Benutzungsordnung für IT-Mittel an der ETH Zürich (BOT) und Anhang RSETHZ 203.21

Stand 17. Dezember 2024

1. Abschnitt: Allgemeine Bestimmungen 2
Artikel 1 Gegenstand 2
Artikel 2 Geltungsbereich 2

2. Abschnitt: Nutzung 3
Artikel 3 Grundsätze 3
Artikel 4 Private Nutzung von IT-Mitteln der ETH Zürich 3
Artikel 5 Nutzung privater IT-Geräte (bring your own device) 4
Artikel 6 Umgang mit geschäftlichen E-Mails 4
Artikel 7 Nutzung externer IT-Dienste (z.B. externe Cloud-Dienste) 5

3. Abschnitt: Grundschutzvorgaben für IT-Mittel 6
Artikel 8 Bildschirmsperre 6
Artikel 9 Identifizierung und Authentisierung 6
Artikel 10 Softwareaktualisierungen 6
Artikel 11 Deaktivieren von Sicherheitsfunktionen 7

4. Abschnitt: Monitoring, Datenaufzeichnung und -auswertung 8
Artikel 12 Grundsatz 8
Artikel 13 Aufzeichnung, Aufbewahrung und Auswertung von Daten 8

5. Abschnitt: Missbräuchliche Nutzung 10
Artikel 14 Missbräuchliche Nutzung 10
Artikel 15 Sichernde und vorsorgliche Massnahmen 11
Artikel 16 Konsequenzen bei Missbrauch 11

6. Abschnitt: Besondere Vorschriften 12
Artikel 17 Datenschutz 12
Artikel 18 Auftritt der ETH Zürich im Internet 12
Artikel 19 Weitere Vorschriften der Informationssicherheit 12

7. Abschnitt: Schlussbestimmungen 13
Artikel 20 Aufhebung bisherigen Rechts und Inkrafttreten 13

Anhang 1: Passwort- und PIN-Regeln 14

Die Schulleitung der ETH Zürich,

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

v e r o r d n e t:

1. Abschnitt: Allgemeine Bestimmungen

Artikel 1 Gegenstand

[1] Diese Benutzungsordnung («BOT») regelt die Grundsätze für die ordnungsgemässe Nutzung der IT-Mittel an der ETH Zürich (in der Folge «IT-Mittel» genannt). Sie ist auch anwendbar für ETH-fremde-Systeme, die Dienste im Datennetzwerk der ETH Zürich in Anspruch nehmen.

[2] 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.

Artikel 2 Geltungsbereich

[1] Diese Benutzungsordnung gilt für jede Nutzung von IT-Mitteln durch Benutzerinnen und Benutzer.

[2] Als Benutzerinnen oder Benutzer gelten die Angehörigen der ETH Zürich gemäss Art. 13 ETH-Gesetz (namentlich Mitarbeitende und Studierende) sowie Gäste gemäss Gästereglement[2].

[1] Organisationsverordnung ETH Zürich (RSETHZ 201.21)

[2] Gästereglement der ETH Zürich (RSETHZ 515.2)

2. Abschnitt: Nutzung

Artikel 3 Grundsätze

[1] IT-Mittel der ETH Zürich sind in erster Linie geschäftlich zu nutzen. Als «geschäftlich» gilt jede Nutzung von IT-Mitteln, die namentlich für Studienzwecke oder für die Aufgabenerfüllung im Rahmen des Anstellungsverhältnisses oder des Gastaufenthalts erfolgt. Als «privat» gilt jede andere Nutzung.

[2] IT-Mittel dürfen nur genutzt werden, soweit die Benutzerin oder der Benutzer dazu berechtigt ist. IT-Mittel sind rechtmässig, bestimmungsgemäss und sorgfältig zu nutzen. Benutzerinnen und Benutzer sind persönlich verantwortlich, dass ihre Nutzung von IT-Mittel namentlich keine Rechte Dritter verletzen (z.B. Urheber-, Lizenz- oder Persönlichkeitsrechte).

[3] Berechtigte Benutzerinnen oder Benutzer verwenden für Ihre Arbeit IT-Mittel, die von den IT-Betreibenden der ETH Zürich angeboten oder zugelassen werden. IT-Betreibende für die ETH Zürich sind namentlich die Informatikdienste, die IT Services Groups (ISG) der Departemente und der zentralen Organe sowie das CSCS und allenfalls Professuren mit eigener IT. IT-Betreibende verwalten, pflegen und entwickeln IT-Mittel weiter.

[4] Die/der Chief Information Security Officer (CISO) ist verantwortlich für die Steuerung der Informationssicherheit an der ETH Zürich.

