Weisung «Inventarisierung und Klassifizierung von Informationen an der ETH Zürich»

vom 01. Januar 2025

Der Chief Information Security Officer der ETH Zürich

gestützt auf Art. 6, Abs. 4, Bst. d und f der Weisung «Informationssicherheit an der ETH Zürich»[1]

v e r o r d n e t:

1. Abschnitt: Allgemeine Bestimmungen

Artikel 1 Gegenstand

[1] Diese Weisung regelt die Inventarisierung und Klassifizierung von Informationen.

[2] Inventarisierung ermöglicht es, eine Übersicht der Informationsbestände zu erhalten. Klassifizierung meint die Einordnung von Informationen in Klassen nach Vertraulichkeit, Integrität und Verfügbarkeit.

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.

2. Abschnitt: Inventarisierung

Artikel 3 Meldepflicht gegenüber dem/der ISO

[1] Die Informationseignerinnen und -eigner melden dem/der Information Security Officer (ISO) periodisch für ihren Verantwortungsbereich:

a. die Informationsbestände mit hohem und sehr hohem Schutzbedarf gemäss Art. 9 der vorliegenden Weisung und

[1] RSETHZ 203.25

[2] RSETHZ 201.021

b. die diesbezüglichen Sicherheitsmassnahmen.

Informationseignerinnen und -eigner meint Personen, die verantwortlich sind für die Informationsbestände, die durch sie oder in ihrem Auftrag erhoben und bearbeitet werden.

[2] Die/Der ISO führt ein Register der gemeldeten Informationsbestände und Sicherheitsmassnahmen.

3. Abschnitt: Klassifizierung von Informationen

Artikel 4 Grundsätze

[1] Informationen werden nach Vertraulichkeit, nach Integrität und nach Verfügbarkeit klassifiziert.

[2] Eine Klassifizierung richtet sich danach, wie stark ein Informationsbestand zu schützen ist (Schutzbedarf).

[3] Die Klassifizierung zeigt an, welchen Umgang die Informationseignerinnen und -eigner von den Benutzenden mit ihren klassifizierten Informationen erwarten.

Artikel 5 Zuständigkeiten

[1] Informationseignerinnen und -eigner sind für die Klassifizierung der in ihrem Verantwortungsbereich vorhandenen Informationen verantwortlich (klassifizierende Stelle).

[2] Klassifizierungen dürfen nur von der klassifizierenden oder einer dieser übergeordneten Stelle geändert werden.

[3] Benutzende bearbeiten Informationen im Auftrag der Informationseignerinnen und -eigner. Sie befolgen die Verhaltensregeln in den Anhängen dieser Weisung.

Artikel 6 Klassifizierungsstufen nach Vertraulichkeit

[1] Informationseignerinnen und -eigner klassifizieren die Informationen gemäss risiko-orientiertem Ansatz (vergleiche Anhang 1a):

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 der/die Informationseigner/in beizuziehen. Im Zweifelsfall ist eine Kommunikationsstelle der ETH Zürich zu konsultieren (departemental oder Hochschulkommunikation). Über die Veröffentlichung von Forschungsresultaten entscheidet, Vorbehalt

vertraglicher oder gesetzlicher Rechte Dritter, wie zum Beispiel Urheberrechte, der/die Informationseignerinnen und -eigner[3].

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[4] 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.

[2] Anhang 1b enthält Empfehlungen zur Klassifizierung ausgewählter Informationen.

Artikel 7 Klassifizierungsstufen nach Integrität

[1] Informationseignerinnen und -eigner klassifizieren die Integrität von Informationen gemäss risikoorientiertem Ansatz auf Aufforderung hin:

a. NORMALE Integrität: Mögliche Auswirkungen unbefugter oder unbeabsichtigter Veränderungen der Informationen sind für die Informationseignerinnen und -eigner akzeptabel (Auswirkungen nicht erheblich oder schwerwiegend). Zugriffsschutz und Back-up werden als ausreichende Sicherheitsmassnahmen zur Gewährleistung von normaler Integrität betrachtet.

Gilt als Standardwert für alle Informationen, die bezüglich Integrität nicht explizit als «hoch» eingestuft sind.

b. HOHE Integrität: Unbefugte oder unbeabsichtigte Veränderungen der Informationen sind für die Informationseignerinnen und -eigner nicht akzeptabel (Auswirkungen erheblich oder schwerwiegend). Sie müssen verhindert oder mindestens erkannt werden. Mögliche Beispiele sind Archive und die Webauftritte der ETH Zürich.

