Weisung «Informationssicherheit an der ETH Zürich»

vom 9. April 2018 (Stand: 1. August 2021)[1]

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[2]

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*)[3] 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.

---

[1] Teilrevision zur Einführung einer vierten Stufe zur Klassifizierung nach Vertraulichkeit sowie zur Nutzung externer Cloud-Dienste gemäss Beschluss der Schulleitung vom 12. Juli 2021.
[2] RSETHZ 201.021
[3] RSETHZ 201.021

[3]Für die Nutzung von Informatikmitteln der ETH Zürich gilt die Benutzungsordnung für Informations- und Kommunikationstechnologie an der ETH Zürich (BOT)[4].

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».[5]
[3] *Integrität*	«Eigenschaft der Richtigkeit und Vollständigkeit».[6]
[4] *IT-Betreiber*	Betreiber von IT-Services und -Infrastrukturen für die ETH Zürich sind namentlich die Informatikdienste, das CSCS, die Informatiksupportgruppen der Departemente (ISG).[7]
[5] *IT-Sicherheit*	Gewährleistung der Informationssicherheit beim Einsatz von Informatikmitteln.
[6] *Klassifizierung von Informationen und Klassifizierungsvermerk*[8]	*Klassifizierung*: Zuweisung einer *Klassifizierungsstufe* gemäss Art. 22. *Klassifizierungsvermerk*: Notwendige Kennzeichnung* einer Klassifikation nach Vertraulichkeit (Art. 22 Abs. 1) durch Anbringen der Bezeichnung «vertraulich» oder «streng vertraulich». *Die notwendige Kennzeichnung gilt nur für als «vertraulich» oder als «streng vertraulich» klassifizierte Informationen.
[7] *Cloud-Computing und Cloud-Dienste* [9]	*Cloud-Computing*: Paradigma, einen netzwerkbasierten Zugang auf ein skalierbares und elastisches Reservoir gemeinsam nutzbarer physikalischer oder virtueller Ressourcen nach dem Selbstbedienungsprinzip und bedarfsgerechter Administration zu ermöglichen. Quelle: ISO/IEC 17788:2014, Informationstechnik – Cloud Computing – Übersicht und Vokabular, Abs. 3.2.5 *Cloud-Dienste*: Eine oder mehrere über Cloud Computing angebotene Tauglichkeiten, die mit Hilfe einer defi-

[4] RSETHZ 203.21; redaktionelle Anpassung, Fassung gemäss Schulleitungsbeschluss vom 26. März 2019, in Kraft seit 1. April 2019.
[5] ISO/IEC DIS 27000:2015 Informationstechnik– IT-Sicherheitsverfahren– Informationssicherheits-Managementsysteme– Überblick und Terminologie
[6] ISO/IEC DIS 27000:2015
[7] Art. 4 Benutzungsordnung Informations- und Kommunikationstechnologie, BOT
[8] Fassung gemäss Schulleitungsbeschluss vom 12. Juli 2021, in Kraft seit 1. August 2021.
[9] Fassung gemäss Schulleitungsbeschluss vom 12. Juli 2021, in Kraft seit 1. August 2021.

	nierten Schnittstelle aufgerufen werden. Quelle: ISO/IEC 17788:2014, Informationstechnik – Cloud Computing – Übersicht und Vokabular, Abs. 3.2.8
[8] *Externer IKT-Service bzw. externer Cloud-Dienst*[10]	Von der ETH Zürich bezogene IKT*-Dienstleistung, die ausserhalb des Netzwerks der ETH Zürich von einer Drittfirma erbracht wird (z.B. ein externer Cloud-Dienst). *IKT: Informations- und Kommunikationstechnologie Quelle: Weisung IT-Richtlinien und IT-Grundschutzvorgaben, RSETHZ 203.23

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 Informationseigner*in sind sie verantwortlich für die Informationsbestände, die durch sie/ihn oder in ihrem/seinem Auftrag erhoben und bearbeitet werden.[11]

[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 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:

---

[10] Fassung gemäss Schulleitungsbeschluss vom 12. Juli 2021, in Kraft seit 1. August 2021.
[11] Art. 6 Richtlinien über den Schutz und den Umgang mit Personaldaten an der ETH Zürich (RSETHZ 612)

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)[12], 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[13] 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[14] 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;

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

---

[12] Zeitpunkt des Inkrafttretens noch nicht bekannt
[13] Nachträgliche redaktionelle Berichtigung vom August 2018
[14] Nachträgliche redaktionelle Berichtigung vom August 2018

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*in;

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 Informationseignerinnen und -eigner[15]

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

[2] Die Einschätzung / Abklärung, welche Vorgaben und Gesetze für ihre Informationsbestände anwendbar sind (wie Datenschutz bei Personendaten, Exportkontrolle z.B. im Umgang mit Fachwissen/Technologien, die Eigenschaften besitzen auch für den militärischen Einsatz geeignet zu sein, sogenannte Dual-Use Technologien), obliegt den Informationseignerinnen – und eigner.