Artikel 4 Private Nutzung von IT-Mitteln der ETH Zürich

[1] Die private Nutzung von IT-Mitteln der ETH Zürich[3] ist möglich, wenn die entsprechenden Bedingungen eingehalten werden (Art. 4 Abs. 5). Sie wird jedoch nicht empfohlen.

[2] E-Mail-Konti der ETH Zürich sollen nur für geschäftliche Zwecke genutzt werden. Für geschäftliche Korrespondenz ist die Verwendung des ETH-E-Mail-Kontos zwingend.

[3] Mit vorherigem Einverständnis[4] der Benutzerinnen und Benutzer dürfen private E-Mails gesendet werden. Private E-Mails werden von der ETH Zürich dann wie geschäftliche Korrespondenz behandelt (Speicherung; Löschung, ggf. Archivierung nach 10 Jahren etc.). Das Einverständnis ist nicht rückwirkend widerrufbar.

[4] Ausgenommen von dieser Einverständniserklärung ist die Nutzung von Leistungen, für die das E-Mail der ETH Zürich zwingend erforderlich ist, wie z.B. Vergünstigungen für ETH-Angehörige, und ebenso alle Kalendereinträge.

[5] Die private Nutzung von IT-Mitteln ist untersagt, wenn sie, insbesondere:
a. gegen Lizenzbestimmungen verstösst[5];
b. geltendes Recht verletzt;

---

[3] z.B. Nutzung des Browsers für private Zwecke

[4] Die Einwilligung kann gegeben werden unter: www.adressen.ethz.ch ("Personalien und Kommunikationsdaten" → Kommunikationsdaten)

[5] Lizenzbestimmungen sind über den ID Service Desk zu erfragen

c. übermässig, belästigend, beleidigend oder für die ETH Zürich rufschädigend ist;
d. kommerziellen Charakter hat;
e. eine technische Störung oder Beeinträchtigung verursacht oder
f. die Erfüllung von Arbeits- oder Studienpflichten beeinträchtigt.

[6] Die zeitgleiche Nutzung von ETH Zürich-lizenzierter Software zu Berufs- oder Studienzwecken auf dem Privat- und Bürocomputer ist untersagt, ausser die Lizenzbestimmungen erlauben dies explizit.

[7] Private, persönliche Inhalte von ETH-Angehörigen sind auf den öffentlichen ETH Zürich-Webseiten nicht zulässig[6]. Ausnahme bilden Lebensläufe, berufsbezogene Publikationen oder Ähnliches der Mitarbeitenden.

Artikel 5 Nutzung privater IT-Geräte (bring your own device)

[1] ETH-Angehörige und berechtigte Gäste, die private IT-Geräte für ihre Arbeit oder ihr Studium an der ETH Zürich verwenden, gelten für diese IT-Geräte als Systemverantwortliche. Es gelten die entsprechenden Weisungen[7]. Die für IT-Betreiber anwendbaren Weisungen, namentlich Art. 4 Abs. 5 dieser Benutzungsordnung, gelten. Wo die direkte Geltung nicht möglich ist, gelten sie sinngemäss.

[2] Private IT-Geräte werden insbesondere für die Multifaktor-Authentisierung auf IT-Systeme der ETH Zürich genutzt.

[3] Die Nutzung privater IT-Geräte durch Mitarbeitende der ETH Zürich (insbesondere Laptops und PCs) kann - abhängig von der Organisationseinheit - restriktiver gehandhabt werden.

[4] Streng vertrauliche Daten[8] dürfen mit privaten IT-Geräten weder gelesen, bearbeitet noch verwendet werden.

Artikel 6 Umgang mit geschäftlichen E-Mails

[1] Für elektronische Post (E-Mail) gilt die gesetzliche Aufbewahrungsdauer von 10 Jahren bis zur automatischen Löschung oder der Archivierung durch das Hochschularchiv der ETH Zürich[9].

[2] Der massenhafte Versand von Mitteilungen an alle ETH-Mitarbeitenden und/oder an alle Studierenden («Massenversand an alle») ist grundsätzlich untersagt. Es gelten folgende Ausnahmen, die vorgängig mit der Hochschulkommunikation abgesprochen werden müssen:

a. Absender sind die Präsidentin / der Präsident oder Mitglieder der Schulleitung; oder
b. es handelt sich um Umfragen oder ähnliche Versände, die vom Präsidenten / von der Präsidentin oder von einem Mitglied der Schulleitung bewilligt wurden.

Versände an Studierende richten sich primär nach den Vorschriften des Rektorats[10].