[3] ETH Gesetz, Art. 36 Abs. 2

[4] ETH Gesetz, Art. 13

Artikel 8 Klassifizierungsstufen nach Verfügbarkeit

[1] Informationseignerinnen und -eigner klassifizieren die Verfügbarkeit von Informationen gemäss risiko-orientiertem Ansatz auf Aufforderung hin:

a. NORMALE Verfügbarkeit: Einschränkungen beim Zugriff auf die Informationen oder ein vollständiger Verlust der Zugriffsmöglichkeiten während bis zu 3 Arbeitstagen[5] ist akzeptabel. Ein Verlust der seit der letzten Datensicherung durchgeführten Änderungen an den Informationen ist akzeptabel. Gilt als Standardwert für alle Informationen, die bezüglich Verfügbarkeit nicht explizit als «hoch» eingestuft sind.

b. HOHE Verfügbarkeit: Einschränkungen beim Zugriff auf die Informationen oder ein vollständiger Verlust der Zugriffsmöglichkeiten während maximal 12 Stunden pro Kalenderjahr, ist akzeptabel. Ein Verlust, der seit der letzten Datensicherung vor einem Vorfall durchgeführten Änderungen an den Informationen, ist akzeptabel oder zusätzliche Massnahmen zum Schutz vor Datenverlust sind erforderlich.

Artikel 9 Modalitäten

[1] Sind unterschiedliche Klassifizierungen auf eine Information anwendbar (z.B. aufgrund vertraglicher Vereinbarungen), so ist die strengere Klassifizierung anzuwenden bzw. der Schutzbedarf zu definieren.

[2] Für alle Informationen gilt das Need-to-Know-Prinzip. Sie dürfen berechtigten Personen bekanntgegeben werden, wenn dies notwendig ist.

[3] «Vertrauliche» und «streng vertrauliche» Informationen müssen einen Klassifizierungsvermerk tragen. Über die Kennzeichnung vertraulicher Forschungsdaten entscheiden die Informationseignerinnen und -eigner. Die Klassifizierungsvermerke (die Kennzeichnung klassifizierter Informationen) sind in Grossbuchstaben zu schreiben.

[4] Die Standard-Klassifizierung nach Vertraulichkeit an der ETH Zürich ist «intern». Dokumente ohne Klassifizierungsvermerk gelten als «intern». Veröffentlichte (publizierte) Informationen müssen nicht mit einem Klassifizierungsvermerk «öffentlich» gekennzeichnet werden.

[5] Die Klassifizierung von Informationen nach Vertraulichkeit erfolgt bei Erstellung der Information. Sie ist während des gesamten Lebenszyklus zu überprüfen. Die Klassifizierung nach Integrität und Verfügbarkeit hingegen erfolgt in der Regel auf Aufforderung hin (z.B. im Rahmen von IT-Projekten).

[6] Anhang 1a-c zeigen das risiko-orientierte Vorgehen zur Klassifizierung von Informationen nach Vertraulichkeit und enthalten Empfehlungen für die Klassifizierung nach Vertraulichkeit sowie Beispiele zur Kennzeichnung (Anbringen der Kennzeichnungsvermerke). Anhang 2 enthält Vorgaben für den Umgang mit nach Vertraulichkeit klassifizierten Informationen.

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

4. Abschnitt: Sicherheitsmassnahmen

Artikel 10 Schutzbedarf

[1] «Öffentliche» Informationsbestände haben keinen Schutzbedarf bezüglich Vertraulichkeit. Sie weisen jedoch mindestens einen normalen Schutzbedarf bezüglich Integrität und/oder Verfügbarkeit auf.

[2] Einen normalen Schutzbedarf haben Informationsbestände, die als «intern» gelten, eine normale Integrität und eine normale Verfügbarkeit aufweisen.

[3] Einen hohen Schutzbedarf haben Informationsbestände, die als «vertraulich» gelten oder eine hohe Integrität oder hohe Verfügbarkeit aufweisen.

[4] Einen sehr hohen Schutzbedarf haben Informationsbestände, die als «streng vertraulich» gelten.

[5] Gleiches gilt für Prozesse und IT-Mittel[6] die Informationsbestände mit einem analogen Schutzbedarf zu Abs. 1 bis 4 bearbeiten.

Artikel 11 Grundschutz und Standardisierung

[1] Der Grundschutz bietet hinreichend Schutz für den normalen oder hohen Schutzbedarf.

