschützt. Informationsbestände sind vor Verlust geschützt und die Integrität von Systemen im Betrieb ist sichergestellt. Ereignisse sind aufgezeichnet und Nachweise erzeugt. Die Ausnutzung technischer Schwachstellen ist verhindert. Die Auswirkung von Audittätigkeiten auf Systeme im Betrieb ist minimiert;

i. Informationen in Netzwerken und in den unterstützenden informationsverarbeitenden Einrichtungen sind geschützt und werden sowohl innerhalb der ETH Zürich als auch im Umgang mit jeglichen externen Stellen sicher übertragen;

j. Informationssicherheit ist ein fester Bestandteil über den gesamten Lebenszyklus von Informationssystemen und wird im Entwicklungszyklus von Informationssystemen geplant und umgesetzt. Der Schutz von Informationen bzw. Daten, die für das Testen verwendet werden, ist sichergestellt;

k. Für Gäste gemäss Gästereglement[4] (z.B. Lieferanten, Emeriti, Dozierende etc.) zugängliche Informationen und IT-Mittel der ETH Zürich sind gemäss einem vereinbarten Niveau der Informationssicherheit und der Dienstleistungserbringung vertraglich geschützt;

l. Informationssicherheitsvorfälle einschliesslich deren Benachrichtigung werden konsistent und wirksam gehandhabt. Dies umschliesst den Umgang mit Schwächen in Prozessen;

m. Informationssicherheit ist in die Notfallplanung der ETH Zürich eingebettet und

n. Informationssicherheit ist in Übereinstimmung mit den Richtlinien und Verfahren der ETH Zürich sowie den gesetzlichen, regulatorischen oder vertraglichen Verpflichtungen umgesetzt. Verstösse werden angemessen geahndet.

[2] Obige Anforderungen werden im Rahmen der Informationssicherheitsstrategie mittels risiko-orientiertem Ansatz auf die Bedürfnisse der ETH Zürich angepasst. Im Zentrum dieser Strategie stehen die Informationsbestände, Prozesse, Applikationen und Systeme sowie Personen und Werte. Den Grundsätzen der Zweckmässigkeit, der Wirtschaftlichkeit und der Benutzerfreundlichkeit wird Rechnung getragen.

[3] Die Berichterstattung zur Informationssicherheit erfolgt mittels compliance-orientiertem Ansatz.

[4] RSETHZ 515.2

3. Abschnitt: Aufgaben, Verantwortlichkeiten, Kompetenzen

Artikel 5 Informationssicherheit als Führungsaufgabe

[1] Informationssicherheit ist eine Führungsaufgabe, die durch die Mitglieder der Schulleitung sowie die Leitenden der Organisationseinheiten der ETH Zürich in ihrem Zuständigkeitsbereich wahrgenommen wird. Informationssicherheit ist eine gemeinsame Verantwortung, an der alle Mitarbeitenden aktiv beitragen.

[2] Die Umsetzung von Informationssicherheit liegt in der Verantwortung der Führungspersonen der zentralen Organe, Departemente und deren Institute, Zentren, Laboratorien und Professuren sowie der Führungspersonen der Einheiten ausserhalb der Departemente.

[3] Die Leitenden der Organisationseinheiten arbeiten mit der/dem CISO aktiv zusammen.

Artikel 6 Chief Information Security Officer

[1] Die ETH Zürich bestellt einen/eine Chief Information Security Officer (CISO).

[2] Er/sie ist administrativ der Abteilung Informatikdienste zugeordnet. Für die Erarbeitung von Regularien und der Informationssicherheitsstrategie oder die Durchführung von Audits im Bereich Informationssicherheit berichtet er/sie an den Generalsekretär/die Generalsekretärin. Er/Sie koordiniert die Informationssicherheit hochschulweit.