[15] Fassung gemäss Schulleitungsbeschluss vom 12. Juli 2021, in Kraft seit 1. August 2021.

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. *aufgehoben*

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 16bis Informationsbestände mit sehr hohem Schutzbedarf

Als Informationsbestände mit sehr hohem Schutzbedarf gelten mindestens:

a. Gesundheitsbezogene Daten gemäss Humanforschungsgesetz und den einschlägigen Verordnungen;

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 Informationseignerin und -eigner zwecks notwendiger Anpassungen.

[3] 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 orientiert sich an gängigen «Good Practices» gemäss Art. 1 Abs. 2 und bietet hinreichend Schutz für Informationsbestände, Prozesse, Applikationen und Systeme mit normalem oder hohem Schutzbedarf.

[2] Informationsbestände, Prozesse, Applikationen und Systeme mit sehr 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 sehr 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.

5. Abschnitt: Klassifizierung von Informationen und Schutzbedarf

Artikel 20 Grundsätze der Klassifizierung[16]

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

[2] Informationseignerinnen und -eigner *klassifizieren* die Informationen in ihrem Verantwortungsbereich (Klassifizierungspflicht) nach risiko-orientierten Prinzipien gemäss Art. 22. Die Klassifizierung erfolgt in der Regel formlos.

[3] Für «vertrauliche» und «streng vertraulichen» Informationen gilt eine Kennzeichnungspflicht mittels Klassifizierungsvermerk. Über die Kennzeichnung vertraulicher Forschungsdaten entscheiden die Informationseignerinnen und -eiger.

[4] Für die Klassifizierung wie auch für die Kennzeichnung von Informationen sind vertragliche Abmachungen zu berücksichtigen. Klassifiziert beispielsweise ein externer Partner die der ETH zur Verfügung gestellten Informationen höher als die ETH, ist die höhere Klassifizierung gemäss Art. 22 zu wählen und umgekehrt.

[5] Das Öffentlichkeitsprinzip der Verwaltung (BGÖ) gilt weiterhin auch für klassifizierte Informationen.

Artikel 21 Zuständigkeiten der Klassifizierung[17]

[1] Informationseignerinnen und -eigner sind für die Klassifizierung der in ihrem Verantwortungsbereich vorhandenen Informationen verantwortlich (klassifizierende Stelle). Sofern Informationseignerinnen und -eigner gemäss Artikel 7 keine Vorgabe zur Klassifizierung machen, kann die Standard-Klassifizierung angenommen werden: «intern» für die Vertraulichkeit und «normal» für die Integrität bzw. für die Verfügbarkeit von Informationen.

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

---

[16] Fassung gemäss Schulleitungsbeschluss vom 12. Juli 2021, in Kraft seit 1. August 2021.
[17] Fassung gemäss Schulleitungsbeschluss vom 12. Juli 2021, in Kraft seit 1. August 2021.

Artikel 22 Klassifizierungsstufen[18]

[1] Klassifikation nach Vertraulichkeit:

a) ÖFFENTLICH:
Als öffentlich gelten Informationen, die von der zuständigen Stelle zur Veröffentlichung freigegeben werden.

Klassifizierungshilfe: Für die Veröffentlichung von Informationen (Klassifizierung als «öffentlich») von administrativ-technischen Informationen ist in der Regel eine Kommunikationsstelle der ETH Zürich beizuziehen (departemental oder Hochschulkommunikation). Über die Veröffentlichung von Forschungsresultaten entscheidet, Vorbehalt vertraglicher oder gesetzlicher Rechte Dritter, wie zum Beispiel Urheberrechte, der/die Informationseignerinnen und -eigner[19].

Veröffentlichte Informationen müssen nicht mit einem Klassifizierungsvermerk als solche gekennzeichnet werden.

b) INTERN:
Als «intern» gelten Informationen, deren Kenntnisnahme durch Unberechtigte die Interessen der ETH Zürich beeinträchtigen kann.

Klassifizierungshilfe: Interne Informationen sind für Angehörige der ETH Zürich[20] bestimmt. Interne Informationen müssen nicht mit einem Klassifizierungsvermerk als solche gekennzeichnet werden.

c) VERTRAULICH:
Als «vertraulich» gelten Informationen, deren Kenntnisnahme durch Unberechtigte die Interessen der ETH Zürich erheblich beeinträchtigen kann.

