Weisung «Informationssicherheit an der ETH Zürich»

vom 9. April 2018

Die Schulleitung der ETH Zürich,

gestützt auf Art. 4 Abs.1 Bst. g der Verordnung über die Organisation der Eidgenössischen Technischen Hochschule Zürich vom 16. Dezember 2003[1]

v e r o r d n e t:

1. Abschnitt: Allgemeine Bestimmungen

Artikel 1 Zweck

[1]Die ETH Zürich ist verantwortlich für die Beurteilung des Schutzbedarfs der bei ihr vorhandenen und für die Erfüllung der Aufgaben nach Art. 2 ETH-Gesetz benötigen Informationen (*Personal- und Studierendendaten, Forschungsdaten, geschäftsrelevante Dokumente, Gebäudepläne, etc*).

[2]Die ETH Zürich sorgt in ihrem Zuständigkeitsbereich dafür, dass die Informationssicherheit nach dem Stand von Wissenschaft und Technik organisiert, umgesetzt und überprüft wird. Sie orientiert sich dabei an den in der Fachwelt bewährten «Good Practices».

[3]Diese Weisung legt die Informationssicherheitsziele, die Eckwerte für den Umgang mit Risiken fest und regelt die Verantwortlichkeiten für Steuerung und Kontrolle der Ziele und Risiken.

Artikel 2 Geltungsbereich

[1]Diese Weisung gilt für alle Einheiten der ETH Zürich, gemäss Verordnung über die Organisation der Eidgenössischen Technischen Hochschule Zürich vom 16. Dezember 2003 (nachfolgend *Organisationsverordnung ETH Zürich*)[2] und deren Angehörige, namentlich für

- die Zentralen Organe
- Departemente und deren Institute, Zentren, Laboratorien und Professuren
- «Lehr- und Forschungseinrichtungen ausserhalb der Departemente gemäss Art. 61 Organisationsverordnung ETH Zürich», die allein von der ETH Zürich betrieben werden

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

[3]Für die Nutzung von Informatikmitteln der ETH Zürich gilt die Benutzerordnung für Telematik (BOT)[3].

---

[1] RSETHZ 201.021
[2] RSETHZ 201.021
[3] RSETHZ 203.21

Artikel 3 Begriffe

[1]*Grundschutz*	Massnahmen zur hinreichenden Absicherung von Informationsbeständen, Prozessen, Applikationen und Systemen mit normalem Schutzbedarf.
[2]*Informationssicherheit*	«Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Information».[4]
[3]*Integrität*	«Eigenschaft der Richtigkeit und Vollständigkeit».[5]
[4]*IT-Betreiber*	Betreiber von IT-Services und -Infrastrukturen für die ETH Zürich sind namentlich die Informatikdienste, das CSCS, die Informatiksupportgruppen der Departemente (ISG).[6]
[5]*IT-Sicherheit*	Gewährleistung der Informationssicherheit beim Einsatz von Informatikmitteln.

2. Abschnitt: Aufgaben, Verantwortlichkeiten, Kompetenzen («Information Security Governance»)

Artikel 4 Grundsatz

[1]Informationssicherheit ist eine Führungsaufgabe, die durch die Mitglieder der Schulleitung sowie die Leitenden der Organisationseinheiten der ETH Zürich in ihrem Zuständigkeitsbereich wahrgenommen wird. Als Informationseignende sind sie verantwortlich für die Informationsbestände, die durch sie/ihn oder in ihrem/seinem Auftrag erhoben und bearbeitet werden.[7]

[2]Die Umsetzung von Informationssicherheit im Sinne dieser Weisung und nach den Vorgaben des CISO gemäss Art. 5 und das zugrundeliegende Risikomanagement für die jeweilige Organisationseinheit liegen in der Verantwortung der Abteilungsleitenden, der Stabsleitenden, Departementsvorstehenden und Leitenden der Lehr- und Forschungseinrichtungen ausserhalb der Departemente.

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

Artikel 5 Chief Information Security Officer

[1]Die ETH Zürich verfügt über einen Chief Information Security Officer (CISO).

[2] Er/Sie koordiniert innerhalb der festgelegten Ziele nach Art. 12 dieser Weisung die Informationssicherheit hochschulweit, berät die Informationseigner/innen und Information Security

[4] ISO/IEC DIS 27000:2015 Informationstechnik– IT-Sicherheitsverfahren– Informationssicherheits-Managementsysteme– Überblick und Terminologie
[5] ISO/IEC DIS 27000:2015
[6] Art. 4 BOT
[7] Art. 6 Richtlinien über den Schutz und den Umgang mit Personaldaten an der ETH Zürich (RSETHZ 612)

Officers (ISOs) und berichtet regelmässig der Risikomanagement Kommission über seine/ihre Aktivitäten.