[3] Der/Die Chief Information Security Officer:

a. erarbeitet und pflegt die Informationssicherheitsstrategie (zu Händen der Schulleitung) sowie Vorgaben, Empfehlungen, Fachkonzepte, Methoden, Prozesse und Hilfsmittel;

b. führt im Rahmen des Informationssicherheitsmanagement-Systems (ISMS) das Controlling der Informationssicherheit durch;

c. erstattet Bericht an die Schulleitung via Kommission Informationssicherheit (vgl. Art. 10);

d. initiiert, koordiniert und unterstützt die Implementierung von Informationssicherheit als oberstes, fachlich unabhängiges Führungsorgan;

e. initiiert, führt durch und koordiniert Sensibilisierungs- und Schulungsmassnahmen;

f. ist zentrale Anlauf- und Beratungsstelle für die Schulleitung und die Information Security Officers (ISOs, vgl. Art. 7);

g. leitet die ISO-Gremien und koordiniert gemeinsame Vorhaben der ISOs. Er/Sie kann auch Arbeitsgruppen einsetzen;

h. ist zuständiger Kontakt zum vom Bund betriebenen «Dienst Überwachung Post- und Fernmeldeverkehr» (ÜPF) und informiert den Rechtsdienst, wenn er/sie von Strafverfolgungsbehörden kontaktiert wird und

i. vertritt die ETH Zürich in externen Fachgremien.

[4] Der/Die Chief Information Security Officer hat folgende Kompetenzen:

a. darf Informationen zum Status der Informationssicherheit und der Informationssicherheitsrisiken einfordern;

b. ordnet Sofortmassnahmen an im Falle dringender Bedrohungslagen für die Informationssicherheit bei einer erheblichen Beeinträchtigung der ordentlichen Nutzung von IT-Mitteln oder einer Schädigung der ETH Zürich, von deren Angehörigen oder von Dritten;

c. ordnet Massnahmen an bei Verdacht auf Missbrauch der IT-Mittel der ETH Zürich;

d. legt den Grundschutz fest und orientiert sich dabei an den in der Fachwelt bewährten Standards und Normen. Grundschutz beinhaltet organisatorische Massnahmen und Technologien zur hinreichenden Absicherung von Informationsbeständen, Prozessen, Applikationen und Systemen;

e. hat ein Prüfrecht bezüglich Informationssicherheit in der gesamten ETH Zürich und bei externen Partnern, die im Auftrag der ETH Zürich Dienstleistungen erbringen, soweit vertraglich vereinbart oder eine gesetzliche Grundlage dafür besteht;

f. ist bezüglich der Einhaltung und Umsetzung von Vorgaben zur Informationssicherheit weisungsbefugt gegenüber Mitarbeitenden, Studierenden und Gästen der ETH Zürich gemäss Gästereglement[5];

g. kann im Rahmen des Grundschutzes befristete Ausnahmebewilligungen erteilen, wobei diese bei Ablauf durch den Antragsteller bzw. die Antragstellerin überprüft und gegebenenfalls neu zu beantragen sind und

h. hat das Recht, Ausnahmebewilligungen zu entziehen oder deren Erteilung in Absprache mit den betroffenen Organisationseinheiten zu delegieren oder wieder zu entziehen.

Artikel 7 Information Security Officers

[1] Die Abteilungsleitenden, Stabsleitenden, Departementsvorstehenden und die Leitenden der Einheiten ausserhalb der Departemente bezeichnen je eine/einen Information Security Officer (ISO) für ihren Verantwortungsbereich.

[2] Der/Die Information Security Officer:

a. ist erste Anlauf- und Beratungsstelle für alle Belange der Informationssicherheit für den eigenen Verantwortungsbereich;

b. führt ein aktuelles Inventar der Informationsbestände basierend auf den Meldungen der Informationseignerinnen und -eigner und meldet diese periodisch dem/der CISO. Die hierzu anzuwendenden Verfahren sind in der Weisung «Inventarisierung und Klassifizierung von Informationen an der ETH Zürich» definiert;

c. erstattet mindestens einmal jährlich Bericht über den Stand der Informationssicherheit an den/die CISO und

[5] RSETHZ 515.2

d. nimmt an den Sitzungen der ISO-Gremien teil und arbeitet aktiv im Rahmen von Arbeitsgruppen der ISOs mit.

Artikel 8 Informationseignerinnen und -eigner

[1] Informationseignerinnen und -eigner sind verantwortlich für die Informationsbestände, die durch sie oder in ihrem Auftrag erhoben und bearbeitet werden. Sie sind in der Regel Leitende mit Budgetverantwortung einer Organisationseinheit (Professorinnen/Professoren, Leitende von Einheiten ausserhalb der Departemente, Abteilungsleitende, Stabsleitende).

[2] Die Informationseignerinnen und -eigner:

a. wissen, welche Vorgaben und Gesetze für ihre Informationsbestände anwendbar sind und kennen die entsprechenden Fachstellen wie z.B. die Exportkontrollfachstelle oder die Datenschutzberatenden innerhalb der ETH Zürich und

b. inventarisieren und klassifizieren ihre Informationen nach Vertraulichkeit, Integrität und Verfügbarkeitsanforderungen.