Klassifizierungshilfe: Als vertraulich gelten Informationen, die (in der Regel) nur für einen bestimmten (ETH-internen wie externen) Personenkreis bzw. Gruppe, Funktion oder Rolle bestimmt sind. Vertrauliche Informationen sind mit einem Klassifizierungsvermerk als solche zu kennzeichnen.

d) STRENG VERTRAULICH:
Als «streng vertraulich» gelten Informationen, deren Kenntnisnahme durch Unberechtigte die Interessen der ETH Zürich schwerwiegend beeinträchtigen kann.
Klassifizierungshilfe: Als streng vertraulich gelten Informationen, die für einen eingeschränkten, genau festgelegten und namentlich bezeichneten Empfängerkreis bestimmt sind. Streng vertrauliche Informationen sind mit einem Klassifizierungsvermerk als solche zu kennzeichnen.

[1bis] Die Klassifizierungsvermerke (die Kennzeichnung klassifizierter Informationen) sind in Grossbuchstaben zu schreiben. Nicht mit einem Klassifizierungsvermerk gekennzeichnete Informationen (z.B. Dokumente) gelten als «intern». Hiervon ausgenommen sind publizierte (öffentliche) Informationen.

---

[18] Fassung gemäss Schulleitungsbeschluss vom 12. Juli 2021, in Kraft seit 1. August 2021.
[19] ETH Gesetz, Art. 36 Abs. 2
[20] ETH Gesetz, Art. 13

[1ter] Anhang 1 enthält Empfehlungen für die Klassifizierung von Informationen nach Vertraulichkeit. Anhang 1 enthält ebenso Beispiele zur Kennzeichnung von Informationen (Anbringen der Kennzeichnungsvermerke).

[1quater] Anhang 2 enthält Vorgaben für den Umgang mit nach Vertraulichkeit klassifizierten Informationen.

1[quinques] Die Umsetzung der Vorgaben aus den Anhängen obliegt den Informationseignerinnen und -eigner.

[2] 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.

[3] Klassifikation der Verfügbarkeit:

a) Normal:
Einschränkungen beim Zugriff auf die Informationen oder ein vollständiger Verlust der Zugriffsmöglichkeiten während mindestens einem Arbeitstag[21] 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.

[21] Als Arbeitstage gelten in dieser Weisung: Montag – Freitag, ausgenommen Feiertage

Artikel 22bis Auslagerung von Informationen in externe IKT-Services (z.B. externe Cloud-Dienste)[22]

[1] Eine Auslagerung (Speicherung oder Bearbeitung) der Informationsbestände in externe IKT-Services erfolgt in **Eigenverantwortung** der Informationseignerinnen und -eigner.

[2] Unter bestimmten Voraussetzungen, dürfen Informationsbestände in externe IKT-Services ausgelagert werden (vgl. hierzu die Vorgaben in Anhang 2 «Elektronische Informationen in Cloud-Dienste» sowie die Weisung «IT-Richtlinien und IT-Grundschutzvorgaben», RSETHZ 203.23).

[3] Vorgängig zur Auslagerung der Informationsbestände in externe IKT-Services führen Informationseignerinnen und -eigner eine Risikoabschätzung durch (vgl. auch Anhang 2 «Elektronische Informationen in der Cloud»).

[4] Die Auslagerung streng vertraulicher Informationsbestände gemäss Art. 22 Abs. 1 in externe IKT-Services ist untersagt.

Artikel 23 Schutzbedarf[23]

[1] Sehr hoher Schutzbedarf

Informationsbestände, die gemäss Artikel 22 dieser Weisung als «streng vertraulich» gelten, haben sehr hohen Schutzbedarf.

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

[1bis] Hoher Schutzbedarf

Informationsbestände, die gemäss Artikel 22 dieser Weisung als «vertraulich» gelten, 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 erheblich beeinträchtigen oder bedeutende Wiederherstellungskosten verursachen.

[2] Normaler Schutzbedarf

Informationsbestände, Prozesse, Applikationen und Systeme, die keinen hohen Schutzbedarf aufweisen, haben normalen Schutzbedarf.

---

[22] Fassung gemäss Schulleitungsbeschluss vom 12. Juli 2021, in Kraft seit 1. August 2021.
[23] Fassung gemäss Schulleitungsbeschluss vom 12. Juli 2021, in Kraft seit 1. August 2021.

6. Abschnitt: Schlussbestimmungen[24]

Artikel 24

aufgehoben

Artikel 24bis Übergangsbestimmung zu Art. 22[25]

Die Klassifizierung nach Vertraulichkeit und der Umgang mit derart klassifizierten Informationen gilt gemäss Art. 22 Absatz 1, 1bis, 1ter und 1quater:

a) für neu generierte Informationen bzw. Informationsbestände (Dokumente, Datensammlungen, Papierdossiers, Archive etc.) ab 1. Dezember 2021.

b) für bereits bestehende Informationen bzw. Informationsbestände ab 1. Dezember 2023. Es obliegt den Informationseignerinnen und -eignern zu prüfen, ob insbesondere Informationen, die bereits als vertraulich klassifiziert wurden, für den Klassifizierungsvermerk streng vertraulich qualifizieren.

