Benutzungsordnung für Informations- und Kommunikationstechnologie an der ETH Zürich (BOT) und Anhang

(Teilrevision Stand 1. Mai 2022)

Benutzungsordnung für Informations- und Kommunikationstechnologie an der ETH Zürich[1]

(BOT)

vom 19. April 2005 (Stand 1. Mai 2022)

Die Schulleitung der ETH Zürich,

gestützt auf Art. 4 Abs. 1 Bst. c 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 Informations- und Kommunikationstechnologie-Mittel (IKT-Mittel) der ETH Zürich sollen in optimaler Weise für die Erfüllung der Aufgaben der ETH Zürich eingesetzt werden.

[2]Die ordnungsgemässe Nutzung der IKT-Mittel der ETH Zürich soll sichergestellt und der störungsfreie Betrieb der IKT-Mittel gewährleistet werden.

Artikel 2 Begriffe[3]

[1] *IKT-Mittel* (Ressourcen) umfasst alle Mittel der Informations- und Telekommunikationstechnologie, die im Eigentum der ETH Zürich sind oder im Auftrag der ETH Zürich eingesetzt werden. Es handelt sich insbesondere um Systeme, Einrichtungen und Dienste , die zur elektronischen Bearbeitung von Daten eingesetzt werden (z.B. Datenverarbeitungsanlagen, Netzwerkkomponenten, Datenspeicher, Drucker, Scanner, Telekommunikationsnetze und auf diesen Mitteln laufende Software, Schliesssysteme oder durch die ETH Zürich ausgelagerte Dienstleistungen wie Cloud-Lösungen). Ferner beinhaltet der Begriff nicht ETH Zürich-eigene Systeme (z.B. private Laptops) im Datennetz der ETH Zürich. Ausgenommen ist die Videoüberwachung gemäss ETH-Gesetz[4].

[2] Unter *Systeme* sind IKT-Mittel zu verstehen.

[3] *Daten* bedeuten Personen- und Sachdaten.

[1] Ersatz eines Ausdrucks: im ganzen Erlass wird der Ausdruck «Telematik» durch «Informations- und Kommunikationstechnologie» bzw. durch die Abkürzung «IKT» ersetzt. Sinngemäss wird im ganzen Erlass der Ausdruck «Telematik-Mittel» durch «Informations- und Kommunikationstechnologiemittel» bzw. «IKT-Mittel» ersetzt.

[2] RSETHZ 201.021

[3] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.

[4] Art. 36i ETH-Gesetz

[4] *Benutzer* sind alle Angehörigen der ETH Zürich (Art. 13 ETH-Gesetz) und Dritte, die zur Nutzung von IKT-Mitteln der ETH Zürich berechtigt sind (z.B. Gäste[5], Kongressteilnehmer, angeschlossene Organisationen, Bibliothekskunden an den öffentlichen Arbeitsplätzen, Mitarbeitende von Spin-off Unternehmen der ETH Zürich oder anderen Unternehmen, sofern eine entsprechende vertragliche Vereinbarung vorliegt, emeritierte Professoren und pensionierte Mitarbeitende).

[5] *Elektronische Kommunikationsmittel* beinhalten Telefon, Fax, E–Mail, SMS, Instant Messaging, Videokonferenzsysteme und Ähnliches.

[6] *Organisationseinheiten* sind von der Schulleitung gemäss Organisationsverordnung ETH Zürich (OV) vom 16.12.2003[6] errichtete zentrale oder dezentrale Organe der ETH Zürich (z.B. Departemente, Institute, Abteilungen[7], Stabsstellen, selbständige Professuren) sowie Lehr- und Forschungseinrichtungen ausserhalb der Departemente gemäss Art. 61 OV.

[7] *Privat* ist jede Nutzung von IKT-Mitteln oder elektronischen Kommunikationsmitteln der ETH Zürich, die nicht für Studienzwecke oder für die Aufgabenerfüllung im Rahmen des Anstellungsverhältnisses erfolgt.

[8] *Anonyme Auswertung* meint die statistische Analyse der Protokollierungen, welche keine personenbezogene Auswertung zulässt.

[9] *Pseudonyme oder nicht personenbezogene Auswertung* meint die Protokollierungsanalyse pseudonymisierter, bestimmbarer Personen. Das Pseudonym muss die Identität der betroffenen Person in der Phase der nicht personenbezogenen Überwachung schützen[8].

[10] *Protokollierung* ist die fortlaufende Aufzeichnung von Verkehrsranddaten (Adressierungsdaten im Kopf von elektronischen Nachrichten, Informationen zum Sessionsaufbau gemäss technischem Kommunikationsprotokoll und Ähnlichem) der IKT-Mittel.

[11] Service-Vermittelnde, System- und Netzwerkzonenverantwortliche[9] sind die in den *IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich[10]* und in Artikel 6 dieses Erlasses definierten Fachpersonen.

[12] Chief Information Security Officer (CISO) ist die Person, die gemäss Art. 5 Weisung Informationssicherheit an der ETH Zürich[11] hochschulweit für die Gewährleistung der Informationssicherheit zuständig und verantwortlich ist. Sie arbeitet dafür mit den Stellen gemäss Art. 6-11 Weisung Informationssicherheit an der ETH Zürich zusammen.[12]

Artikel 3 Geltungsbereich[13]

Diese Verordnung gilt für jede Nutzung von IKT-Mitteln durch Benutzer (Begriffe siehe Art. 2 Abs. 2 und 4), d.h., sie gilt sowohl für jede Benutzung und Mitbenutzung aller ETH Zürich-eigenen IKT-Mittel oder für IKT-Mittel, die im Auftrag der ETH Zürich eingesetzt werden (z.B. ausgelagerte Dienstleistungen wie Cloud-Lösungen), als auch für nicht ETH Zürich-eigene Systeme, die aber im Datennetzwerk der ETH Zürich betrieben werden, und zwar durch **ETH Zürich-Angehörige** oder **Dritte**.

[5] Vgl. Weisung des Vizepräsidenten für Personal und Ressourcen vom 13. November 2018 betreffend den Gast-Aufenthalt an der ETH Zürich (RSETHZ 515.2).
[6] RSETHZ 201.021
[7] Redaktionelle Anpassung.
[8] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.
[9] Ersatz eines Ausdrucks: im ganzen Erlass wird der Ausdruck «Netzanschlussverantwortlicher» durch «Netzwerkzonenverantwortlicher» ersetzt.
[10] RSETHZ 203.23
[11] RSETHZ 203.25
[12] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[13] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.