[2] Informationsbestände, Prozesse und IT-Mittel mit sehr hohem Schutzbedarf werden mit verschärften Mitteln gegen den Zugriff durch Unbefugte geschützt. Dies betrifft insbesondere auch den physischen Zutritt. Dafür werden standardisierte Sicherheitsmassnahmen umgesetzt. Diese Massnahmenpakete werden durch den/die CISO in Absprache mit den ISOs und den zuständigen IT-Betreibenden festgelegt.

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

[6] 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.

5. Abschnitt: Schlussbestimmungen

Artikel 12 Verantwortung für die Weisung

Diese Weisung wird durch den/die CISO periodisch überprüft.

Artikel 13 Inkrafttreten

Diese Weisung tritt am 01. Januar 2025 in Kraft.

Zürich, 01. Januar 2025

Johannes Hadodo
Chief Information Security Officer
ETH Zürich

Anhang 1a: Risiko-orientierte Klassifizierung von Informationen nach Vertraulichkeit

Folgend wird das empfohlene Vorgehen zur Klassifizierung der Vertraulichkeit von Informationen nach Risiko aufgezeigt. Das Vorgehen folgt den Leitlinien Risikomanagement der ETH Zürich (vgl. Kapitel 4.4). Der/die ISO gibt Auskunft.

Die Klassifizierung der Vertraulichkeit erfolgt entlang folgender Dimensionen

- Finanzielle Auswirkungen [CHF];
- Personenschäden;
- Beeinträchtigung der Reputation;
- Beeinträchtigung der Geschäftsprozesse (z.B. Lehr-, Forschungs-, Verwaltungstätigkeit);
- Auswirkungen auf die Umwelt und zusätzlich
- Beeinträchtigung der Persönlichkeitsrechte.

Die Risikobeurteilung geht vom «Credible Worst Case»-Szenario aus und bezieht sich auf die grösste Auswirkung / Beeinträchtigung aus:

- 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)

In der folgenden Tabelle ist zur Einschätzung der Vertraulichkeit der Informationen von einem «Credible Worst Case»-Szenario auszugehen. Es gilt der Farbcode:

- Grün: die Informationen sind als «intern» zu klassifizieren
- Gelb: die Informationen sind als «vertraulich» zu klassifizieren
- Rot: die Informationen sind als «streng vertraulich» zu klassifizieren

Dimensionen	sehr gering	gering	moderat	wesentlich	hoch	sehr hoch
Finanzielle Auswirkungen [CHF]	< 0.13 Mio.	0.13 – 1.13 Mio.	1.13 – 13.1 Mio.	13.1 – 66 Mio.	66 – 131 Mio.	> 131 Mio.
Personenschäden	Leichte Verletzung	Leichte Verletzung, ambulante Behandlung	Mittlere Verletzung, stationäre Behandlung	Schwerverletzte	Ab 10 bis 50 Schwerverletzte oder Tote	Mehr als 50 Schwerverletzte oder mehr als 10 Tote
Beeinträchtigung Reputation	Lokale Medienpräsenz	Nationale Medienpräsenz bis zu 1 Woche nicht flächendeckend	Nationale Medienpräsenz bis zu 1 Woche flächendeckend	Nationale und teilweise internationale Medienpräsenz Bis zu einem Jahr	Nationale und internationale Medienkampagne Bis mehrere Jahre	Internationale Medienkampagne bis mehrere Jahre, nachhaltiger Vertrauensverlust mit politischen Konsequenzen
Beeinträchtigung Geschäftsprozesse	½ Tag Ausfall nicht zentraler Funktionen	½ Tag Ausfall zentraler Funktionen	Ab ½ bis 2 Tage Ausfall nicht zentraler Funktionen	Ab ½ bis 2 Tage Ausfall zentraler Funktionen	Längerfristiger Ausfall nicht zentraler Funktionen	Längerfristiger Ausfall zentraler Funktionen
Auswirkungen auf die Umwelt	Lokaler Beeinträchtigung der Umwelt, keine Sanierungskosten	Regionale Beeinträchtigung der Umwelt, Sanierungszeit < 1 Woche, kleinere Sanierungskosten	Nationale Beeinträchtigung der Umwelt, Sanierungszeit < 1 Monat, mittlere Sanierungskosten	Nationale und teilweise internationale Beeinträchtigung der Umwelt, Sanierungszeit > 1 Monat, grosse Sanierungskosten	Nationale und internationale Beeinträchtigung der Umwelt, Sanierungszeit > 1 Jahr, sehr grosse Sanierungskosten	Internationale Beeinträchtigung der Umwelt, Sanierungszeit > 10 Jahre, immense Sanierungskosten
Beeinträchtigung Persönlichkeitsrechte [obigen Dimensionen gelten subsidiär]	Nicht sensible personenbezogene Daten, die keine besonders negativen Folgen für die betroffene Person haben – vorausgesetzt, sie werden nicht in einem sensiblen Kontext veröffentlicht.		Besonders schützenswerte Personendaten gemäss Schweizer Datenschutzgesetz Art. 5, die die Persönlichkeitsrechte von Einzelpersonen verletzen würden, wenn sie unzulässig offengelegt oder verarbeitet werden. Der Missbrauch solcher Informationen könnte zu erheblichen negativen Auswirkungen auf die wirtschaftliche und/oder soziale Stellung einer Person führen.		Informationen, die unter das Berufsgeheimnis gemäss Art. 321 bzw. Art. 321bis des Schweizerischen Strafgesetzbuches fallen, oder die bei unzulässiger Offenlegung oder Verarbeitung schwerwiegende Auswirkungen auf die Gesundheit und die wirtschaftliche Situation einer Person (Leib und Leben) haben würden.	