Artikel 24ter Übergangsbestimmung zu Art. 22bis[26]

Artikel 22bis zur Auslagerung von Informationen in externe IKT-Services (z.B. externe Cloud-Dienste) tritt am 1. Dezember 2021 in Kraft.

Artikel 25 Inkrafttreten

Die Weisung tritt am 01. Mai 2018 in Kraft.

Zürich, 9. April 2018

Im Namen der Schulleitung:

Der Präsident: Lino Guzzella

Die Generalsekretärin: Katharina Poiger Ruloff

---

[24] Fassung gemäss Schulleitungsbeschluss vom 12. Juli 2021, in Kraft seit 1. August 2021.
[25] Fassung gemäss Schulleitungsbeschluss vom 12. Juli 2021, in Kraft seit 1. August 2021.
[26] Fassung gemäss Schulleitungsbeschluss vom 12. Juli 2021, in Kraft seit 1. August 2021.

Anhang 1a: Klassifizierungsempfehlung (Vertraulichkeit)[27]

In untenstehender Liste finden sich Empfehlungen zur Klassifizierung ausgewählter Informationen nach Vertraulichkeit. Diese Empfehlung gilt vorbehältlich einer abweichenden (in der Regel höheren) Klassifizierung durch den/die Informationseigner*in. Für eine korrekte Klassifizierung der Vertraulichkeit soll insbesondere auch Anhang 1b berücksichtigt werden. Bei Unklarheiten gibt der/die Information Security Officer Auskunft.

Information / Informationsbestand (Auswahl)	Klassifikation
Web Auftritt der ETH Zürich / Internet Dokumente	**öffentlich**
Presseinformationen / Mitteilungen an die Presse	
Listen von Vorlesungen / Stundenpläne für Vorlesungen	
Forschungsdaten, Primär- und Sekundärdaten (veröffentlicht)	
veröffentlichte Dissertationen	
Rechtssammlung der ETH Zürich	
Rund-Mails	**intern**
Kalendereinträge (je nach Handhabung Informationseigner*in)	
internes Telefonbuch / Adressverzeichnis	
Newsletters/Blogs	
Townhall Meetings	
Vorlesungsskripte (sofern nicht vom Urheber öffentlich zugänglich gemacht)	
«nicht-sensible» Personendaten ohne besondere Schutzwürdigkeit (Personendaten, deren Missbrauch in der Regel für die betroffene Person keine besonderen Folgen hat, beispielsweise Name, Vorname, [Firmen]-Adresse, Geburtsdatum, [ETH]-Telefonnummer oder Informationen, die in den Medien erschienen sind, soweit sie nicht in einem sensiblen Zusammenhang stehen, vgl. Risikostufen im Leitfaden)	
Anträge Schulleitung / Departement inkl. Protokolle	**vertraulich**
Strategie der ETH Zürich (mindestens während Erarbeitung)	
Mittelfristplanung, Budgetierung & Finanzplanung, Jahresbericht in Arbeit	
Finanz-/Risikobericht	
Management Reporting inkl. Führungskennzahlen	
Personaldossiers/-dokumente: Bewerbungen, Beurteilungen, Arbeitsverträge, etc.	
Leistungsbeurteilungen Studierende, Noten, Prüfungsunterlagen	
Verträge (Kooperationen, Drittfirmen, Forschung, Geheimhaltung)	
Netzwerkpläne der Informatik	
Forschungsdaten, Primär- und Sekundärdaten vor Veröffentlichung	
(geplante und laufende) Forschungsprojekte	
Ergebnisse Umfragen	
Berater- und Lieferantenverträge	

[27] Fassung gemäss Schulleitungsbeschluss vom 12. Juli 2021, in Kraft seit 1. August 2021. Redaktionelle Anpassung diverser Hyperlinks in den Anhängen am 12. Januar 2022.