---

[6] RSETHZ 203.22 ETH Zürich: Web-Richtlinien

[7] z.B. «IT-Richtlinien und IT-Grundschutzvorgaben» (RSETHZ 203.23), «Protokollierung, Auswertung und Monitoring von Log-Daten» (RSETHZ 203.29)

[8] «Weisung Inventarisierung und Klassifizierung von Informationen an der ETH Zürich» (RSETHZ 203.28)

[9] Vgl. Kapitel 14, «Finanzreglement» (RSETHZ 245)

[10] Siehe «Richtlinien für die Unterstützung von schriftlichen und elektronischen Versänden an die Studierenden der ETH Zürich durch das Rektorat», abgelegt in der Weisungssammlung des Rektorats

[3] Zulässig sind «Massenversände an alle» ferner, wenn sie betriebs- oder studienbezogene Informationen beinhalten, die alle ETH-Mitarbeitenden oder Studierenden zwingend kennen müssen (z.B. Notfälle wie ausserordentliche Gebäudeschliessungen) oder die für ihre Tätigkeit an der ETH Zürich grundlegend sind (z.B. das Einrichten der Multifaktor-Authentifizierung).

[4] Betriebs- oder studienbezogene Massenversände innerhalb der eigenen Organisationseinheit (Departement, Schulleitungsbereich) sind zulässig und erfolgen durch die zuständigen Fachstellen.

[5] Betriebs- oder studienbezogene Massenversände ausserhalb der eigenen Organisationseinheit an mehr als 500 Adressatinnen oder Adressaten («Massenversand an viele») müssen vorher schriftlich beim Rektorat (Versände an Studierende) oder bei der Abteilung Hochschulkommunikation (Versände an Mitarbeitende) beantragt werden.

[6] Für Massenversände werden keine Adressdaten von ETH-Angehörigen an externe oder interne Anfragende herausgegeben. Versände an Studierende richten sich primär nach den Vorschriften des Rektorats.

[7] Newsletter, bei denen die Empfängerinnen oder Empfänger die Möglichkeit haben, sich an- und abzumelden, gelten nicht als elektronische Massenversände.

Artikel 7 Nutzung externer IT-Dienste (z.B. externe Cloud-Dienste)

[1] Die Nutzung externer IT-Dienste ist erlaubt, sofern diese Dienste von der ETH Zürich freigegeben[11] sind und das Einverständnis der Informationseignerinnen und -eigner zur Bearbeitung von deren Daten in diesen Diensten vorliegt.

[2] Die gelegentliche angemessene Nutzung externer IT-Dienste zur Unterstützung im Tagesgeschäft (z.B. Suchmaschinen, Online-Übersetzungsservices, Chatbots mit künstlicher Intelligenz, ChatGPT), die nicht von der ETH Zürich mittels Cloud-Assessment freigegeben sind, liegt in der Verantwortung der Benutzenden. Besonders schützenswerte Personendaten gemäss Datenschutzgesetz (DSG)[12] Art. 5 Bst. c sowie anderweitig vertrauliche oder streng vertrauliche (Sach- oder Personen) Daten dürfen mit solchen Diensten nicht bearbeitet werden.

[3] Einschränkend gilt, dass die Informationseignerinnen und -eigner[13] die Bearbeitung und Ablage ihrer Daten in der Cloud untersagen können. Im Zweifelsfall sind die Informationseignerinnen und -eigner zu kontaktieren.

[11] Link zum Verzeichnis freigegebener Cloud-Dienste

[12] Dies beinhaltet abschliessend Angaben zu Religion, Weltanschauung, Politik- oder Gewerkschaftsaktivität, Gesundheit, Intimsphäre, Rasse oder Ethnie, Genetik, Biometrie, Rechtsverfolgung, Sozialhilfe (massgebend ist der Gesetzestext)

[13] Informationseignerinnen/Informationseigner sind verantwortlich für die Daten, die durch sie oder in ihrem Auftrag erhoben und bearbeitet werden. Sie sind in der Regel Leitende mit Budgetverantwortung einer Organisationseinheit.

3. Abschnitt: Grundschutzvorgaben für IT-Mittel

Artikel 8 Bildschirmsperre

Unbeaufsichtigte IT-Mittel müssen grundsätzlich (auch kurzzeitig) durch eine zugangsgeschützte Bildschirmsperre/Gerätesperre gesichert werden. Dies wird auch für IT-Geräte von Studierenden oder Gästen empfohlen.

Artikel 9 Identifizierung und Authentisierung

[1] Grundsätzlich müssen sich Benutzerinnen und Benutzer von IT-Mitteln mit dem Benutzernamen (User ID) bzw. mit der E-Mail-Adresse der ETH Zürich identifizieren und authentisieren. Diese Daten von Benutzerinnen und Benutzern dürfen Dritten zur Authentisierung und Autorisierung elektronischer Services (namentlich Cloud-Diensten) bekanntgegeben werden.