Anhang 1b: Klassifizierungsempfehlungen nach Vertraulichkeit

In untenstehender Liste finden sich Empfehlungen zur Klassifizierung ausgewählter Informationen. Diese gelten vorbehaltlich einer abweichenden (i.d.R. höheren) Klassifizierung durch die Informationseignerinnen und -eigner. Für die Klassifizierung soll insbesondere auch Anhang 1a berücksichtigt werden. Der/die ISO gibt 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)	
Projektunterlagen: Anträge, Berichte, Protokolle	
Anträge Schulleitung / Departement inkl. Protokolle; Konferenz- und Sitzungsunterlagen (z.B. von Professorenkonferenzen)	**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, Personalgespräche etc. (Religiöses, Politisches, Gewerkschaftliches, Gesundheitliches [z.B. Arztzeugnisse], Sozialhilfe, Strafrechtliche und Administrativrechtliche Verfolgung und Sanktionen)	
Leistungsbeurteilungen Studierende, Noten, Prüfungsunterlagen	
Verträge (Kooperationen, Drittfirmen, Forschung, Geheimhaltung)	
Netzwerkpläne der Informatik	
Forschungsdaten, Primär- und Sekundärdaten vor Veröffentlichung	
geplante und laufende Forschungsprojekte (inkl. Forschungsprojekte mit Drittparteien, soweit vertraglich nicht anders geregelt)	
Ergebnisse Umfragen	
Berater- und Lieferantenverträge	
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)	
besonders schützenswerte Personendaten und Profiling mit hohem Risiko gemäss Art. 5 Datenschutzgesetz sowie medizinische Gesundheitsdaten, die dem Humanforschungsgesetz unterliegen (Risikoabschätzung empfohlen vgl. insbesondere Anhang 1a und die Risikostufen im Leitfaden)	
laufende Patentverfahren	
Berufs-, Amts- und Geschäftsgeheimnisse (Risikoabschätzung empfohlen)	
Intellectual Property (IP wie technische Erfindungen, Programm-Code, etc., wo eine Verpflichtung zur Geheimhaltung besteht) (Risikoabschätzung empfohlen)	
Passwörter	
Passwörter mit sehr hohem Schutzbedarf (z.B. Administratoren-Passwörter)	**streng vertraulich**
Informationen, die direkt zur De-Identifizierung von Personen verwendet werden (z.B. Listen zur Codierung oder Pseudonymisierung von Patientennamen und Gesundheitsdaten)	
Forschungsdaten (sofern vertraglich als streng vertraulich vereinbart, z.B. mit Kooperationspartnern, Dritte)	
Interne Reorganisationsprojekte mit Personalabbau	
Patienten- und medizinische Daten, die unter das Berufsgeheimnis (vgl. Art. 321* bzw. Art. 321bis Strafgesetzbuch) oder unter das Humanforschungsgesetz** fallen (sofern gemäss Anhang 1a angezeigt) *Hinweis: Art. 321 gilt auch für Studierende, die ein Geheimnis offenbaren, das sie bei ihrem Studium wahrnehmen **falls Patienten- und medizinische Daten nicht irreversibel anonymisiert gemäss HFG-Verordnung Art. 25 sind	
Forschungsergebnisse, die bei vorzeitiger Offenlegung hoher/sehr hoher Schaden anrichten können (Risikoabschätzung empfohlen, vgl. auch Anhang 1a)	
Informationen die gemäss Art. 162 StGB unter das Fabrikations- oder Geschäftsgeheimnis fallen (Risikoabschätzung empfohlen)	
Unternehmenskäufe, -gründungen sofern bei vorzeitiger Offenlegung ein hoher/sehr hoher Schaden entstehen kann	
hochsensible Personendaten (Risikoabschätzung empfohlen: Personendaten, deren Missbrauch das Leben der betroffenen Person gefährden kann; vgl. Risikostufen im Leitfaden)	