2. Abschnitt: Zuständigkeiten

Artikel 4 Abteilung Informatikdienste, Informatiksupportgruppen und CSCS[14]

[1] Die Abteilung Informatikdienste (nachfolgend *Informatikdienste*) der ETH Zürich erbringt Informatikdienstleistungen für die einzelnen Benutzer und Organisationseinheiten der ETH Zürich. Sie ernennt dazu einen IT Security Officer Informatikdienste (ITSO ID) gemäss Art. 8 Weisung Informationssicherheit an der ETH Zürich. Die Informatikdienste sind im Bereich der IT-Sicherheit (Teil der Informationssicherheit) insbesondere zuständig für[15]:

a) die Umsetzung technischer Massnahmen zur Gewährleistung der IT-Sicherheit der IKT-Mittel und Services, die sie für die zentralen und dezentralen Organisationseinheiten der ETH Zürich betreiben, einschliesslich der Feststellung und Behebung von Sicherheitsmängeln;

a[bis]) die ETH Zürich-weite technisch-operative Überprüfung von IKT-Mitteln[16] auf Sicherheitsmängel im Auftrag des CISOs und die Information an die für deren Behebung Verantwortlichen. Überprüfungen ausgelagerter IKT-Mittel erfolgen im Rahmen der jeweiligen vertraglichen Bestimmungen und sinnvoll umsetzbaren Prüfmöglichkeiten.

a[ter]) Auswahl und Betrieb der für diese Prüfungen notwendigen technischen Lösungen, wobei deren Einsatz gemäss den Vorgaben des CISO angeordnet werden darf;

b) die Instruktion und Information der Benutzer zwecks Behebung erkannter Sicherheitsmängel;

c) die Erarbeitung der *IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich* sowie die technisch-operative Überwachung von deren Einhaltung im Auftrag des CISO zuhanden des Vizepräsidenten für Infrastruktur und der/des CISO[17];

d) die Koordination bei der Umsetzung technischer und organisatorischer Neuerungen;

e) die Bereitstellung der notwendigen Verschlüsselungstechniken (Art. 13 Abs. 2) gemäss den Vorgaben der/des CISO;

f) die ihr gemäss Weisung Informationssicherheit an der ETH Zürich[18] obliegenden Aufgaben im Bereich der Informationssicherheit;

g) das Erteilen von Ausnahmen gemäss Art. 15[bis] zur Integrität des IKT-Netzwerks gemäss den Vorgaben der/des CISO;

h) *aufgehoben;*

i) den Informationsaustausch innerhalb der ETH Zürich und des ETH-Bereichs sowie zwischen den Hochschulen, SWITCH und den Bundesstellen, sofern nicht gemäss Art. 5 Weisung Informationssicherheit an der ETH Zürich[19] durch den/die CISO abgedeckt;

[14] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.
[15] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[16] Gemäss Definition nach Art. 2 Abs. 1 sind ausdrücklich ETH- und nicht ETH-eigene IKT-Mittel gemeint.
[17] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021. Hinweis: die bisher bestehenden Dokumente *IT Best Practice Rules* und *Standards für Verantwortlichkeiten und Systempflege* (RSETHZ 203.23) wurden zu einem neuen Dokument *IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich* (RSETHZ 203.23) zusammengefasst.
[18] RSETHZ 203.25, namentlich Art. 10
[19] RSETHZ 203.25

j) die Unterstützung der/des CISO[20] bei der Wahrnehmung von deren/dessen Aufgaben gemäss den Regeln zur *Überwachung der Nutzung von IKT-Mitteln an der ETH Zürich* im Anhang sofern diese nicht von anderen Stellen (z.B. Informatiksupportgruppen oder das CSCS) erbracht wird;

k) *aufgehoben*;

l) die Abklärung der Zulässigkeit einer kommerziellen Nutzung der IKT-Mittel und das Abschliessen entsprechender Verträge (Art. 8 Abs. 6).

m) *aufgehoben*[21]

[2] Die Informatiksupportgruppen in den Departementen sind, mit Ausnahme der in den Buchstaben a[bis], a[ter], c, i und g beschriebenen Aufgaben, innerhalb ihres Verantwortungsbereichs im Wesentlichen für dieselben Aufgaben zuständig.

[3] Das Swiss National Supercomputing Center (CSCS) ist in seiner Funktion als nationales Zentrum, mit Ausnahme der in den Buchstaben a[bis] , a[ter], c und g beschriebenen Aufgaben, für die Erbringung von Leistungen auf dem Gebiet des Hochleistungsrechnens zuständig.

Artikel 5 Chief Information Security Officer (CISO)[22]

[1] Zur Gewährleistung der Informationssicherheit verfügt die ETH Zürich über eine/n CISO. Diese/r hat die Aufgaben und Kompetenzen gemäss Art. 5 Weisung Informationssicherheit an der ETH Zürich[23]. Sie/er ist fachlich unabhängig, organisatorisch im Bereich des Präsidenten angegliedert und erstattet Bericht an die Risikomanagement Kommission (RMK) der ETH Zürich.

[2-5] *aufgehoben*

Artikel 6 Verantwortlichkeiten und Schutzbedarfsfeststellung[24]

[1] Für alle IKT-Mittel gibt es eine verantwortliche Person und mindestens eine Stellvertretung, namentlich Service-Vermittelnde für jeden ausgelagerten IKT-Service, Systemverantwortliche für jedes IKT-Mittel im Datennetz der ETH Zürich und Netzwerkzonenverantwortliche für jede Netzwerkzone des Datennetzes der ETH Zürich.

[2] Jede Organisationseinheit bestimmt die verantwortlichen Personen für ihre IKT-Mittel im Datennetz der ETH Zürich, ihre Netzwerkzonen, sowie für die durch sie bezogenen ausgelagerten IKT-Services. Diesbezügliche Umsetzungsbestimmungen, inkl. der Möglichkeiten der Delegation an Dienstleister (z.B. IT-Betreiber), sind in den *IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich* geregelt.

[2bis] Bei nicht ETH-eigenen Systemen, die im Datennetz der ETH Zürich betrieben werden («Bring Your Own Device», BYOD und selbstverwaltete Systeme), gilt der angemeldete Benutzer gegenüber der ETH Zürich als Systemverantwortlicher, wenn für die Abteilung Informatikdienste kein Administrator des Systems ansprechbar ist.

[3] IT-Betreiber der ETH Zürich sind namentlich die Informatikdienste, das CSCS, die Informatiksupportgruppen der Departemente (ISG).[25] Die IT-Betreiber legen aufgrund der Meldungen der zuständigen Information Security Officer (ISO)[26] fest, welche IKT-Mittel Daten mit hohem Schutzbedarf im Sinne von Art. 16 und 23 Abs. 1 Weisung Informationssicherheit an der ETH Zürich bearbeiten.

---

[20] Die Funktionsbezeichnung «IT-Sicherheitsbeauftragte» wird im ganzen Dokument durch «CISO» ersetzt (vgl. Art. 2 Abs. 12).
[21] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[22] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[23] RSETHZ 203.25
[24] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.
[25] IT-Betreiber gemäss Art. 3 Abs. 4 Weisung Informationssicherheit an der ETH Zürich (RSETHZ 203.25)
[26] Art. 6 Weisung Informationssicherheit an der ETH Zürich

[4] Die/der Systemverantwortliche, respektive der/die Service-Bezieher/in, hat insbesondere folgende Aufgaben:

a) Sie/er stuft den Schutzbedarf für ETH-eigene Systeme oder ausgelagerte IKT-Services ein, die nicht von einem IT-Betreiber betreut werden.
b) Sie/er ist verantwortlich für die Einhaltung und zuständig für die Umsetzung der *IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich*[27].
c) Sie/er meldet Sicherheitsprobleme, Defekte etc. unverzüglich an die zuständigen Stellen bei den Informatikdiensten oder den Informatiksupportgruppen.
d) Sie/er löscht vor Weitergabe oder Entsorgung von Datenträgern (Harddisk u.ä.) die darauf vorhandenen Daten der ETH Zürich (Anhang zur BOT Ziffer 1 Abs. 7).