[2] Identifikations- und Authentisierungsmittel wie Passwörter, PINs, Private Keys oder Chip-Karten sind persönlich und «streng vertraulich». Sie müssen geschützt aufbewahrt werden und die Anforderungen von Anhang 1 «Passwort- und PIN-Regeln» erfüllen. Die Bekannt- oder Weitergabe ist untersagt ausser bei zwingenden technischen Gründen.

[3] ETH-Stellen verlangen niemals die Bekanntgabe von Identifikations- und Authentisierungsmitteln. Solche Aufforderungen sind unrechtmässig. Sie stellen einen böswilligen Versuch dar (phishing), um unerlaubt an Daten der ETH Zürich zu gelangen. Sie sind umgehend dem zuständigen IT-Support[14] zu melden.

[4] Besteht die Vermutung eines Missbrauchs von Identifikations- und Authentisierungsmitteln durch Unbefugte, muss die Benutzerin oder der Benutzer den Zugriff umgehend sperren lassen und den Vorfall dem zuständigen IT-Support melden.

[5] Verwendet die Benutzerin oder der Benutzer einen verschlüsselnden Passwort-Manager, so muss das Passwort zum Öffnen des Managers den Regeln in Anhang 1 entsprechen. Sofern die technische Möglichkeit besteht, ist auch eine Multifaktorauthentisierung zu verwenden.

Artikel 10 Softwareaktualisierungen

[1] Patches und Updates sicherheitsrelevanter Aktualisierungen müssen so bald wie möglich (generell innerhalb von zwei Arbeitstagen) nach Verteilung durch den zuständigen IT-Support installiert und bei Bedarf durch einen Neustart des IT-Systems aktiviert werden. Dabei muss situationsbezogen auf den (wissenschaftlichen) Betrieb Rücksicht genommen werden, z.B. auf eine laufende Messreihe. Kurze Verlängerungen sind mit den zuständigen Systemverantwortlichen abzusprechen.

[2] Bei geplanter Abwesenheit ohne Möglichkeit zur Softwareaktualisierung muss ein IT-System heruntergefahren oder vom Netzwerk getrennt werden. Spätestens nach der Rückkehr ist die darauf installierte Software unmittelbar zu aktualisieren.

[3] Nachlässigkeiten können zur Ermahnung der Benutzerin/des Benutzers oder zum Ausschluss des betreffenden Geräts aus dem Datennetzwerk durch die/den CISO führen. Bei erfolgloser Ermahnung

[14] z.B. Service Desk der Informatikdienste oder IT Services Group

und bestehender technischer Möglichkeit, können sicherheitsrelevante Updates auch remote durch die/den zuständigen Systemverantwortlichen durchgeführt werden.

Artikel 11 Deaktivieren von Sicherheitsfunktionen

[1] Veränderungen an den von der ETH Zürich zur Verfügung gestellten IT-Mitteln (z.B. Virenschutzprogramme, lokale Firewalls oder Sicherheitseinstellungen) sind nur mit schriftlicher Zustimmung der jeweiligen zuständigen Systemverantwortlichen oder, im Fall externer IT-Dienste, mit schriftlicher Zustimmung der Service-Vermittelnden erlaubt.

[2] Die Ausschaltung, Umgehung oder Entfernung von Sicherheitsvorkehrungen bedürfen der vorgängigen Bewilligung der/des CISO.

4. Abschnitt: Monitoring, Datenaufzeichnung und -auswertung

Artikel 12 Grundsatz

[1] Die Aufzeichnung, Aufbewahrung und Auswertung von Daten sind erlaubt. Dies beinhaltet namentlich Inhaltsdaten oder Verkehrsdaten, die bei der Nutzung oder beim Betrieb von IT-Mitteln anfallen, wie z.B. Benutzeraktivitäten oder technische Sicherheitszustände.

[2] Ebenso dürfen Daten gesichert werden (z.B. im Rahmen von Backups).

[3] Die technische Prävention sowie die Sensibilisierung und Mitwirkung der ETH-Angehörigen hat hierbei Vorrang gegenüber einer Überwachung.

Artikel 13 Aufzeichnung, Aufbewahrung und Auswertung von Daten

[1] Benutzeraktivitäten und technische Sicherheitszustände der IT-Mittel dürfen aufgezeichnet bzw. protokolliert werden. Dabei dürfen Zugriffe und Änderungen protokolliert werden, beispielsweise das Speichern, Lesen, Verändern, Bekanntgeben, Löschen und Vernichten der Daten.