Anhang 1c: Empfehlungen für die Kennzeichnung (Klassifizierungsvermerke)

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 «STRENG VERTRAULICH». Die Kennzeichnung für «VERTRAULICH» und «STRENG VERTRAULICH» wiederholt sich auf jeder (Folge)-Seite (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)

Anhang 2: Umgang mit klassifizierten Informationen (Vertraulichkeit)[1]

Der Umgang mit Informationen ist je nach Vertraulichkeitsstufe unterschiedlich zu handhaben. Bei Unklarheiten gibt der Information Security Officer Auskunft. Bei Datenverlust ist der/die zuständige Vorgesetzte und der/die CISO zu informieren. Bei Diebstahl zusätzlich die Abteilung SGU.

A. Generelle Vorgaben für klassifizierte Informationen

Umgang	öffentlich	intern	vertraulich	streng vertraulich
Klassifikation erfolgt	durch Informationseignerinnen und -eigner oder in deren Auftrag			
Änderung der Klassifikation	nicht anwendbar	erfolgt durch die Informationseignerinnen und -eigner oder der übergeordneten Stelle		
Kennzeichnung der Klassifikation	nicht notwendig	nicht notwendig	als «vertraulich» markieren* *fakultativ für Forschungsdaten	als «streng vertraulich» markieren
Vergabe Leserechte	keine Einschränkung	nur an Berechtigte (z.B. ETH-Angehörige dürfen prinzipiell auf alle internen Informationen zugreifen, sofern diese für den Zugriff freigeschaltet wurden)	an verifizierbar Berechtigte (z.B. berechtigte Personengruppen)	an individuell Berechtigte, Eigner führt Liste der Berechtigten
Überprüfung Leserechte	nicht anwendbar	nicht anwendbar	nach Bedarf	sofort bei Änderung von Zugriffsrechten oder Klassifikation

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

B. Informationen auf analog lesbaren Medien (z.B. Papier, Film, Folie, Tonband)

Umgang	öffentlich	intern	vertraulich	streng vertraulich
Bearbeitung	keine Einschränkung	Keine Einschränkung	Keine Einsichtnahme durch Unberechtigte	Keine Einsichtnahme durch Unberechtigte
Ablage/Aufbewahrung	keine Einschränkung	Clean Desk	Clean Desk, unter Verschluss halten	Clean Desk, nach Möglichkeit in Tresor
ETH-interne Weitergabe	keine Einschränkung	nur an Berechtigte	an verifizierbar Berechtigte (z.B. berechtigte Personengruppen)	an individuell Berechtigte, in verschlossenem Behältnis, Empfangsbestätigung, durch Eigner 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, in verschlossenem Behältnis, 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	Informationseignerinnen und -eigner informieren nach Anweisungen des Informationseigners vorgehen Empfänger*in informieren	Informationseignerinnen und -eigner 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[1]	Aktenvernichter Klasse 3[2], bei Vernichtung durch Dritte: schriftliche Bestätigung	Aktenvernichter Klasse 3[3], bei Vernichtung durch Dritte: schriftliche Bestätigung

C. Informationen auf entfernbaren digital lesbaren Datenträgern[4]

Umgang	**öffentlich**	**intern**	**vertraulich**	**streng vertraulich**
Ablage/Aufbewahrung	keine Einschränkung	Clean Desk	Clean Desk, unter Verschluss halten	Clean Desk, nach Möglichkeit in Tresor
Versand / Empfang	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 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
irrtümlicher Erhalt	analog wie Informationen auf analog lesbaren Medien			
irrtümlicher Versand	analog wie Informationen auf analog lesbaren Medien			
Mitnahme Dienstreisen	analog wie Informationen auf analog lesbaren Medien			
Mitnahme Home-Office	analog wie Informationen auf analog lesbaren Medien			