[5] Weitere Aufgaben, Kompetenzen und Verantwortlichkeiten der Netzwerkzonenverantwortlichen, Systemverantwortlichen und Service-Vermittelnde sind in Art. 17 und Art. 18 sowie im Anhang der BOT geregelt. Zudem sind die *IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich* zu beachten[28].

[6] *aufgehoben*

Artikel 7 Präsenz im Intranet / Internet[29]

[1] Für den Auftritt der ETH Zürich und ihrer Organisationseinheiten im Internet bzw. Intranet ist die Hochschulkommunikation zuständig. Sie erlässt dafür die entsprechenden Ausführungsbestimmungen.[30]

[2] Dabei trägt die Hochschulkommunikation den Bestimmungen der Behindertengleichstellung[31] angemessen Rechnung.

[3] Kommerzielle Werbung ist untersagt. Über Ausnahmen entscheidet der Präsident/die Präsidentin. Das Erwähnen von Sponsoren bleibt von dieser Regel ausgenommen.

[28] RSETHZ 203.23
[29] Fassung gemäss Schulleitungsbeschluss vom 17. September 2013, in Kraft seit 1. Oktober 2013.
[30] Web-Richtlinien der ETH Zürich vom 1. September 2016 (RSETHZ 203.22) und Social-Media-Richtlinien der ETH Zürich vom 26. Februar 2013 (RSETHZ 203.24).
[31] Behindertengleichstellungsgesetz vom 13. Dezember 2002 (BehiG; SR **151.3**); Behindertengleichstellungsverordnung, vom 19 November 2003 (BehiV; SR **151.31**).

3. Abschnitt: Nutzung

Artikel 8 Nutzungszweck und Nutzungsbefugnis[32]

[1] Die Nutzung von IKT-Mitteln ist für diejenigen Zwecke erlaubt, für welche die IKT-Mittel dem Benutzer zur Verfügung gestellt werden („bestimmungsgemässe Nutzung"). Vorbehalten bleiben Anwendungen, die einer ausdrücklichen Bewilligung bedürfen.

[2] Die Benutzer haben ihre Nutzung der IKT-Mittel auf das im Rahmen der erlaubten Nutzungszwecke angemessene Mass zu beschränken.

[2bis] Die Mitarbeitenden der ETH Zürich sind für die Pflege ihres E-Mail-Postfachs verantwortlich.[33]

[3-4] *aufgehoben*

[5] Allgemeine Veränderungen durch die Benutzer an den von der ETH Zürich zur Verfügung gestellten IKT-Mitteln, insbesondere Eingriffe in und Veränderungen an Software, sind nur mit schriftlicher Zustimmung des zuständigen Systemverantwortlichen oder im Fall von ausgelagerten IKT-Services, mit schriftlicher Zustimmung des Service-Beziehers / der Service-Bezieherin erlaubt. Ausgenommen sind Veränderungen im Rahmen der ordentlichen Nutzung der IKT-Mittel.

[5bis] Die Ausschaltung, Umgehung oder Entfernung von verbindlichen Sicherheitsvorkehrungen bedürfen der vorgängigen Bewilligung der/des ITSO ID im Auftrag der/des CISO. Die diesbezüglichen Ausführungsbestimmungen sind in den *IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich* festgelegt.

[6] Spinoff-Firmen der ETH Zürich haben grundsätzlich eigene IKT-Mittel zu gebrauchen. Die kommerzielle Nutzung von IKT-Mitteln der ETH Zürich (z.B. im Rahmen von Spin-Off-Verträgen) ist grundsätzlich nicht erlaubt. Ausnahme ist die Netzwerkanbindung in einer Netzwerkzone der ETH Zürich. Allfällige Kosten werden den betreffenden Kunden verrechnet.[34]

[6bis] Betrieb und Nutzung von Hochleistungsrecheninfrastruktur am CSCS oder die Nutzung von IKT-Mitteln im Rahmen einer Forschungskooperation wird vertraglich geregelt.

[7] In Bezug auf die Aussonderung von IKT-Mitteln im Eigentum der ETH Zürich gelten ferner Art. 134 Finanzreglement der ETH Zürich[35] sowie Ziff. 8 der Wegleitung für die Inventarführung an der ETHZ[36] vom Januar 2019.

Artikel 8bis Private Nutzung[37]

[1] Die Nutzung von IKT-Mitteln der ETH Zürich, insbesondere E-Mail und Internet für private Zwecke ist grundsätzlich erlaubt, soweit sie nicht

a. übermässig ist,
b. die Erfüllung der Arbeits- oder Studienpflichten beeinträchtigt oder verletzt,
c. gegen die schweizerische Rechtsordnung (insbesondere gegen Bestimmungen des Strafgesetzbuches) oder Rechte Dritter (Persönlichkeitsrechte, Urheberrechte) verstösst,
d. einen kommerziellen Charakter hat oder
e. für die ETH Zürich rufschädigend ist.

[32] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.
[33] Fassung gemäss Schulleitungsbeschluss vom 7. April 2022, in Kraft seit 1. Mai 2022.
[34] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[35] Finanzreglement der ETH Zürich vom 1. Januar 2019 (RSETHZ 245).
[36] abrufbar unter ETH Zürich > Finanzen und Controlling > Downloads (zuletzt 21.01.2019).
[37] Fassung gemäss Schulleitungsbeschluss vom 7. April 2022, in Kraft seit 1. Mai 2022.

[2] Den ETH-Angehörigen wird die Nutzung von IKT Mitteln der ETH Zürich zu privaten Zwecken jedoch nicht empfohlen, da die ETH Zürich bei privaten Sachverhalten die Privatsphäre nicht vollständig gewährleisten kann. Über IKT-Mittel der ETH Zürich erhaltene oder versandte private E-Mails oder bearbeitete private Dokumente werden technisch wie geschäftliche Korrespondenz der ETH Zürich behandelt.

[3] Die Pflege des eigenen E-Mail Postfachs gemäss Art. 8 Abs. 2[bis] beinhaltet das Löschen privater E-Mails oder deren Verschieben in einen allenfalls vom Systemverantwortlichen bereitgestellten «Privat»-Ordner, wenn ETH Angehörige vermeiden wollen, dass diese langfristig im Sinne von Absatz 4 zwischengespeichert und später allenfalls dauerhaft archiviert werden. Im von der Abteilung Informatikdienste zur Verfügung gestellten E-Mailsystem muss dieses Löschen oder Verschieben von E-Mails innert 60 Tagen nach Erstellung oder Erhalt eines E-Mails erfolgen.

[4] Nach Absatz 3 im geschäftlichen Postfach verbleibende E-Mails gelten als geschäftlich relevant für die ETH Zürich. Sie werden nach spätestens 60 Tagen gesichert und während mindestens 10 Jahren sicher und unveränderbar aufbewahrt. Mit Ablauf dieser Frist werden sie gemäss dem Bundesgesetz über die Archivierung[38] und Art. 4 Reglement für das Archiv der ETH Zürich[39] dem Archiv der ETH Zürich zur dauerhaften Archivierung angeboten. Vom Archiv der ETH Zürich als nicht-archivwürdig resp. als redundant bewertete E-Mails[40] werden gelöscht.

[5] Benötigt die/der ETH-Angehörige seine/ihre geschäftlichen E-Mails über die 10 Jahre hinaus weiterhin für geschäftliche Zwecke, so muss sie/er beim Systemverantwortlichen die Aussetzung des Löschprozesses beantragen.