exportkontrollierte Informationsbestände (Risikoabschätzung in Rücksprache mit Auftraggeber/Partner oder Exportkontrolle empfohlen)	
Bibliotheksausleihdaten (Interessen- resp. Persönlichkeitsprofil des Ausleihenden erkennbar)	
personenbezogene Forschungsdaten, die nicht dem Humanforschungsgesetz unterliegen	
Lohndaten (Risikoabschätzung empfohlen)	
Revisionsstellenbericht, Audits	
Protokoll-, Nutzungs- und Verkehrsdaten zu E-Mail, Internet oder Intranet und Telefonie	
Lehr- und Lernplattformen (Leistungs- und Verhaltensdaten von Studierenden erkennbar)	
Self-Assessments	
Studierendenverwaltung, Prüfungsverwaltung	
Verfahrensinformationen	
Krisenstabsdokumente (Alarmorganisation, Notfallszenarien, BCM, Protokolle)	
Projektunterlagen: Anträge, Berichte, Protokolle	
besonders schützenswerte Personendaten sowie Persönlichkeitsprofile gemäss Art. 3 Datenschutzgesetz; ohne medizinische Gesundheitsdaten, die dem Humanforschungsgesetz unterliegen (Risikoabschätzung empfohlen: Personendaten, deren Missbrauch zu einer [erheblichen] Beeinträchtigung z.B. der wirtschaftlichen Situation oder der gesellschaftlichen Stellung führen kann, vgl. Risikostufen im Leitfaden)	
laufende Patentverfahren	
(persönliche) Passwörter	**streng vertraulich**
Intellectual Property (IP wie technische Erfindungen, Programm-Code, etc., wo eine Verpflichtung zur Geheimhaltung besteht) (Risikoabschätzung empfohlen)	
Informationen, die Personen direkt identifizieren (z. B. Tabellen mit Schlüssel, die zur De-Identifizierung eines Patienten durch Codierung / Pseudonymisierung verwendet werden)	
Forschungsdaten (vertraglich vereinbart, z.B. mit Kooperationspartner, Dritte)	
Interne Reorganisationsprojekte mit Personalabbau	
Daten, die unter das Berufsgeheimnis fallen sowie Patienten- und medizinische Daten, die unter das Berufsgeheimnis in der Forschung am Menschen oder unter das Humanforschungsgesetz* fallen (vgl. Art. 321** bzw. Art. 321bis Strafgesetzbuch) *falls Patienten- und medizinische Daten nicht irreversibel anonymisiert gemäss HFG-Verordnung Art. 25 oder explizit anders klassifiziert worden sind (Risikoabschätzung empfohlen) **Hinweis: Art. 321 gilt auch für Studierende, die ein Geheimnis offenbaren, das sie bei ihrem Studium wahrnehmen	
Forschungsergebnisse, die bei vorzeitiger Offenlegung schwerwiegenden Schaden anrichten können (Risikoabschätzung empfohlen, vgl. auch Anhang 1b)	
Informationen die gemäss Art. 162 StGB unter das Fabrikations- oder Geschäftsgeheimnis fallen (Risikoabschätzung empfohlen)	
Unternehmenskäufe, -gründungen	
hochsensible Personendaten (Risikoabschätzung empfohlen: Personendaten, deren Missbrauch das Leben der betroffenen Person gefährden kann; vgl. Risikostufen im Leitfaden)	

Anhang 1b: Klassifizierungsempfehlung (Vertraulichkeit) unter Beachtung von Risikobewertungen («Risikoabschätzung»)[28]

In untenstehender Liste finden sich Empfehlungen zur Klassifizierung der Vertraulichkeit ausgewählter Informationen nach Risikobewertung. Diese Empfehlung gilt vorbehältlich einer abweichenden (in der Regel höheren) Klassifizierung durch den/die Informationseigner*in. Bei Unklarheiten gibt der/die Information Security Officer Auskunft.

Es wird eine Risikobeurteilung nach dem Risikomanagement Handbuch der ETH Zürich empfohlen (vgl. Kapitel 6.3). Die Risikobeurteilung soll entlang folgenden Kategorien durchgeführt werden

- Finanzen
- Reputation
- geltendes Recht (z.B. Persönlichkeitsrechte)

Die Risikobeurteilung bezieht sich hierbei – wo angemessen – auf mindestens eines der folgenden Punkte:

- die ETH als Institution
- eines (oder mehrere) Departemente
- Einzelpersonen oder Gruppen von Personen (z.B. ETH-Angehörige aber auch Personen ausserhalb der ETH, die Daten der ETH zur Verfügung gestellt haben, z.B. Gesundheitsdaten zu Forschungszwecken)

Risikobewertung	Klassifikation
Information gilt als «nicht klassifiziert» im Sinne des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung (BGÖ) und/oder ist vom/von der Informationseigner/in zur Veröffentlichung freigegeben worden. Für Informationseigner/in: falls eine Risikobewertung zweckmässig erscheint, dann soll eine solche auch durchgeführt werden.	**öffentlich**
Höchstens **tiefes/geringes Risiko** für die ETH als Institution. Eine analoge Risikobewertung kann auch auf ein einzelnes (oder mehrere) Departement(e), auf Einzelpersonen oder Gruppen von Personen bezogen werden.	**intern**
Höchstens **mittleres/erhebliches Risiko** für die ETH als Institution. Eine analoge Risikobewertung kann auch auf ein einzelnes (oder mehrere) Departement(e), auf Einzelpersonen oder Gruppen von Personen bezogen werden. Beispiele: Der Vertraulichkeitsverlust kann nach sich ziehen (Konsequenzen):	**vertraulich**

[28] Fassung gemäss Schulleitungsbeschluss vom 12. Juli 2021, in Kraft seit 1. August 2021. Redaktionelle Anpassung der Hyperlinks am 12. Januar 2022.