[1] gemäss Norm DIN 66399

[2] gemäss Norm DIN 66399

[3] gemäss Norm DIN 66399

[4] z.B. Lochkarten, Speicherkarten und (USB)-Sticks, externe Festplatten/SSDs oder Wechselfestplatten, CD/DVD, Disketten, die ohne grösseren zeitlichen Aufwand vom schreibenden bzw. lesenden Gerät entfernt werden können

Entsorgung / Vernichtung (Büro)	Abfall/Elektroschrott (umweltgerecht)	Aktenvernichter Klasse 1[1] bzw. Formatieren	Aktenvernichter Klasse 3[2] bzw. zerstören, bei Vernichtung durch Dritte: schriftliche Bestätigung

D. Elektronisch lesbare Informationen (mobile und stationäre IT-Mittel)

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 IT-Systeme 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 IT-Systeme auf ETH-Accounts ist die Eingabe von ETH-Passwörtern erlaubt		nicht erlaubt
		erlaubt	Zugriff nur via VPN	
Zugriff mittels öffentlich zugänglicher IT-Systeme (z.B. Internet-Café)	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

[1] gemäss Norm DIN 66399

[2] gemäss Norm DIN 66399

				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/in kontaktieren	Empfänger/in informieren Löschung anfordern	Informationseignerinnen und -eigner informieren nach Anweisungen des Informationseigners vorgehen Empfänger/in informieren	Informationseignerinnen und -eigner informieren nach Anweisungen des Informationseigners vorgehen Vorfall an CISO oder Rechtsdienst melden
ETH-externe Weiterverwendung/Verkauf/Donation PC[1]	keine Einschränkung	PC neu Aufsetzen		PC-internen Datenträger überschreiben/«wipen»[2] und neu Aufsetzen

[1] Personal Computer

[2] Ein Verfahren, das die Speicherzellen nur als gelöscht markiert, ist unzulässig.

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

<table>
<tr><th>Umgang</th><th>öffentlich</th><th colspan="2">intern</th><th>vertraulich</th><th>streng vertraulich</th></tr>
<tr><td>Personendaten nach Datenschutzgesetz (ohne medizinische Daten nach Humanforschungsgesetz)</td><td>keine Einschränkung</td><td colspan="3">Möglich unter Einhaltung des Datenschutzgesetzes (DSG) und insbesondere auch der Einhaltung der Vorgaben/Erläuterungen des EDÖB zu Cloud Computing:
• Datenverarbeitung nur im Sinne von Art. 9 DSG
• Cloud-Anbieter erfüllt Datensicherheit gemäss Art. 8 DSG bzw. 1 ff. DSV
• Datenbekanntgabe ins Ausland nur bei Gewährleistung von Art. 16 ff. DSG (siehe auch Stellungnahme, Erklärungen und Erläuterungen sowie Staatenliste EDÖB und Mustervertrag Datentransfer ins Ausland [SCC])
• nur bei Gewährleistung von Auskunftsrecht nach Art. 25 DSG und Recht auf Löschung und Berichtigung nach Art. 41 Abs. 2 DSG
• Verzeichnis der Bearbeitungstätigkeiten Art. 12 DSG
Risikoabschätzung notwendig*</td><td>nicht zulässig</td></tr>
<tr><td>Forschungsdaten nach den Regeln der Exportkontrolle</td><td>nicht anwendbar</td><td colspan="4">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).</td></tr>
<tr><td>Sachdaten</td><td>keine Einschränkung</td><td colspan="3">erlaubt mit Risikoabschätzung* (durch Informationseignerinnen und -eigner), 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)</td><td>nicht zulässig</td></tr>
<tr><td rowspan="2">Kennzeichnung der Daten</td><td rowspan="2">nein</td><td colspan="2">als «intern» markieren**
fakultativ</td><td>als «vertraulich» markieren
**fakultativ für Forschungsdaten</td><td rowspan="2">nicht anwendbar</td></tr>
<tr><td colspan="3">Angabe, für welche Cloud-Dienste die jeweilige Information bestimmt ist**
**fakultativ für Forschungsdaten</td></tr>
</table>

Nutzung externer Cloud-Dienste (z.B. Back-up Dienst)	Erlaubt, sofern der Dienst freigegeben ist und eine Einverständniserklärung des/der Informationseigenerinnen und -eigner vorliegt*.	nicht erlaubt

*unterstützendes Material (Template) ist bei dem/der CISO erhältlich