[6] Weiter darf die private Nutzung nicht zu einer technischen Störung oder Beeinträchtigung der Nutzung für die gesetzlichen Aufgaben der ETH Zürich oder zu einer unverhältnismässigen Beanspruchung oder Belastung von allgemein genutzten Ressourcen (Netzwerke, Internetzugang, Speicherplatz etc.) führen.

[7] Private, persönliche Inhalte von ETH-Angehörigen sind, mit Ausnahme von Lebensläufen, Publikationen o.ä. der Forschenden, auf den öffentlichen ETH-Webseiten nicht zulässig. Für die Einrichtung von persönlichen Webseiten können die Informatikdienste zentral entsprechende Systeme zur Verfügung stellen.

[8] Die berufliche Nutzung von zu Hause aus («Home-Office-Nutzung») von an der ETH Zürich-lizenzierter Software ist erlaubt für Mitarbeitende der ETH Zürich in einem Beschäftigungsgrad von mindestens 50% sowie für an der ETH Zürich immatrikulierte Studierende, soweit dies der jeweilige Lizenzvertrag zulässt[41]. Die Einräumung des Rechts, die Software auf einem privaten Computer zu installieren und die Art der Softwareverwendung (z.B. allfälliges Recht zur auch privaten Nutzung), ist vom jeweiligen Lizenzvertrag abhängig. Die gleichzeitige Nutzung von an der ETH Zürich-lizenzierter Software auf dem Privat- und Bürocomputer ist untersagt, ausser die Lizenzbestimmungen erlauben dies explizit.[42]

[38] SR **152.1**

[39] RSETHZ 420.1

[40] Gemäss Bewertungsentscheid des Archivs der ETH Zürich vom 31. August 2021 sind namentlich die E-Mails der Schulleitungsmitglieder und der/des Generalsekretärs/in archivwürdig. Archivwürdig sind Unterlagen, die von besonderer juristischer oder administrativer Bedeutung sind oder einen grossen Informationswert haben.

[41] Erläuterndes Hilfsblatt der Abt. Informatikdienste unter https://www.softwareinfo.ethz.ch/home-use-of-eth-software/ , zuletzt abgerufen 24. Januar 2021. Massgebend sind die jeweiligen Lizenzbedingungen.

[42] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.

Artikel 9 Nutzung von IKT-Mitteln ausserhalb der ETH Zürich[43]

[1] Erbringt eine Mitarbeiterin oder ein Mitarbeiter die Arbeitsleistung im Einvernehmen mit der zuständigen Stelle zu Hause, so soll sie/er dafür IKT-Mittel der ETH Zürich nutzen[44].

[2] Der Einsatz von portablen ETH Zürich eigenen Systemen wie Laptops, Smartphone etc. ausserhalb des ETH Zürich Campus ist erlaubt. Dabei sind die *IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich* zu beachten.

Artikel 10 Private Nutzung von ETH Zürich lizenzierter Software[45]

aufgehoben

Artikel 11 Datenschutz[46]

[1] Die Bearbeitung von Personendaten[47] ist nur im Rahmen der gesetzlichen Zwecke der ETH Zürich sowie nach Massgabe der Datenschutzbestimmungen[48] erlaubt.

[2] Personendaten von Benutzern dürfen Dritten zur Autorisierung und Authentisierung von elektronischen Services (namentlich Cloud-Diensten) bekanntgegeben werden, soweit es sich nicht um besonders schützenswerte Daten[49] handelt und diese Personendaten für die Benutzung dieser Services notwendig sind.

[3] Massenversände an ETH-interne Adressaten **ausserhalb** der eigenen Organisationseinheit für Informationszwecke erfolgen auf schriftlichen Antrag durch das Rektorat oder die Informatikdienste (im Auftrag HK/HR). Vorbehalten bleiben Massenversände im Auftrag der Schulleitung oder interdepartementale Ankündigungen von Seminaren o.ä (z.B. Seminarinformationen D-INFK/D-MATH, Schulungsinformationen der SGU).

[4] Beim Einsatz von Web Analyse Programmen (z.B. Google Analytics) sind die Vorgaben des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zu beachten.[50]

[5] Fragen des Datenschutzes ganz allgemein sind an den Rechtsdienst zu richten.

Artikel 12 Kopien von Software[51]

aufgehoben

Artikel 13 Nutzung elektronischer Kommunikationsmittel[52]

[1] Die Vertraulichkeit des Nachrichtenversands über IKT-Mittel ist nicht gewährleistet.

---

[43] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.

[44] Im Sinne von PVO Art. 43. Der Arbeitgeber stellt den Arbeitnehmenden zur Erfüllung der Arbeitsleistung die entsprechenden IKT-Mittel zur Verfügung.

[45] Fassung gemäss Schulleitungsbeschluss vom 17. September 2013, in Kraft seit 1. Oktober 2013.

[46] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.

[47] Personendaten sind gemäss Legaldefinition des Datenschutzgesetzes vom 19. Juni 1992 (DSG; SR **235.1**) alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen.

[48] Datenschutzgesetz vom 19. Juni 1992 (DSG; SR **235.1**); Datenschutzverordnung vom 14. Juni 1993 (VDSG; SR **235.11**); Art. 59 f. Personalverordnung ETH-Bereich (PVO-ETH; SR **172.220.113**). Weiter gelten Art. 36a bis 36e ETH-Gesetz (SR **414.110**), die Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen (SR **172.010.442**) sowie die Richtlinien über den Schutz und den Umgang von Personaldaten der ETH Zürich (RSETHZ 612).

[49] Daten im Sinne von Art. 3 lit. c Datenschutzgesetz (SR **235.1**).

[50] www.edoeb.admin.ch. Bei Fragen sind der Rechtsdienst oder die HK zu kontaktieren.

[51] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.

[52] Fassung gemäss Schulleitungsbeschluss vom [SL-Datum NEU], in Kraft seit 1. Juni 2021.

[2] Berufs-, Amts- und Geschäftsgeheimnisse oder andere vertrauliche Informationen[53] aus dem Bereich der ETH Zürich (z.B. aus Personalakten) sind mittels sicherer IKT-Mittel zu übermitteln, insbesondere mit geeigneter Verschlüsselungstechnik, sofern verfügbar.

[3] IKT-Mittel dürfen nicht anonym, unter einem Pseudonym oder unter falschem Absender benutzt werden.

4. Abschnitt: Sicherheitsmassnahmen

Artikel 14 Systeme mit normalem Schutzbedarf[54]

[1] Systeme mit **normalem Schutzbedarf** sind Systeme mit Daten gemäss Art. 23 Abs. 2 Weisung Informationssicherheit an der ETH Zürich, für die Grundschutzmassnahmen gemäss Art. 19 Abs. 1 Weisung Informationssicherheit an der ETH Zürich ausreichend sind.

[2] *aufgehoben*[55]

[3] *aufgehoben*

Artikel 14bis Zugriffsschutzmassnahmen[56]

[1] Die Benutzer halten die persönlichen Zugriffsberechtigungsmittel und Identifikationsmethoden wie Passwörter, PINs, Private Keys, Chip-Karten, physische Schlüssel, Tokens etc. geheim. Deren Bekanntgabe oder das Zugänglichmachen für Dritte, insbesondere für andere Benutzer, ist untersagt.