- erhebliche finanzielle Schädigung oder erhebliche Rufschädigung - Verletzung Persönlichkeitsrechte z.B. gemäss Datenschutzgesetz	
Hohes/sehr hohes Risiko für die ETH als Institution. Eine analoge Risikobewertung kann auch auf ein einzelnes (oder mehrere) Departement(e), auf Einzelpersonen oder Gruppen von Personen bezogen werden. Beispiele: Der Vertraulichkeitsverlust kann nach sich ziehen (Konsequenzen): - schwerwiegende finanzielle Schädigung oder nachhaltige Rufschädigung - schwerwiegende juristische Konsequenzen (z.B. gemäss Strafgesetzbuch) - schwerwiegende Konsequenzen für Einzelpersonen oder Gruppen (Gesundheit, Leib und Leben)	**streng vertraulich**

Legende:
Die Angaben «tiefes/geringes», «mittleres/erhebliches» und «hohes/sehr hohes» Risiko richten sich nach der Farbgebung der im Risikomanagement Handbuch aufgeführten Risikotabellen. Analoges gilt für die Bedeutung von «erhebliche» und «schwerwiegende» Konsequenzen.

Anhang 1c: Empfehlungen für die Kennzeichnung von als vertraulich und streng vertraulich klassifizierter Informationen (Klassifizierungsvermerke)[29]

Klassifizierungsvermerke sind in Grossbuchstaben zu schreiben. Für als «öffentlich» oder «intern» klassifizierte Informationen muss kein Klassifizierungsvermerk angebracht werden.

- *für Word-Dokumente*: Verwendung eines Deckblatts mit der Kennzeichnung «VERTRAULICH» bzw. «STRENG VERTRAULICH». Die Kennzeichnung wiederholt sich auf jeder (Folge)-Seite (z.B. im Header/Footer). Vergleiche auch: Vorlagen mit Klassifizierungsvermerk. Analoges gilt auch für Excel-Sheets, Graphiken etc. sofern anwendbar

- *Video/Filme*: zu Beginn des Videos wird «VERTRAULICH» bzw. «STRENG VERTRAULICH» eingeblendet

- *Erstellen/Verwenden einer Datenbank*: beim Einloggen (Einstiegsbildschirm) z.B. einblenden: "Diese Daten sind «VERTRAULICH» bzw. «STRENG VERTRAULICH» (z.B. bei ETHIS)

[29] Fassung gemäss Schulleitungsbeschluss vom 12. Juli 2021, in Kraft seit 1. August 2021.

Anhang 2: Umgang mit klassifizierten Informationen (Vertraulichkeit)[30]

Der Umgang mit Informationen ist je nach Vertraulichkeitsstufe unterschiedlich zu handhaben. Bei Unklarheiten gibt der Information Security Officer Auskunft.

Generelle Vorgaben für klassifizierte Informationen

Umgang	öffentlich	intern	vertraulich	streng vertraulich
Klassifikation erfolgt	durch Informationseigner/in oder in dessen Auftrag			
Änderung der Klassifikation	nicht anwendbar	erfolgt durch den/die Informationseigner/in oder der übergeordneten Stelle		
Kennzeichnung der Klassifikation	nicht notwendig	nicht notwendig	als «vertraulich» markieren* *fakultativ für Forschungsdaten	als «streng vertraulich» markieren
Gewährung Zugriff / Vergabe Zugriffsrechte	keine Einschränkung	nur an Berechtigte	an verifizierbar Berechtigte (z.B. berechtigte Personengruppen)	an individuell Berechtigte, Eigner führt Liste der Berechtigten
Überprüfung Zugriffe / Zugriffsrechte	nicht anwendbar	nicht anwendbar	nach Bedarf	sofort bei Änderung von Zugriffsrechten oder Klassifikation

Informationen auf physischen Datenträgern (Papier, Film, Folie, etc.)

Umgang	öffentlich	intern	vertraulich	streng vertraulich
Bearbeitung	keine Einschränkung	Keine Einschränkung	Keine Einsichtnahme durch Unberechtigte	Keine Einsichtnahme durch Unberechtigte
Ablage/Aufbewahrung	keine Einschränkung	Clear Desk	Clear Desk, unter Verschluss halten	Clear Desk, nach Möglichkeit in Tresor
ETH-interne Weitergabe	keine Einschränkung	nur an Berechtigte	an verifizierbar Berechtigte (z.B. berechtigte Personengruppen)	an individuell Berechtigte, verschlüsselte Datenträger, Empfangsbestätigung, durch Eigner zu genehmigen, Geheimhaltungsvereinbarung

[30] Fassung gemäss Schulleitungsbeschluss vom 12. Juli 2021, in Kraft seit 1. August 2021.