Artikel 9 IT-Betreibende

[1] IT-Betreibende verwalten, pflegen und entwickeln IT-Mittel weiter. IT-Betreibende für die ETH Zürich sind namentlich die Abteilung Informatikdienste, die IT Services Groups (ISG) der Departemente und der zentralen Organe sowie Professuren mit eigener IT und das CSCS.

[2] Die IT-Betreibenden:

a. setzen die Vorgaben der/des CISO um;

b. stufen in ihrer Verantwortung den Schutzbedarf von IT-Mittel ein;

c. gewährleisten die Informationssicherheit ihrer IT-Mittel;

d. überwachen ihre IT-Mittel und

e. sind zuständig für die Behandlung von Informationssicherheitsvorfällen in ihrem Verantwortungsbereich.

[3] Meldung von Vorfällen der Informationssicherheit:

a. IT-Betreibende sind zur umgehenden Meldung[6], spätestens innerhalb von 24 Stunden[7] nach Bekanntwerden, an die Abteilung Informatikdienste verpflichtet.

b. IT-Betreibende melden darüber hinaus Verletzungen der Datensicherheit mit Bezug zu Personendaten umgehend, spätestens innerhalb 72 Stunden, an die/den Datenschutzberaterin/Datenschutzberater[8] der ETH Zürich.

[6] E-Mail Adresse: security@ethz.ch
[7] Cybersicherheitsverordnung (CSV) SR 120.73, Art. 21, Abs. 1
[8] E-Mail Adresse: ds@ethz.ch

[4] Die Informatikdienste (ID) sind ausserdem zuständig für die Überwachung der IT-Sicherheit aller IT-Mittel, um Schwachstellen und Informationssicherheitsvorfälle zu identifizieren.

a. Sie stellen sicher, dass die IT-Sicherheitsvorfälle detektiert und geeignet behandelt werden können.

b. Sie unterstützen den/die CISO mit technischen Abklärungen zu Vorfällen der Informationssicherheit.

4. Abschnitt: Steuerung

Artikel 10 Kommission Informationssicherheit

[1] Die Kommission Informationssicherheit empfiehlt der Schulleitung im Sinne eines vorbehandelnden Ausschusses:

a. die Aktualisierung der Informationssicherheitsstrategie inklusive der Definition und der Massnahmen zur Umsetzung und

b. den Bericht zum Stand der Informationssicherheit.

[2] Der/Die CISO erstellt die vorgenannten Unterlagen und bespricht diese mit der Kommission Informationssicherheit.

[3] Die Kommission Informationssicherheit tritt so oft zusammen, wie es die Geschäfte erfordern, mindestens aber einmal jährlich.

Artikel 11 Gremien der Informationssicherheit

[1] Die beiden Gremien der Informationssicherheit sind die «ISOs der Departemente» und die «ISOs der Zentralen Organe und Einheiten ausserhalb der Departemente».

[2] Die Gremien dienen der Koordination übergreifender Vorhaben, dem gegenseitigen Informationsaustausch und dem fachlichen Review. Des Weiteren sind die beiden Gremien beratend für den/die CISO tätig.

Artikel 12 Weisungslandschaft

Die Weisungslandschaft der Informationssicherheit unterscheidet die folgenden hierarchischen Ebenen (siehe Anhang «Rahmenwerk der Informationssicherheit»):

a. Die Schulleitung erlässt Weisungen zur Umsetzung der Vorgaben aus dem strategischen Management;

b. Der/Die CISO setzt Weisungen in Kraft, welche die ETH Zürich-weiten Verfahren der Informationssicherheit festlegen und

c. Die Leitungsfunktionen der Organisationseinheiten konkretisieren die Verfahren (Prozeduren der Informationssicherheit) nötigenfalls in eigenen Weisungen und berücksichtigen hierbei die technischen und organisatorischen Gegebenheiten.

5. Abschnitt: Schlussbestimmungen

Artikel 13 Inkrafttreten

Die Weisung tritt am 01. Januar 2025 in Kraft.

Zürich, 17. Dezember 2024

Im Namen der Schulleitung:

Der Präsident: Prof. Joël Mesot

Die Generalsekretärin: Katharina Poiger Ruloff

Anhang – Rahmenwerk Informationssicherheit