[2] Besteht die Vermutung, dass ein Identifikations[57]- oder Zugangsmittel der ETH Zürich Unbefugten bekannt oder zugänglich gemacht wurde oder von diesen genutzt wird, muss der Benutzer den Zugang bzw. Zugriff umgehend sperren lassen und den Vorfall dem zuständigen IT-Support melden.

[3] Die zuständigen Stellen der ETH Zürich verlangen niemals auf elektronischem Weg die Bekanntgabe von Zugriffsmitteln. Erhält der Benutzer eine solche Aufforderung, handelt es sich um einen böswilligen Versuch, an vertrauliche Daten zu gelangen (Phishing). Ein solcher Vorfall ist umgehend dem Service Desk der Informatikdienste zu melden.

[4] *aufgehoben*

Artikel 15 Systeme mit hohem und sehr hohem Schutzbedarf[58]

[1] Systeme mit **hohem Schutzbedarf** sind Systeme mit Daten gemäss Art. 16 und 23 Abs. 1bis Weisung Informationssicherheit an der ETH Zürich.

[1bis] *aufgehoben*

[2] Solche Systeme müssen gemäss Art. 19 Abs. 1 Weisung Informationssicherheit an der ETH Zürich gegen den Zugriff und Zutritt durch Unbefugte geschützt werden.

[2bis] Systeme mit **sehr hohem Schutzbedarf** sind Systeme mit Daten gemäss Art. 16 und 23 Abs. 1 Weisung Informationssicherheit an der ETH Zürich.

---

[53] Vgl. Art. 16 und 23 Abs. 1bis Weisung Informationssicherheit an der ETH Zürich (RSETZH 203.25); Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[54] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[55] verschoben in Artikel 6
[56] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.
[57] auch Authentisierungsmittel
[58] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.

[2ter] Solche Systeme müssen gemäss Art. 19 Abs. 2 und 3 Weisung Informationssicherheit an der ETH Zürich mit verschärften Mitteln gegen den Zugriff und Zutritt durch Unbefugte geschützt werden.

[3] *aufgehoben*[59]

[4-9] aufgehoben

[10] Der Verlust oder die ungewollte Weitergabe von Daten der ETH Zürich aus Verwaltung, Lehre und Forschung im Sinne von Art. 15 Abs. 1 muss verhindert werden. Es liegt deshalb in der Verantwortung des jeweiligen Benutzers, dass von ihm genutzte mobile Datenträger (CDs/DVDs, USB-Sticks, Speicherkarten, Flash-Speicher u.ä.) sowie die Daten auf mobilen Geräten vor der Entsorgung auf geeignete Weise gelöscht und unlesbar gemacht werden.[60] Bei Datenverlust ist der/die zuständige Vorgesetzte und der/die CISO zu informieren. Bei Diebstahl zusätzlich die Abteilung SGU.

Artikel 15[bis] Integrität des IKT-Netzwerks[61]

Das IKT-Netzwerk der ETH-Zürich darf von Benutzern oder Dritten nicht eigenmächtig erweitert oder verändert werden[62]. Ausnahmen bedürfen der schriftlichen Zustimmung der Informatikdienste.

5. Abschnitt: Verantwortlichkeit und Haftung

Artikel 16 Verantwortlichkeit[63]

[1] Jeder Benutzer ist persönlich dafür verantwortlich, dass seine Benutzung der IKT-Mittel nicht gegen Bestimmungen dieser Benutzungsordnung oder gegen die Rechtsordnung (z.B. Strafrecht, Datenschutz) verstösst bzw. die Rechte Dritter (z.B. Urheberrechte, Lizenzbestimmungen, Persönlichkeitsrechte) verletzt.

[2] *aufgehoben*

Artikel 17 Haftung

[1] Die Benutzer haben die ihnen von der ETH Zürich zur Verfügung gestellten IKT-Mittel mit der gebotenen Sorgfalt zu nutzen.

[2] Technische und betriebliche Anordnungen der Informatikdienste, der Informatiksupportgruppen, des CSCS und der/des Systemverantwortlichen, der Service-Vermittelnden, Anordnungen der/des CISO sowie Ausführungsbestimmungen zur BOT wie die *IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich*[64] sind für alle Benutzenden verbindlich[65].

[3] Vorbehältlich einer schriftlichen Zusicherung der zuständigen Organe übernimmt die ETH Zürich keine Haftung für Mängel der IKT-Mittel und deren Folgen.

[59] aktualisiert und verschoben in Art. 6
[60] vgl. auch Anhang zur BOT Ziffer 1 Abs. 7.
[61] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[62] z.B. durch Anschluss an fremde IKT-Netzwerke mittels Direktanschluss (z.B. ins Internet) oder mittels Installation von Routern, Switches, Access points, Firewalls, Load balancern etc.
[63] Fassung gemäss Schulleitungsbeschluss vom 17. September 2013, in Kraft seit 1. Oktober 2013.
[64] RSETHZ 203.23 (siehe namentlich Artikel 8)
[65] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.

[4] Für grobfahrlässig oder absichtlich verursachte Schäden und technische Störungen an IKT-Mitteln der ETH Zürich haftet in jedem Fall der Verursacher. Bei nicht bestimmungsgemässer Nutzung haftet der Verursacher auch für leichte Fahrlässigkeit.

[5] Bei grobfahrlässiger oder absichtlicher Verletzung von Rechten Dritter (insbesondere von Urheberrechten und Lizenzbestimmungen) wird der Benutzer auch für denjenigen Schaden haftbar, für den die ETH Zürich allenfalls von Dritten belangt wird.

[6] Im Übrigen gilt für Mitarbeitende der ETH Zürich bei der Benutzung der IKT-Mittel in Erfüllung öffentlich-rechtlicher Aufgaben des Bundes das Verantwortlichkeitsgesetz.[66]

6. Abschnitt: Missbrauch und Umgang mit Schwachstellen

Artikel 18 Technisch-operative Systemüberwachung zur Feststellung von Missbrauch[67]

[1] Die IKT-Mittel protokollieren laufend oder bei Bedarf die wichtigsten auf ihnen durchgeführten Aktivitäten.

[2] Zur Kontrolle der Einhaltung der Bestimmungen dieser Benutzungsordnung sind auf Anordnung der/des CISO stichprobenweise nicht personenbezogene Überprüfungen der Protokollierungen zulässig.

[2bis] Die Protokollierung der E-Mails betrifft u.a. die Betreffzeile, Datum, Zeit, Absender- und Empfängeradressen.

[2ter] Daten über den technischen Zustand von IKT-Mitteln, insbesondere über deren Sicherheitszustand, werden durch das IT-Security Center der Abteilung Informatikdienste im Auftrag der/des CISO kontinuierlich oder stichprobenweise erhoben und ausgewertet.

[3] Bei festgestellten Missbräuchen im Sinne von Art. 19 oder beim Vorliegen des konkreten Verdachts auf solche Missbräuche sowie zur Analyse und Behebung von technischen Störungen der IKT-Mittel und zur Abwehr konkreter Bedrohungen dieser Infrastruktur, können die Aufzeichnungen im Auftrag der/des CISO personenbezogen ausgewertet werden. Dabei sind die *Regeln zur Überwachung der Nutzung von IKT-Mitteln an der ETH Zürich* einzuhalten (Anhang).