[3]Zur Gewährleistung der Unabhängigkeit wird der/die CISO im Bereich des Präsidenten (z.B. bei der Generalsekretärin/dem Generalsekretär) eingegliedert.

[4]Die Aufgaben und Verantwortlichkeiten der/des CISO/s sind namentlich:

a. Initiierung, Koordination und Unterstützung der Implementierung der Informationssicherheit an der ETH Zürich;

b. Erarbeitung, Abstimmung, Vernehmlassung und Pflege der Informationssicherheitsstrategie der ETH Zürich sowie von Empfehlungen, Fachkonzepten, Methoden, Prozessen und Hilfsmitteln zu Themen der Informationssicherheit;

c. Erarbeitung von Sicherheitsmassnahmen gemäss Art. 19 dieser Weisung;

d. Leitung der ISO-Gremien nach Art. 11 dieser Weisung und Koordination gemeinsamer Vorhaben der ISOs. Er/Sie kann auch Arbeitsgruppen einsetzen;

e. Initiierung, Durchführung und Koordination von Sensibilisierungs- und Schulungsmassnahmen zur Informationssicherheit unter Berücksichtigung der rechtlichen Vorgaben zur Informationssicherheit im Sinne der Grundsätze des Informationssicherheitsgesetzes des Bundes (ISG)[8], des Datenschutzgesetzes, des Humanforschungsgesetzes und entsprechenden Verordnungen;

f. Zentrale Anlauf- und Beratungsstelle für alle Belange der Informationssicherheit;

g. Controlling des Informationssicherheitsmanagements der ETH Zürich;

h. ETH Zürich-weites Management[9] von Informationssicherheitsrisiken: Konsolidierung und Beurteilung der von den ISOs gemäss Art. 6 dieser Weisung gelieferten Informationen;

i. Regelmässige Aktualisierung des Inventars von Informationsbeständen mit erhöhtem Schutzbedarf aufgrund der Meldungen der ISOs (Art. 6);

j. Berichterstattung an die Risikomanagement Kommission (RMK) über den Stand der Informationssicherheit, sowie über besondere Vorkommnisse, Missbräuche nach Art. 19 BOT und getroffene Sanktionen nach Art. 20 BOT;

k. Leitung der RMK Fachgruppe Informationssicherheit;

l. Vertretung der ETH Zürich in externen Fachgremien.

[5]Die/Der CISO hat folgende Kompetenzen:

a. Festlegung des Grundschutzes[10] gemäss Art. 19 dieser Weisung;

b. Weisungsbefugnis gegenüber Professoren und Professorinnen, Mitarbeitenden, Studierenden, internen und externen Leistungserbringern (sofern vertraglich vereinbart), Gästen und Partnern der ETH Zürich bezüglich der Einhaltung und Umsetzung verbindlicher Informationssicherheitsvorgaben;

---

[8] Zeitpunkt des Inkrafttretens noch nicht bekannt
[9] Nachträgliche redaktionelle Berichtigung vom August 2018
[10] Nachträgliche redaktionelle Berichtigung vom August 2018

c. Einfordern von Informationen zum Status von Informationssicherheit und Informationssicherheitsrisiken;

d. 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;

e. Anordnung von Massnahmen bei Verdacht auf Missbrauch der Telematik-Mittel der ETH Zürich gemäss Art. 20 BOT;

f. Anordnung von Sofortmassnahmen nach Ziffer 4 Anhang BOT im Falle dringender akuter Bedrohungslagen oder Angriffen mit grossem Risiko für die Informationssicherheit der ETH Zürich in Zusammenarbeit mit den in dieser Weisung genannten Fachstellen, namentlich dem ITSO ID.

Artikel 6 Information Security Officers

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

[2]Sofern nicht abweichend festgelegt, nehmen in den Departementen die Informatiksupportleitenden (ISL) die Rolle der ISOs wahr.

[3]Die Aufgaben und Verantwortlichkeiten der ISOs sind namentlich:

a. Führen eines aktuellen Inventars der Informationsbestände mit hohem Schutzbedarf basierend auf den Meldungen der Informationseigner;

b. Erste Anlauf- und Beratungsstelle für alle Belange der Informationssicherheit;

c. Berichterstattung über den Stand der Informationssicherheit, sowie der Informationssicherheitsrisiken an den/die CISO;

d. Teilnahme an den Sitzungen der ISO-Gremien, sowie aktive Mitarbeit in Rahmen von Arbeitsgruppen der ISOs.