[2] Von E-Mails dürfen die Betreffzeile, Datum, Zeit, Absender- und Empfängeradressen protokolliert werden. Bei einer Auswertung von E-Mail-Verkehr wird im Normalfall keine Einsicht in den Inhalt privater E-Mails genommen. Wenn die Unterscheidung zwischen privaten und geschäftlichen E-Mails unklar ist, darf die ETH Zürich davon ausgehen, dass das E-Mail geschäftlich ist.

[3] Personendaten, die bei der Nutzung oder beim Betrieb von IT-Mitteln anfallen oder Protokolle dürfen zu folgenden Zwecken aufgezeichnet und ausgewertet werden[15]:

a. nicht personenbezogen:

1. zur Aufrechterhaltung der Informations- und Dienstleistungssicherheit	(2 J.);
2. zur technischen Wartung der IT-Mittel	(2 J.);
3. zur Kontrolle der Einhaltung von Nutzungsreglementen	(2 J.);
4. zum Nachvollzug des Zugriffs auf Datensammlungen	(2 J.);
5. zur Erfassung der Kosten, die durch die Benutzung der elektronischen Infrastruktur entstehen	(2 J.);
6. bei Daten über die Arbeitszeiten des Personals: zur Bewirtschaftung der Arbeitszeit	(5 J.);
7. bei Daten über das Betreten oder Verlassen von Gebäuden und Räumen und den Aufenthalt darin: zur Gewährleistung der Sicherheit	(3 J.).

[15] Art. 57l ff. Regierungs- und Verwaltungsorganisationsgesetz (RVOG; SR **172.010**) i.V.m. Art. 4 f. Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen vom 22. Februar 2012 (SR **172.010.442**); siehe ferner die Weisung «Protokollierung, Auswertung und Monitoring an der ETH Zürich» (RSETHZ 203.29).

b. **stichprobenweise nicht namentlich personenbezogen** (z.B. pseudonymisiert):
   1. zur Kontrolle der Nutzung von IT-Mitteln (2 J.);
   2. zur Kontrolle der Arbeitszeiten des Personals (5 J.).

c. **personenbezogen**:
   1. zur Abklärung eines konkreten Verdachts auf Missbrauch von IT-Mitteln oder Ahndung eines erwiesenen Missbrauchs (2 J.);
   2. zur Analyse und Behebung von Störungen der elektronischen Infrastruktur und Abwehr konkreter Bedrohungen dieser Infrastruktur (2 J.);
   3. zur Bereitstellung benötigter Dienstleistungen (2 J.);
   4. zur Erfassung und Fakturierung erbrachter Leistungen (2 J.);
   5. zur Kontrolle der individuellen Arbeitszeiten (5 J.).

Die erlaubte Aufbewahrungsdauer von Personendaten, einschliesslich Protokollen (Logdaten) ist in Klammern angegeben; spätestens danach werden die Daten gelöscht. Kürzere Aufbewahrungsdauern sowie Abs. 4 und 5 sind vorbehalten. Für Personaldossiers und medizinische Personaldaten gelten Art. 59 ff. Personalverordnung ETH-Bereich[16] (Personaldossier: Aufbewahrungsdauer 10 Jahre).

[4] Zur Abklärung eines konkreten Verdachts auf Missbrauch von IT-Mitteln oder Ahndung eines erwiesenen Missbrauchs (oben Absatz 3 Buchstabe c Ziffer 1) dürfen Daten ohne schriftliche Information der betroffenen Person gesichert werden. Die Aufbewahrungsdauer gemäss Absatz 3 Buchstabe c Ziffer 1 gilt in diesem Fall nicht. Die personenbezogene Auswertung der sichergestellten Daten ist nur nach schriftlicher Information der betroffenen Person über den Verdacht oder Missbrauch erlaubt[17].

[5] Besteht ein konkreter Verdacht auf das Vorliegen strafbarer Handlungen, so werden die massgeblichen Daten zuhanden der zuständigen Strafbehörde gesichert. Weitere personenbezogene Auswertungen obliegen allein der Strafbehörde. Der Entscheid, ob Anzeige gegen fehlbare Mitglieder des Lehrkörpers oder Mitarbeitende der ETH Zürich erstattet wird, liegt bei dem Präsidenten/der Präsidentin der ETH Zürich.[18]

[6] Benutzerinnen und Benutzer sind, soweit zulässig, verpflichtet, bei der Aufklärung von Missbrauch oder von finanziellen Schadensfällen mitzuwirken.

[7] Für die Bearbeitung und Aufbewahrung von Daten, die in den elektronischen Personal- und Studieninformationssystemen gemäss Art. 36a und 36b ETH-Gesetz aufgezeichnet werden, gelten die Ausführungsbestimmungen des ETH-Rates[19] bzw. der Schulleitung der ETH Zürich.