[3bis] Die Feststellung (Datenaufzeichnung, Sichtung, Sicherung) und allenfalls Sanktionierung (selbst oder mittels Strafantrag/ Strafanzeige) von missbräuchlichem Verhalten, Sicherheitsgefährdungen oder Straftaten mittels Videoaufzeichnungen oder mittels elektronischen Zutrittskontrollen bei Gebäuden oder Arealen der ETH Zürich obliegt der Leiterin/dem Leiter der Abteilung Sicherheit, Gesundheit und Umwelt. Die Bestimmungen dieses Abschnitts 6 der BOT sowie des Anhangs gelangen analog zur Anwendung, soweit keine anderen Normen vorgehen.

[4] Einzelheiten zur Erhebung des Systemzustands zur Aufzeichnung des Nutzerverhaltens, Zuständigkeiten, Protokollierung von Missbräuchen, Aufbewahrung der Nutzungsdaten und deren Auswertung sind im Anhang geregelt (*Regeln zur Überwachung der Nutzung von IKT-Mitteln an der ETH Zürich)*.

[5] Benutzende, Service-Vermittelnden, Systemverantwortliche, Netzwerkzonenverantwortliche und IT-Betreibende sind verpflichtet, bei der Aufklärung von Fällen missbräuchlicher und rechtswidriger Nutzung und von Schadensfällen mitzuwirken.

[66] SR **170.32**

[67] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.

Artikel 19 Missbräuchliche Nutzung

[1] Missbräuchlich ist jede Nutzung von IKT-Mitteln der ETH Zürich, die die Vorschriften dieser Benutzungsordnung missachtet, gegen übergeordnetes Recht verstösst oder Rechte Dritter verletzt.

[2] Demzufolge gelten insbesondere 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 (Art. 197 des Schweizerischen Strafgesetzbuches [StGB; SR 311.0]), Aufforderung zu Verbrechen oder Gewalttätigkeit (Art. 259 StGB), Störung der Glaubens- und Kultusfreiheit (Art. 261 StGB) oder Rassendiskriminierungen (Art. 261bis StGB);

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 Anleitung zur Herstellung von solchen Programmen zu Zwecken der Lehre und Forschung kann erlaubt werden, wenn angemessene Vorkehrungen gegen ihre schädigende Verwendung getroffen werden und vorgängig die schriftliche Zustimmung der Schulleitung oder der von dieser als zuständig erklärten Stelle eingeholt worden ist;

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). Im Einzelfall kann das „Hacking" in einer sicheren Testumgebung zu Zwecken der Lehre und Forschung[68] erlaubt sein, sofern vorgängig die schriftliche Zustimmung der Schulleitung oder der von dieser als zuständig erklärten Stelle eingeholt worden ist; Scanning nach Verwundbarkeiten mit dem Ziel, diese zu beseitigen, sind den zuständigen Netzwerkzonenverantwortlichen und Systemverantwortlichen und dem IT-Security Center der Informatikdienste[69] erlaubt.

d) Datendiebstahl (Art. 143 StGB) und Datenbeschädigung (Art. 144bis Ziff. 1 StGB);

e) Die Nutzung von IKT-Mitteln der ETH Zürich in absichtlicher Verletzung von Lizenzbestimmungen oder Urheberrechten;

f) Das Versenden von Mitteilungen mittels elektronischer Kommunikationsmittel mit vorgetäuschten oder irreführenden Absenderangaben oder Inhalten (z.B. betrügerische E-Mails wie Phishing, CEO-Fraud etc.);

g) Die Belästigung oder Irreführung von Angehörigen der ETH Zürich oder Dritter durch Mitteilungen mit elektronischen Kommunikationsmitteln (z.B. mit beleidigenden, sexistischen, rassistischen, rufschädigenden oder diskriminierenden Inhalten);

h) Das Einrichten von Direktanschlüssen an die ETH Zürich-Kommunikationsnetze (z.B. durch Modems, oder WLAN Access Points) ohne vorgängige schriftliche Zustimmung der Informatikdienste und der jeweiligen Systemverantwortlichen (Art. 15bis);

i) Der Versand von Massenwerbung ohne direkten Zusammenhang mit einem angeforderten Inhalt und ohne vorgängige Einwilligung der Kunden, korrekte Absenderangabe oder den Hinweis auf eine problemlose und kostenlose Ablehnungsmöglichkeit (Spam); ETH-interner Massenversand im Sinne von Art. 11 Abs. 3 dieser Benutzerordnung ist davon ausgeschlossen.

[3] Als schwerer Missbrauch gelten:

a) Missbräuche gemäss Abs. 2 Bst. a, b, c, d, soweit diese vorsätzlich bzw. absichtlich erfolgen;

b) andere Missbräuche im Wiederholungsfall.

[68] z.B. Information Security Lab, D-INFK

[69] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021; Namensänderung von "Network Security Group" in "IT-Security Center"

[4] Die Kenntnis schwerer oder wiederholter missbräuchlicher Nutzung verpflichtet die direkten Vorgesetzten, das IT-Security Center der Informatikdienste, die Service-Vermittelnden sowie die System- bzw. Netzwerkzonenverantwortlichen zur Meldung an die/den CISO[70].

Artikel 20 Konsequenzen von Missbräuchen[71]

[1] Wird ein Missbrauch oder ein konkreter Verdacht eines Missbrauchs im Sinne von Art. 19 dieser Benutzungsordnung festgestellt, so kann die/der CISO die folgenden Massnahmen anordnen:

a) Abmahnung leichter Verstösse gegen die vorliegende Benutzungsordnung; [72]

b) Vorsorgliche Sperrung des Zugangs zu IKT-Mitteln[73], die davon betroffen sind;

c) Blockierung missbräuchlicher und rechtswidriger Daten sowie deren Sicherung und Aufbewahrung zu Beweiszwecken;

d) Löschung missbräuchlicher und rechtswidriger Daten, soweit dies aus Sicherheitsgründen erforderlich ist.

[2] Als Sanktionen gegen Missbräuche können die fehlbaren Benutzer mit der Sperrung des Zugangs zu IKT-Mitteln, mit einer Nutzungseinschränkung oder einem Nutzungsverbot belegt werden. Sie fallen dahin, wenn nicht innerhalb von drei Monaten ein Disziplinarverfahren eingeleitet oder Strafanzeige erstattet wird.

[3] *aufgehoben*

[4] Gegen fehlbare Benutzer können zudem disziplinarische oder personalrechtliche Massnahmen[74] ergriffen, ein Zivilverfahren (Schadenersatzklage) eingeleitet oder Strafanzeige erstattet werden[75]. Besonders schwere Fälle (Art. 19 Abs. 3) können zur Exmatrikulation oder Entlassung führen.

[5] Ein schwerer Missbrauch durch Studierende gilt als nicht geringfügiger Verstoss im Sinne von Art. 8 der Disziplinarordnung ETH Zürich[76]. Für Mitarbeitende gilt jede Art des Missbrauchs als Verletzung der arbeitsrechtlichen Pflichten.[77]

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

Artikel 20bis Umgang mit Schwachstellen[78]

[1] Festgestellte technische Schwachstellen von IKT-Mitteln müssen gemäss *IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich* behoben oder so gemildert werden, dass sie keine Bedrohung für andere IKT-Mittel oder für Datenbestände der ETH Zürich darstellen.