Artikel 7 Informationseigner

Informationseigner sind verantwortlich für die Informationsbestände, die durch sie/ihn oder in ihrem/seinem Auftrag erhoben und bearbeitet werden (vgl. Art. 4 Abs. 1). Sie sind in der Regel die Leiter/innen einer Organisationseinheit (Professoren/Professorinnen, Abteilungsleitende, Leitende von ausserdepartementalen Lehr- und Forschungseinrichtungen, Stabsleitende). Sie sind auch die klassifizierenden Stellen gemäss Art. 21 dieser Weisung.

Artikel 8 IT Security Officer Informatikdienste

[1]Der Abteilungsleiter Informatikdienste ernennt eine/n IT Security Officer Informatikdienste (ITSO ID).

[2]Er/Sie ist fachlich verantwortlich für die IT-Sicherheit der Services, die durch die ID für die zentralen und dezentralen Organisationseinheiten der ETH Zürich erbracht werden und diesbezüglich zentrale Ansprechpartner/in des/der CISO. Darüber hinaus berät er/sie den/die CISO und die ISOs bei Bedarf in Fragen der IT-Sicherheit.

[3]Er/Sie veranlasst im Auftrag des CISOs Kontrollen im Sinne von Art. 18 Abs. 2 BOT.

[4]Während akuter Bedrohungslagen oder Angriffen mit grossem Risiko für die IT-Sicherheit der ETH Zürich, die sofortiges Handeln notwendig machen, kann er/sie sichernde und vorsorgliche Massnahmen im Sinne Ziffer 4 Abs. 2 Anhang der BOT anordnen, unter gleichzeitiger Benachrichtigung des CISOs.

Artikel 9 IT Betreiber

Die IT-Betreiber sind zuständig für die Einstufung des Schutzbedarfs von Systemen, Applikationen und Prozessen in ihrer Verantwortung gemäss Art. 23 dieser Weisung, sowie für die Beurteilung von Informationssicherheitsrisiken der von ihnen verantworteten Services und die Umsetzung von Sicherheitsmassnahmen gemäss Art. 19 dieser Weisung.

Artikel 10 Informatikdienste

Die Informatikdienste sind zuständig für die Sicherheitsüberwachung des gesamten Netzwerkverkehrs der ETH Zürich und die Koordination der Behandlung von Informationssicherheitsvorfällen in ihrem Verantwortungsbereich. Im Übrigen werden die Zuständigkeiten der Informatikdienste in Art. 4 BOT geregelt.

Artikel 11 Gremien

[1]Die Fachgruppe Informationssicherheit der Risikomanagement Kommission (RMK) ist eine Arbeitsgruppe von Risikomanagement Fachexperten. Sie unterstützt den/die CISO beim Aufbau der Informationssicherheit und wirkt neben den ISOs und dem/der ITSO ID als fachliches Review-Gremium.

[2]Zur Koordination übergreifender Vorhaben, zum gegenseitigen Informationsaustausch und zur fachlichen Review bestehen die Gremien der «ISOs der Departemente» und der «ISOs der Zentralen Organe & Lehr- und Forschungseinrichtungen ausserhalb der Departemente».

3. Abschnitt: Informationssicherheitsziele

Artikel 12 Ziele

Um ihre Handlungsfähigkeit sicherzustellen und zur Vermeidung von Schäden, werden die folgenden Informationssicherheitsziele für die ETH Zürich festgelegt:

a. Einhaltung der rechtlichen Anforderungen in Bezug auf Informationssicherheit;
b. Bedarfsgerechter Schutz von Verfügbarkeit, Vertraulichkeit und Integrität von Informationsbeständen, Prozessen, Applikationen und IT-Komponenten;
c. Erkennung und Behandlung von erfolgreichen Angriffen auf die Informationssicherheit.

Artikel 13 Umsetzung der Ziele

Die Organisationseinheiten setzen Ziele und Massnahmen, soweit finanziell und personell möglich, eigenverantwortlich und nach den Vorgaben und Empfehlungen des CISO um.

Artikel 14 Kultur der Informationssicherheit

[1]Die ETH Zürich fördert durch bedarfsgerechte Schulungs- und Sensibilisierungsmassnahmen eine Kultur des bewussten Umgangs mit Informationen.

[2]In Prozessen, Projekten und im Betrieb werden die jeweils relevanten Informationssicherheitsaspekte durchgehend berücksichtigt.

4. Abschnitt: Umgang mit Risiken

Artikel 15 Risikobasierter Ansatz

[1]Im Zusammenhang mit der Informationssicherheit verfolgt die ETH Zürich einen risikobasierten Ansatz. Sie orientiert sich dabei an den in der Fachwelt bewährten «Good Practices», Standards und Normen im Sinne von Art. 1 Abs. 2 dieser Weisung.