---

[16] Personalverordnung ETH-Bereich (PVO-ETH; SR **172.220.113**)

[17] Art. 57o Abs. 1 Bst. a Regierungs- und Verwaltungsorganisationsgesetz (RVOG; SR **172.010**) i.V.m. Art. 11 Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen vom 22. Februar 2012 (SR **172.010.442**).

[18] Art. 14 Abs. 2 Geschäftsordnung der Schulleitung vom 10. August 2004 (RSETHZ 202.3).

[19] Personendatenschutzverordnung ETH-Bereich, PDV-ETH (SR **172.220.113.42)**

5. Abschnitt: Missbräuchliche Nutzung

Artikel 14 Missbräuchliche Nutzung

[1] Missbräuchlich ist jede Nutzung von IT-Mitteln der ETH Zürich, die die Vorschriften dieser Benutzungsordnung missachtet, gegen übergeordnetes Recht verstösst (namentlich Berufspflichten verletzt, z.B. zur Integrität in der Forschung) oder Rechte Dritter verletzt.

[2] Insbesondere gelten die folgenden Verhaltensweisen als missbräuchlich und sind verboten:

a. die Verarbeitung, Speicherung oder Übermittlung von Material mit widerrechtlichem oder unsittlichem Inhalt, wie z.B. Gewaltdarstellungen, Pornographie[20], Aufforderung zu Verbrechen oder Gewalttätigkeit[21], Störung der Glaubens- und Kultusfreiheit[22] oder Diskriminierung und Aufruf zu Hass[23];

b. die Herstellung, die Anleitung zur Herstellung oder absichtliche Verbreitung von schädlichen Programmen oder Programmteilen im Sinne von Art. 144bis Ziff. 2 StGB (Viren, Würmer, Trojaner etc.). Die Herstellung und Anleitung zur Herstellung solcher Programme zu Zwecken der Lehre und Forschung ist erlaubt, wenn angemessene Vorkehrungen gegen ihre schädigende Verwendung getroffen werden;

c. das unbefugte Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB „Hacking“): Ausspionieren von Passwörtern, unautorisiertes Absuchen von internen und externen Netzwerken auf Schwachstellen (z.B. Port-Scanning), Vorkehrung und Durchführung von Massnahmen zur Störung von Netzwerken und Computern (z.B. Denial of Service Attacks). Das „Hacking“ in einer abgeschotteten Umgebung zu Zwecken der Lehre und Forschung ist erlaubt;

d. das Versenden von Mitteilungen mit irreführenden Absenderangaben oder Inhalten (z.B. betrügerische E-Mails wie Phishing, CEO-Fraud etc.). Begründete Ausnahmen sind nur erlaubt, wenn sie für Lehre und Forschung zwingend erforderlich sind und von angemessenen Massnahmen der Transparenz begleitet werden[24];

e. Unbefugte Datenbeschaffung (Art. 143 StGB) und Datenbeschädigung (Art. 144bis Ziff. 1 StGB);

f. die Nutzung von IT-Mitteln der ETH Zürich in absichtlicher Verletzung von Lizenzbestimmungen oder Urheberrechten;

g. die Belästigung Angehöriger der ETH Zürich oder Dritter durch Mitteilungen (z.B. mit beleidigenden, sexistischen, rassistischen, rufschädigenden oder diskriminierenden Inhalten) namentlich durch Inhalte, die im Widerspruch zum «Verhaltenskodex Respekt[25]» der ETH Zürich stehen;

h. der Verstoss gegen die Vorschriften zum Massenversand gemäss Art. 6;

i. das Einrichten von nicht zugewiesenen Direktanschlüssen an die ETH Zürich-Kommunikationsnetze (z.B. durch WLAN Access Points) ohne vorgängige schriftliche Zustimmung der Informatikdienste und der jeweiligen Systemverantwortlichen.

---

[20] Art. 197 Strafgesetzbuches (StGB; SR **311.0**)

[21] Art. 259 StGB

[22] Art. 261 StGB

[23] Art. 261bis StGB

[24] z.B. nachträgliche Information Betroffener oder Offenlegung der Umstände in der wissenschaftlichen Publikation

[25] Verhaltenskodex Respekt bzw. https://respekt.ethz.ch/verhaltenskodex.html

[3] Als schwer gilt:

a. Missbrauch gemäss Strafgesetzbuch, namentlich Abs. 2 Bst. a, b, c, d, soweit dieser vorsätzlich bzw. absichtlich erfolgt;
b. vorsätzliche Zuwiderhandlung gegen Art. 10 oder
c. anderer Missbrauch im Wiederholungsfall.

[4] Die Kenntnis schweren Missbrauchs verpflichtet die direkten Vorgesetzten, die IT-Betreibenden sowie die Service-Vermittelnden zur Meldung an die/den CISO.