[2] Werden technische Schwachstellen auf IKT-Mitteln von den Verantwortlichen nicht innerhalb von 20 Tagen ab deren Erkennung behoben oder hinreichend gemildert, ist das IT-Security Center der Informatikdienste

[70] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.
[71] Fassung gemäss Schulleitungsbeschluss vom [SLB Datum NEU], in Kraft seit 1. Juni 2021.
[72] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[73] vgl. Anhang Ziffer 4
[74] Studierende: gemäss Art. 3 Disziplinarordnung ETH Zürich vom 2.11.2004 (SR **414.138.1**);
Mitarbeitende: gemäss Art. 58a Personalverordnung ETH-Bereich vom 15.3.2001 (PVO-ETH; SR **172.220.113**).
[75] Das Vorgehen richtet sich nach Art. 22a Bundespersonalgesetz (BPG; SR **172.220.1**).
[76] Disziplinarordnung ETH Zürich vom 4. November 2004 (SR **414.138.1).**
[77] Art. 25 Bundespersonalgesetz (SR **172.220.1**) bzw. Art. 53 PVO-ETH; Fassung gemäss Schulleitungsbeschluss vom 20. August 2013, in Kraft seit 1. Oktober 2013.
[78] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.

berechtigt, den Zugang zu den IKT-Mitteln zu sperren, sofern die Schwachstellen kritisch sind und andere IKT-Mittel oder Datenbestände durch diese Schwachstelle gefährdet sein könnten. Das IT-Security Center der Informatikdienste informiert umgehend die/den CISO über solche Fälle.

[3] Im Falle dringender, akuter Bedrohungslagen oder Angriffen mit grossem Risiko für die Informationssicherheit der ETH Zürich, die sofortiges Handeln notwendig machen, können – im Auftrag der/des CISO – der/die IT Security Officer der Informatikdienste (ITSO ID) oder die zuständigen IT-Betreiber eine unmittelbare Verteilung und Installation von Sicherheitsaktualisierungen anordnen. Die/der ITSO ID bzw. die IT-Betreiber informieren umgehend die/den CISO über solche Fälle.

[4] Zuwiderhandlungen im Umgang mit Schwachstellen können zur Ermahnung durch die/den CISO führen. Vorsätzliche Zuwiderhandlungen können als schwere Missbräuche im Sinne von Art. 19 Abs. 3b eingestuft werden und zu Sanktionen führen.

7. Abschnitt: Besondere Vorschriften

Artikel 21 Besondere Vorschriften und Weisungen[79]

[1] Im Übrigen sind von den Benutzenden, Service-Vermittelnden, Systemverantwortlichen und Netzwerkzonenverantwortlichen, soweit sie ihre Tätigkeit oder die von ihnen genutzten IKT-Mittel betreffen, die folgenden Vorschriften in ihrer jeweils aktuellen Fassung zu beachten:

a) Allfällige besondere Weisungen der jeweiligen Organisationseinheiten betreffend Nutzung einzelner Systeme, insbesondere bezüglich Datenschutz und Datensicherheit;

b) Ausführungsbestimmungen über den Auftritt der ETH Zürich im Internet[80];

c) Wegleitung für die Inventarführung an der ETHZ vom Januar 2019[81];

d) IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich[82];

e) Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen;[83]

f) Art. 36a bis Art. 36e ETH-Gesetz[84] (Personalinformationssysteme, Studieninformationssysteme; Umgang mit Personendaten in Forschungsprojekten) sowie

g) *aufgehoben*[85]

[79] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.

[80] Web-Richtlinien der ETH Zürich vom 1. September 2016 (RSETHZ 203.22) und Social-Media-Richtlinien ETH Zürich vom 26. Februar 2013 (RSETHZ 203.24). Fussnote aktualisiert, in Kraft seit 1. April 2019.

[81] Wegleitung für die Inventarführung an der ETHZ vom Januar 2019; abrufbar unter ETH Zürich > Finanzen und Controlling > Downloads (zuletzt 21.01.2019).

[82] IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich (RSETHZ 203.23)

[83] Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen vom 22. Februar 2012 (SR **172.010.442**).

[84] ETH Gesetz (SR **414.110)**

[85] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.

8. Abschnitt: Schlussbestimmungen

Artikel 22 Vollzug[86]

aufgehoben

Artikel 23 Aufhebung bisherigen Rechts und Inkrafttreten[87]

[1] Folgende Erlasse werden aufgehoben:

a) Die Benutzungsordnung für Informations- und Kommunikationstechnologie an der ETH Zürich (BOT; RSETHZ 203.21; Stand 1. April 2019);

b) Die IT Best Practice Rules[88] (Stand 3. Juni 2019) sowie die Standards für Verantwortlichkeiten und Systempflege (Stand 6. Februar 2003; RSETHZ 203.23);

[2] Diese Verordnung tritt am 1. Mai 2005 in Kraft.

Artikel 24 Koordination mit der Weisung «Informationssicherheit an der ETH Zürich» und den «IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich»[89]

Folgende Artikel des vorliegenden Erlasses treten erst zusammen mit dem Inkrafttreten der kommenden Teilrevisionen der Weisung *Informationssicherheit an der ETH Zürich* (RSETHZ 203.25) und der *IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich* (RSETHZ 203.23) in Kraft[90]:

Art. 2 Abs. 11
Art. 4 Abs. 1c
Art. 6 Abs. 2, 4b und 5
Art. 8 Abs. 5bis
Art. 9 Abs. 2
Art. 17 Abs. 2
Art. 18 Abs. 5
Art. 19 Abs. 4
Art. 20bis Abs. 1
Art. 21 Abs. 1d
Art. 23 Abs. 1b
Ziff. 2.1, 3.1, 3.3 und 7.1 Anhang BOT

Zürich, 19. April 2005

Im Namen der Schulleitung:

Der Präsident: Kübler
Der Delegierte: Kottusch

[86] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[87] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.
[88] Die *IT Best Practices Rules* wurden von der Abteilung Informatikdienste als Empfehlung erlassen, doch nie formell in Kraft gesetzt. Der Klarheit halber werden sie hier als aufgehoben erklärt. Wie die *Standards für Verantwortlichkeiten und Systempflege* (RSETHZ 203.23) werden diese ersetzt durch die *IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich*, die separat in Kraft gesetzt werden.
[89] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.
[90] voraussichtlich per 1. Juli 2021

Anhang[91]

Regeln zur Überwachung der Nutzung von IKT-Mitteln der ETH Zürich

1. Aufzeichnung, Aufbewahrung und Vernichtung von Daten

[1] Die technische Prävention, die Sensibilisierung und Mitwirkung der ETH-Angehörigen hat Vorrang gegenüber der Überwachung. Die ETH Zürich ist dafür besorgt, dass die technischen Schutzmassnahmen regelmässig dem neuesten Stand der Technik angepasst werden.

[2] Werden IKT-Mittel der ETH Zürich genutzt oder IKT-Mittel in deren Auftrag betrieben, so dürfen die dabei anfallenden Daten zu folgenden Zwecken aufgezeichnet werden[92]:

a. alle Daten, einschliesslich Daten über den Inhalt elektronischer Post: zu deren Sicherung (Backups);
b. die Daten über den technischen Zustand der IKT-Mittel (z.B. Patch-Stände, Virenschutzmeldungen, Schwachstellenscans) und Randdaten über deren Nutzung:
   - zur Aufrechterhaltung der Informations- und Dienstleistungssicherheit,
   - zur technischen Wartung der elektronischen Infrastruktur,
   - zur stichprobenweisen Kontrolle der Einhaltung der BOT,
   - zum Nachvollzug des Zugriffs auf Datensammlungen,
   - zur Kostenkontrolle;
c. die Daten über das Betreten oder das Verlassen von Gebäuden und Räumen der ETH Zürich und über den Aufenthalt darin: zur Gewährleistung der Sicherheit.