[2]Informationssicherheitsrisiken sollen mittels geeigneter Massnahmen auf ein akzeptables Risikoniveau reduziert werden, wobei den Grundsätzen der Zweckmässigkeit, der Wirtschaftlichkeit und der Benutzerfreundlichkeit Rechnung getragen wird.

[3]Im Zentrum des risikobasierten Ansatzes stehen die Informationsbestände, Prozesse, Applikationen und Systeme mit hohem Schutzbedarf gemäss Art. 23 dieser Weisung.

Artikel 16 Informationsbestände mit hohem Schutzbedarf

Als Informationsbestände mit hohem Schutzbedarf gelten mindestens:

a. Besonders schützenswerte Personendaten und Persönlichkeitsprofile gemäss Bundesgesetz über den Datenschutz und Art. 59 ff. PVO-ETH, die insbesondere in Personal- und Studienadministrationssystemen gemäss Art. 36a und 36b ETH-Gesetz bearbeitet werden;
b. Gesundheitsbezogene Daten gemäss Humanforschungsgesetz und den einschlägigen Verordnungen;
c. Forschungsbezogene Daten in Forschungsprojekten, bei welchen aus vertraglichen oder anderen Gründen ein hoher Schutzbedarf erforderlich ist;
d. Lehrbezogene Daten mit Informationen über Studienleistungen und -abschlüsse;
e. Finanzinformationen (SAP, online Banking, produktives Buchungssystem, etc.);
f. Infrastrukturdaten (z.B. Gebäudepläne und extern gelagerte Gebäudepläne);
g. Archive sowie
h. Webauftritte der ETH Zürich.

Artikel 17 Meldepflicht gegenüber dem/der CISO

[1]Mindestens einmal jährlich sind dem/der CISO von den ISOs zu melden:

- Informationsbestände mit hohem Schutzbedarf
- Informationssicherheitsrisiken und Sicherheitsmassnahmen

[2]Die/Der CISO führt ein Register der gemäss Abs. 1 gemeldeten Informationsbestände, Risiken und Sicherheitsmassnahmen.

Artikel 18 Risikobeurteilung durch den/die CISO

[1]Der/Die CISO beurteilt die ihm gemäss Artikel 17 gemeldeten Informationsbestände, Informationssicherheitsrisiken und Massnahmen.

[2]Im Falle einer von der Einschätzung des Informationseigners abweichenden Beurteilung konsultiert der/die CISO den/die Corporate Risk Manager, den/die zuständige Information Security Officer und den/die Informationseigner/in zwecks notwendiger Anpassungen.

[2]Konfliktfälle können von den Beteiligten der «RMK Fachgruppe Informationssicherheit» zur Klärung vorgelegt werden. Der CISO tritt dabei in den Ausstand.

Artikel 19 Sicherheitsmassnahmen

[1]Die/Der CISO legt den Grundschutz fest. Der Grundschutz orientieren sich an gängigen «Good Practices» gemäss Art. 1 Abs. 2 und bieten hinreichend Schutz für Informationsbestände, Prozesse, Applikationen und Systeme mit normalem Schutzbedarf.

[2]Informationsbestände, Prozesse, Applikationen und Systeme mit hohem Schutzbedarf werden mit verschärften Mitteln gegen den Zugriff durch Unbefugte geschützt. Dies betrifft insbesondere den Zugriff auf Systeme, Applikationen und Informationen, als auch den physischen Zutritt zu den Systemen selber. Dafür werden standardisierte Sicherheitsmassnahmen umgesetzt. Diese Massnahmenpakete werden durch den/die CISO in Absprache mit den ISOs und den zuständigen IT-Betreibern festgelegt.

[3]Für Informationsbestände mit hohem Schutzbedarf wählt der/die Informationseigener/in die geeigneten Sicherheitsmassnahmen nach Absatz 2 und stellt deren Umsetzung sicher. Der/Die zuständige ISO berät den/die Informationseigner/in hinsichtlich Massnahmenauswahl. Sollten die standardisierten Massnahmen nicht eingesetzt werden können, werden in Absprache mit ISO und CISO alternative Massnahmen ergriffen.

6. Abschnitt: Klassifizierung von Informationen und Schutzbedarf

Artikel 20 Grundsätze der Klassifizierung

[1]Die Klassifizierung von Informationen nach den in Artikel 22 genannten Klassifizierungsstufen wird auf das erforderliche Mindestmass und wenn möglich zeitlich beschränkt.