Artikel 15 Sichernde und vorsorgliche Massnahmen

Wird eine erhebliche Beeinträchtigung der ordentlichen Nutzung von IT-Mitteln der ETH Zürich oder eine Schädigung der ETH Zürich, ihrer Angehörigen oder Dritter befürchtet oder sind diese wahrscheinlich oder eingetreten, dürfen folgende sichernde und vorsorgliche Massnahmen angeordnet werden:

a. Sperrung des Zugangs zu IT-Mitteln, von denen ein festgestellter Missbrauch ausgeht oder die davon betroffen sind;
b. Blockierung von Daten sowie
c. deren Sicherung und Aufbewahrung zu Beweiszwecken.

Artikel 16 Konsequenzen bei Missbrauch

[1] Wird ein Missbrauch oder der konkrete Verdacht eines Missbrauchs gemäss Art. 14 festgestellt, so kann die/der CISO involvierte Personen anhören und/oder die folgenden Massnahmen anordnen:

a. Abmahnung leichter Verstösse;
b. vorsorgliche Sperrung des Zugangs zu IT-Mitteln, die davon betroffen sind;
c. Blockierung missbräuchlicher und/oder rechtswidriger Daten;
d. Entfernung oder Löschung missbräuchlicher und/oder rechtswidriger Daten;
e. Sicherung und Aufbewahrung von Daten zu Beweiszwecken.

[2] Ferner kann die/der CISO die fehlbaren Benutzerinnen und Benutzer vorübergehend oder dauerhaft mit der Sperrung des Zugangs zu IT-Mitteln, mit einer Nutzungseinschränkung oder einem Nutzungsverbot belegen.

[3] Gegen fehlbare Benutzerinnen und Benutzer können zudem disziplinarische oder personalrechtliche Massnahmen ergriffen[26], ein Zivilverfahren (Schadenersatzklage) eingeleitet oder Strafanzeige erstattet werden[27]. Für Mitarbeitende gilt jede Art des Missbrauchs als Verletzung der arbeitsrechtlichen Pflichten[28]. Schwere Fälle gemäss Art. 14 Abs. 3 können zur Entlassung führen.

[4] Die durch Missbrauch und dessen Folgen, einschliesslich der Aufklärung und Sanktionierung, verursachten Kosten (Untersuchungs-, Gerichts- und Anwaltskosten eingeschlossen), kann die ETH Zürich auf fehlbare Benutzerinnen und Benutzer überwälzen.

---

[26] Studierende: gemäss Art. 2 ff. Disziplinarverordnung ETH Zürich vom 10.11.2020 (SR **414.138.1**);
Mitarbeitende: gemäss Art. 58a Personalverordnung ETH-Bereich vom 15.3.2001 (PVO-ETH; SR **172.220.113**).

[27] Vgl. Art. 22a Bundespersonalgesetz (BPG; SR **172.220.1**).

[28] Art. 25 Bundespersonalgesetz (SR **172.220.1**) bzw. Art. 53 PVO-ETH

6. Abschnitt: Besondere Vorschriften

Artikel 17 Datenschutz

[1] Bei der Bearbeitung von Personendaten sind die rechtlichen Vorgaben des Datenschutzes einzuhalten. Namentlich gelten Art. 36a-36f ETH-Gesetz[29].

[2] Verletzungen der Datensicherheit mit Bezug zu Personendaten («data breaches») sind der Datenschutzberaterin oder dem Datenschutzberater umgehend, spätestens aber 72 Stunden nach Entdeckung, zu melden (Mailadresse: ds@ethz.ch).

[3] Die ETH Zürich hat eine/n Datenschutzberaterin/Datenschutzberater. Die Datenschutzseite des Rechtsdienstes gibt weitere Informationen zum Datenschutz[30].

Artikel 18 Auftritt der ETH Zürich im Internet

Die Hochschulkommunikation erlässt die Ausführungsbestimmungen[31] für den Auftritt der ETH Zürich und ihrer Organisationseinheiten in online-Medien.

Artikel 19 Weitere Vorschriften der Informationssicherheit

[1] Es gelten insbesondere:

a. die «Weisung Informationssicherheit an der ETH Zürich[32]
b. für System- und Netzwerkzonenverantwortliche: die Weisung IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich[33];
c. für Informationseignerinnen/Informationseigner: die Weisung zur «Inventarisierung und Klassifizierung von Informationen»[34];
d. für Service-Vermittelnde und Informationseignerinnen/Informationseigner im Rahmen der Nutzung externer Cloud-Dienste: die Weisung «IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich»[35]
e. für System- und Netzwerkzonenverantwortliche sowie Service-Vermittelnde die Weisung «Protokollierung, Auswertung und Monitoring von Log-Daten»[36]

[2] Benutzerinnen und Benutzer selbstverwalteter IT-Mittel, beispielsweise Professuren mit eigener IT, nehmen die Rolle der Systemverantwortlichen wahr.