Verwendung mit Dritten	keine Einschränkung	nur an Berechtigte, Geheimhaltungsvereinbarung* *fakultativ für Forschungsdaten	an verifizierbar Berechtigte (z.B. berechtigte Personengruppen), Geheimhaltungsvereinbarung* *fakultativ für Forschungsdaten	an individuell Berechtigte, verschlüsselte Datenträger, Empfangsbestätigung, durch Eigner/in zu genehmigen, Geheimhaltungsvereinbarung
irrtümlicher Erhalt	Absender informieren	Absender informieren	Absender informieren, unter Verschluss halten, nach Anweisung des Absenders retournieren oder vernichten	Absender informieren, unter Verschluss halten, nach Anweisung des Absenders retournieren oder vernichten
irrtümlicher Versand	Empfänger/in informieren	Empfänger/in informieren Vernichtung oder Retournierung anfordern	Informationseigner/in informieren nach Anweisungen des Informationseigners vorgehen Empfänger*in informieren	Informationseigner/in informieren nach Anweisungen des Informationseigners vorgehen Vorfall an CISO oder Rechtsdienst melden
Mitnahme Dienstreisen	erlaubt	erlaubt	vermeiden, wenn möglich, Vorsicht in ÖVs!	durch Eigner zu genehmigen, Vorsicht in ÖVs!
Mitnahme Home-Office	erlaubt	erlaubt	vermeiden, wenn möglich, Vorsicht in ÖVs!	durch Eigner zu genehmigen, Vorsicht in ÖVs!
Entsorgung / Vernichtung (Büro)	Altpapier/Abfall	Aktenvernichter Klasse 1[31]	Aktenvernichter Klasse 3[32], bei Vernichtung durch Dritte: schriftliche Bestätigung	Aktenvernichter Klasse 3[33], bei Vernichtung durch Dritte: schriftliche Bestätigung

[31] gemäss Norm DIN 66399
[32] gemäss Norm DIN 66399
[33] gemäss Norm DIN 66399

Elektronische Informationen

Umgang	öffentlich	intern	vertraulich	streng vertraulich
Bearbeiten am Bildschirm	keine Einschränkung	keine Einschränkung	keine Einsichtnahme durch Unberechtigte	keine Einsichtnahme durch Unberechtigte
Ablage auf ETH Fileserver	keine Einschränkung	keine Einschränkung	Gruppenlaufwerk mit entsprechend eingeschränkter Zugriffsberechtigung	Gruppenlaufwerk mit eingeschränkter Zugriffsberechtigung, es gilt ein sehr hoher Schutzbedarf, z.B. Verschlüsselung (vgl. Weisung IT-Richtlinien und IT-Grundschutzvorgaben)
Zugriff mittels privater IKT-Mittel auf ETH Daten (z.B. via PC, Smartphone)	erlaubt	nach Möglichkeit ETH-Infrastruktur verwenden* (*wo die Verwendung von ETH-Infrastruktur nicht möglich ist: für Zugriff via privater IKT-Mittel auf ETH-Accounts ist die Eingabe von ETH-Passwörtern erlaubt)		nicht erlaubt
Zugriff mittels öffentlich zugänglicher IKT-Mittel (z.B. Internet Cafe)	erlaubt	nicht erlaubt	nicht erlaubt	nicht erlaubt
ETH-interne Weitergabe	keine Einschränkung	nur an Berechtigte	an verifizierbar Berechtigte (z.B. berechtigte Personengruppen)	an individuell Berechtigte, Verschlüsselung, Empfangsbestätigung, durch Eigner/in zu genehmigen, Geheimhaltungsvereinbarung
Verwendung mit Dritten	keine Einschränkung	nur an Berechtigte, Geheimhaltungsvereinbarung* *fakultativ für Forschungsdaten	an verifizierbar Berechtigte (z.B. berechtigte Personengruppen), Geheimhaltungsvereinbarung* *fakultativ für Forschungsdaten	an individuell Berechtigte, Verschlüsselung, Empfangsbestätigung, durch Eigner/in zu genehmigen, Geheimhaltungsvereinbarung
irrtümlicher Erhalt (z.B. E-Mail)	Absender informieren	Absender informieren	Absender informieren, keine Weiterleitung, sofern möglich nach Anweisung des Absenders löschen	Absender informieren, keine Weiterleitung, sofern möglich nach Anweisung des Absenders löschen
irrtümlicher Versand (z.B. E-Mail)	Empfänger kontaktieren	Empfänger/in informieren Löschung anfordern	Informationseigner/in informieren nach Anweisungen des Informationseigners vorgehen Empfänger/in informieren	Informationseigner/in informieren nach Anweisungen des Informationseigners vorgehen Vorfall an CISO oder Rechtsdienst melden