[2]Die Informationseigner/innen bezeichnen Informationen in ihrem Verantwortungsbereich, die vertraulich sind, eine hohe Integrität oder hohe Verfügbarkeit haben müssen.

Artikel 21 Zuständigkeiten der Klassifizierung

[1]Die Informationseigner/innen sind für die Klassifizierung der in ihrem Verantwortungsbereich vorhandenen Informationen zuständig (klassifizierende Stelle).

[2]Klassifizierungen dürfen nur von der klassifizierenden Stelle oder von der Stelle, die dieser übergeordnet ist, geändert oder aufgehoben werden.

Artikel 22 Klassifizierungsstufen

Klassifikation der Vertraulichkeit:

a) Öffentlich:
Als öffentlich gelten alle Informationen, die von der zuständigen Stelle zur Veröffentlichung frei gegeben werden (z.B. durch die Schulleitung oder die Hochschulkommunikation). Bis dahin sind alle Informationen intern oder vertraulich.

b) Intern:
Interne Informationen sind für Angehörige der ETH Zürich[11] bestimmt. Als intern gelten alle Informationen der ETH, die vom Informationseigner nicht anderweitig klassifiziert wurden.

c) Vertraulich:
Informationen, die für einen eingeschränkten, explizit festgelegten Empfängerkreis bestimmt sind.

Klassifikation der Integrität:

a) Normal:
Mögliche Auswirkungen unbefugter oder unbeabsichtigter Veränderungen der Informationen sind für den/die Informationseigner/in akzeptabel. Ein sorgfältiger Umgang mit den Informationen im Tagesgeschäft, sowie die Anwendung von Grundschutzmassnahmen (wie Zugriffsschutz und Backup) werden als ausreichende Sicherheitsmassnahmen betrachtet.
Gilt als Standardwert für alle Informationen, die bezüglich Integrität nicht explizit als «hoch» eingestuft sind.

b) Hoch:
Unbefugte oder unbeabsichtigte Veränderungen der Informationen sind für den/die Informationseigner/in nicht akzeptabel. Sie müssen verhindert oder mindestens erkannt werden.

Klassifikation der Verfügbarkeit:

a) Normal:
Einschränkungen beim Zugriff auf die Informationen oder ein vollständiger Verlust der Zugriffsmöglichkeiten während mindestens einem Arbeitstag[12] ist akzeptabel.
Ein Verlust der seit der letzten Datensicherung vor einem Vorfall durchgeführten Änderungen an den Informationen ist akzeptabel.
Gilt als Standardwert für alle Informationen, die bezüglich Verfügbarkeit nicht explizit als «hoch» eingestuft sind.

b) Hoch
Einschränkungen beim Zugriff auf die Informationen oder ein vollständiger Verlust der Zugriffsmöglichkeiten während bis zu 12 Stunden ist akzeptabel.
Ein Verlust der seit der letzten Datensicherung einem Vorfall durchgeführten Änderungen an den Informationen ist akzeptabel oder zusätzliche Massnahmen zum Schutz vor Datenverlust sind erforderlich.

---

[11] ETH Gesetz, Art. 13
[12] Als Arbeitstage gelten in dieser Weisung: Montag – Freitag, ausgenommen Feiertage

Artikel 23 Schutzbedarf

[1]Hoher Schutzbedarf
Informationsbestände, die gemäss Artikel 22 dieser Weisung als «vertraulich» oder als «hoch» bezüglich Integrität oder Verfügbarkeit eingestuft sind, haben hohen Schutzbedarf.

Gleiches gilt für Prozesse, Applikationen und Systeme, die Informationsbestände mit hohem Schutzbedarf bearbeiten, bzw. deren Verlust die Erfüllung der gesetzlichen Aufgaben der ETH Zürich wesentlich beeinträchtigen oder bedeutende Wiederherstellungskosten verursachen.

[2]Normaler Schutzbedarf
Informationsbestände, Prozesse, Applikationen und Systeme, die keinen hohen Schutzbedarf aufweisen, haben normalen Schutzbedarf.

7. Abschnitt: Schlussbestimmungen

Artikel 24 Übergangsbestimmung

Die Leiterin SGU in ihrer Rolle als IT-Sicherheitsbeauftragte und der Leiter Informatikdienste in seiner Rolle als CISO bleiben bis zum Amtsantritt des/der CISO zuständig für die Anliegen der Informationssicherheit.

Artikel 25 Inkrafttreten

Die Weisung tritt am 1. Mai 2018 in Kraft.

Zürich, 9. April 2018

Im Namen der Schulleitung:

Der Präsident: Lino Guzzella

Die Generalsekretärin: Katharina Poiger Ruloff