---

[29] siehe auch Datenschutzgesetz (DSG, SR **235.1)** und -verordnung (DSV, SR **235.11**), situativ auch EU-Datenschutz-Grundverordnung (DSGVO); Regelungen des ETH-Bereichs wie Personendatenschutzverordnung ETH-Bereich (PDV-ETH), Vorgaben des eidg. Datenschutzbeauftragten EDÖB (www.edoeb.admin.ch).

[30] https://ethz.ch/staffnet/de/service/rechtliches/datenschutz.html

[31] z.B. Web-Richtlinien (RSETHZ 203.22), Social-Media-Richtlinien (RSETHZ 203.24) , Richtlinien über die Verwendung des Logos (RSETHZ 202.4)

[32] RSETHZ 203.25

[33] RSETHZ 203.23

[34] RSETHZ 203.28

[35] RSETHZ 203.23

[36] RSETHZ 203.29

7. Abschnitt: Schlussbestimmungen

Artikel 20 Aufhebung bisherigen Rechts und Inkrafttreten

[1] Die Benutzungsordnung für Informations- und Kommunikationstechnologie an der ETH Zürich vom 19. April 2005 (BOT; RSETHZ 203.21) wird aufgehoben.

[2] Diese Verordnung tritt am 01. Januar 2025 in Kraft.

Zürich, 17. Dezember 2024

Im Namen der Schulleitung:

Der Präsident: Prof. Dr. Joël Mesot
Die Generalsekretärin: Katharina Poiger Ruloff

Anhang 1: Passwort- und PIN-Regeln

1. Passwörter

a. Passwörter müssen schwer zu erraten sein. Namen, Geburtsdaten, Telefonnummern, Buchstaben- und Zahlenfolgen, unveränderte Einträge aus Wörterbüchern oder ähnliche leicht zu erratene Begriffe, dürfen nicht verwendet werden.
b. Sofern technisch möglich, müssen Passwörter mindestens:

- 12 Zeichen lang sein. Ausnahme: Für das Netzwerk der ETH Zürich (RADIUS-Authentisierung) ist eine Länge von 10 Zeichen ausreichend;
- Mindestens drei der folgenden Kategorien enthalten
  - Grossbuchstaben
  - Kleinbuchstaben
  - Zahlen
  - Sonderzeichen

c. Bei einem Passwortwechsel muss ein neues, bisher nicht verwendetes Passwort gewählt werden.
d. Das Passwort für das "virtual private network" - VPN - der ETH Zürich (VPN mit RADIUS-Authentisierung) muss verschieden von jedem der anderen Passwörter sein, z.B. von der Anmeldung in Windows etc.
e. Ein im privaten Umfeld eingesetztes Passwort darf nicht für ein Benutzerkonto an der ETH Zürich eingesetzt werden und umgekehrt.
f. Vom Hersteller voreingestellte Passwörter müssen unmittelbar nach Inbetriebnahme der IT-Mittel geändert werden. Initialpasswörter, die beispielsweise bei der Eröffnung eines neuen Benutzerkontos vergeben werden, müssen bei der ersten Nutzung des Benutzerkontos geändert werden.
g. Bei Missbrauch eines Benutzerkontos oder bei Verdacht auf Missbrauch muss das betroffene Passwort von einem sicheren IT-System aus unmittelbar gewechselt werden.
h. Ändert sich der Kreis der für den Zugriff auf ein geteiltes Benutzungskonto (wo ein Passwort geteilt werden muss) berechtigten Personen, ist das Passwort zu ändern, sofern dies technisch möglich ist.

2. PINs

a. Kommen PINs zum Schutz von IT-Mitteln zum Einsatz, müssen diese, sofern technisch möglich, mindestens 6-stellig sein.
b. PINs müssen schwer zu erraten sein. Geburtsdaten, Zahlenfolgen (wie 123456) oder Wiederholungen (z.B. 111111) sind nicht erlaubt.
c. Bei Missbrauch oder Verdacht auf Missbrauch, muss die betroffene PIN gewechselt werden.
d. Beim Wechsel einer PIN muss eine neue, bisher nicht verwendete PIN gewählt werden.
e. Vom Hersteller voreingestellte PINs müssen unmittelbar nach Inbetriebnahme der IT- Systeme geändert werden.
f. Ändert sich der Kreis der Personen, die mit einer gemeinsamen PIN arbeiten, ist die PIN zu ändern, sofern dies technisch möglich ist.