irrtümlicher Erhalt (mobiler Datenträger)	Absender informieren	Absender informieren	Absender informieren, unter Verschluss halten, nach Anweisung des Absenders retournieren oder vernichten	Absender informieren, unter Verschluss halten, nach Anweisung des Absenders retournieren oder vernichten
irrtümlicher Versand (mobiler Datenträger)	Empfänger informieren	Empfänger/in informieren Vernichtung oder Retournierung anfordern	Informationseigner/in informieren nach Anweisungen des Informationseigners vorgehen Empfänger/in informieren	Informationseigner/in informieren nach Anweisungen des Informationseigners vorgehen Vorfall an CISO oder Rechtsdienst melden
Versand / Empfang mobiler Datenträger[34]	keine Einschränkung	ETH-intern: nur an Berechtigte ETH-extern: nur an Berechtigte Geheimhaltungsvereinbarung* *fakultativ für Forschungsdaten	ETH-intern: an verifizierbar Berechtigte, verschlüsselter Datenträger verschlossenes Behältnis ETH-extern: an verifizierbar Berechtigte, verschlüsselter Datenträger, verschlossenes Behältnis, Geheimhaltungsvereinbarung* *fakultativ für Forschungsdaten	Empfehlung: nach Möglichkeit auf Medium «mobiler Datenträger» verzichten. Wenn notwendig, dann: ETH-intern: an individuell Berechtigte, verschlüsselter Datenträger in verschlossenem Behältnis, Empfangsbestätigung, durch Eigner/in genehmigt, Geheimhaltungsvereinbarung ETH-extern: wie ETH-intern
Entsorgung / Vernichtung mobiler Datenträger	Abfall/Elektroschrott (umweltgerecht)	Aktenvernichter Klasse 1[35] bzw. Formatieren	Aktenvernichter Klasse 3[36] bzw. zerstören, bei Vernichtung durch Dritte: schriftliche Bestätigung	
ETH-externe Weiterverwendung/Verkauf/Donation PC[37]	keine Einschränkung	PC neu Aufsetzen	PC-internen Datenträger überschreiben/«wipen»[38] und neu Aufsetzen	

[34] z.B. CD/DVD/Blu Ray, USB, SSD/Flash Memory, Kameras, wechselbare Harddisks, etc.
[35] gemäss Norm DIN 66399
[36] gemäss Norm DIN 66399
[37] Personal Computer
[38] Ein Verfahren, das die Speicherzellen nur als gelöscht markiert, ist unzulässig.

Elektronische Informationen in Cloud-Dienste (zusätzliche «Cloud»-spezifische Vorgaben)

Umgang	öffentlich	intern	vertraulich	streng vertraulich
Personendaten nach Datenschutzgesetz (ohne medizinische Daten nach Humanforschungsgesetz)	keine Einschränkung	Möglich unter Einhaltung des Datenschutzgesetzes (DSG) und insbesondere auch der Einhaltung der Erläuterungen des EDÖB zu Cloud Computing: • Datenverarbeitung nur im Sinne von Art. 10a DSG • Cloud-Anbieter erfüllt Datensicherheit gemäss Art. 7, 8ff bzw. 20ff VDSG • Datenbekanntgabe ins Ausland nur bei Gewährleistung von Art. 6 DSG (siehe auch Stellungnahme, Erklärungen und Erläuterungen sowie Staatenliste und Mustervertrag des EDÖB) • nur bei Gewährleistung von Auskunftsrecht nach Art. 8 DSG und Recht auf Löschung und Berichtigung nach Art. 5 DSG • ggf. Anmelden von Datensammlungen Art. 11a • Risikoabschätzung notwendig*		nicht zulässig
Forschungsdaten nach den Regeln der Exportkontrolle	nicht anwendbar	Fallen Forschungsdaten unter die Regeln der Exportkontrolle und sind sie auch für das Ausland bestimmt, ist eine behördliche Bewilligung für das Hochladen auf einer Cloud zwingend notwendig. Die Bewilligung erteilt das SECO (via Exportkontrollstelle der ETH Zürich). Dasselbe gilt für Daten/Informationen, die auf Clouds hochgeladen werden, dessen Server zwar in der Schweiz ist, aber die Daten /Informationen für Empfänger im Ausland zugänglich gemacht werden (Deemed-Export).		
Sachdaten	keine Einschränkung	erlaubt mit Risikoabschätzung* (durch Informationseigner/in), entsprechender organisatorischer und allfällig notwendiger technischer Schutzmassnahmen, unter Beachtung bestehender Gesetzgebung (z.B. Exportkontrolle), vertraglicher Vereinbarungen sowie der Rechte Dritter (z.B. Persönlichkeits- oder Urheberrechte)		nicht zulässig

< weiter auf der nächsten Seite >

<table>
<tr><td rowspan="2">Kennzeichnung der Daten</td><td rowspan="2">nein</td><td>als «intern» markieren**
fakultativ für Forschungsdaten</td><td>als «vertraulich» markieren
**fakultativ für Forschungsdaten</td><td rowspan="2">nicht anwendbar</td></tr>
<tr><td colspan="2">Angabe, für welche Cloud-Dienste
die jeweilige Information bestimmt ist**
**fakultativ für Forschungsdaten</td></tr>
</table>

*unterstützendes Material (Template) ist beim CISO erhältlich