[3] Soweit der Auswertungszweck dies erfordert, können die soeben in Abs. 2 genannten Daten längstens wie folgt aufbewahrt werden:[93]

a. Daten gemäss Abs. 2 Bst. a: bis zur dauerhaften Archivierung der zugrundeliegenden Informationen durch das Archiv der ETH Zürich[94]; falls keine Übernahme erfolgt: 2 Jahre;
b. Daten gemäss Abs. 2 Bst. b: 2 Jahre;
c. Daten gemäss Abs. 2 Bst c: 3 Jahre.

[4] Die aufgezeichneten Daten sind nach Ablauf der Aufbewahrungsdauer durch die zuständigen Stellen zu vernichten.

[5] Soweit der Inhalt elektronischer Post (E-Mail) von geschäftlicher und oder rechtlicher Relevanz für die ETH Zürich ist, gilt die gesetzliche Aufbewahrungsdauer von 10 Jahren bis zur Archivierung oder Löschung.[95]

[91] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[92] Aufzeichnung zu den Zwecken gemäss Art. 57l Regierungs- und Verwaltungsorganisationsgesetz (RVOG; SR **172.010**); redaktionelle Anpassung in Kraft seit 1.1.2019.
[93] Art. 4 Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen vom 22. Februar 2012 (SR **172.010.442**).
[94] Die ETH-Bibliothek hat für die ETH Zürich und den ETH-Rat die Funktion eines öffentlichen Archivs gemäss Bundesgesetz über die Archivierung (BGA; SR **152.1**, RSETHZ 420.1).
[95] Fassung gemäss Schulleitungsbeschluss vom 7. April 2022, in Kraft seit 1. Mai 2022.

[6] Für die Bearbeitung und Aufbewahrung von Daten, die in den elektronischen Personal- und Studieninformationssystemen gemäss Art. 36a und 36b ETH-Gesetz aufgezeichnet werden, gelten entsprechende Ausführungsbestimmungen des ETH-Rates bzw. der Schulleitung der ETH Zürich[96].

[7] Die Aufbewahrungsdauer und Vernichtung von Daten auf Druckern, Scannern etc. ist abhängig von der Speicherkapazität des Geräts, auf dem die Daten aufgezeichnet werden. Diese Daten müssen spätestens bei der Weitergabe oder Entsorgung des Geräts von den zuständigen Stellen unwiederbringlich vernichtet werden.[97]

[8] Für die Aufbewahrung von Forschungsdaten gilt Artikel 11 der Richtlinien für Integrität in der Forschung und gute wissenschaftliche Praxis an der ETH Zürich.[98]

2. Zuständigkeiten

2.1 IT-Betreiber, Systemverantwortliche und Service-Vermittelnde der Organisationseinheiten

a) Einrichtung und Betrieb der IKT-Mittel zur Vornahme der Aufzeichnungen gemäss Ziff. 1 dieses Anhangs.

b) Vornahme von Stichproben gemäss Ziff. 3 auf Anordnung des/der CISO.

c) Unterstützung der/des CISO oder der/des ITSO ID bei der Wahrnehmung von deren/dessen Aufgaben gemäss diesen Regelungen.

2.2 Netzwerkzonenverantwortliche

Unterstützung der/des CISO oder der/des ITSO ID bei der Wahrnehmung von deren/dessen Aufgaben gemäss diesen Regelungen.

2.3 Informatikdienste der ETH Zürich

a) Unterstützung der/des CISO bei der Wahrnehmung von deren/dessen Aufgaben gemäss diesen Regelungen sowie Überwachung der IKT-Mittel (namentlich des IKT-Netzwerks) der ETH Zürich.

b) Erhebung der technischen Zustände der IKT-Mittel gemäss Art. 18 Abs. 2ter und Art. 20bis Abs. 2.[99]

2.4 IT Security Officer Informatikdienste (ITSO ID)

Soweit nicht in Art. 8 Weisung Informationssicherheit an der ETH Zürich[100] geregelt, obliegt der/dem ITSO ID namentlich die Anordnung der Durchführung von Stichproben im Auftrag der/des CISO gemäss Ziff. 3 Abs. 1 dieses Anhangs.

2.5 Chief Information Security Officer (CISO)

Soweit nicht in Art. 5 Weisung Informationssicherheit an der ETH Zürich[101] geregelt, obliegen der/dem CISO namentlich folgende Aufgaben:

a) Kontakt mit dem Dienst für Überwachung des Fernmeldeverkehrs (Dienst ÜPF);

[96] Richtlinien über den Schutz und den Umgang mit Personaldaten an der ETH Zürich vom 15. November 2011 (RSETHZ 612).

[97] Art. 5 Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen vom 22. Februar 2012 (SR **172.010.442**).

[98] Richtlinien für Integrität in der Forschung und gute wissenschaftliche Praxis an der ETH Zürich vom 14. November 2007 (RSETHZ 414).

[99] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.

[100] Weisung Informationssicherheit an der ETH Zürich vom 9. April 2018 (RSETHZ 203.25).

[101] Weisung Informationssicherheit an der ETH Zürich vom 9. April 2018 (RSETHZ 203.25).

b) Anordnung der Durchführung von Stichproben gemäss Ziff. 3 Abs. 1 dieses Anhangs;

c) Ergreifung von vorsorglichen Massnahmen gemäss Ziff. 4 dieses Anhangs;

d) Entscheid über die personenbezogene Auswertung von aufgezeichneten Daten gemäss Ziff. 5 Abs. 1 Bst. a dieses Anhangs[102];

e) Befragung von Angehörigen der ETH Zürich gemäss Ziff. 3 Abs. 2 dieses Anhangs;

f) Anordnung von personenbezogenen Aufzeichnungen in Absprache mit den zuständigen direkten Vorgesetzten (bei Mitarbeitenden) bzw. der Studiendirektorin/ des Studiendirektors (bei Studierenden) gemäss Ziff. 5.

2bis Auswertung von Aufzeichnungen[103]

Die Auswertung der Aufzeichnungen kann sowohl nicht personenbezogen (pseudonyme Auswertung) wie auch personenbezogen erfolgen. Sie hat den in diesem Reglement festgehaltenen Grundsätzen zu folgen.

3. Nicht personenbezogene Stichproben[104]

[1] Die Systemverantwortlichen und Service-Vermittelnden können auf Anordnung der/des CISO stichprobenweise nicht personenbezogene Überprüfungen zur Kontrolle der Nutzung der IKT-Mittel vornehmen.

[1bis] Nicht personenbezogene (anonyme, pseudonyme) Auswertungen der Daten gemäss Ziffer 1 Abs. 2 lit. b[105] durch die Informatikdienste zur Überprüfung der IKT-Sicherheit dürfen permanent und ohne Anordnung der/des CISO erfolgen.

[2] Bei der Überprüfung des E-Mail-Verkehrs darf keine Einsicht in den Inhalt privater Emails der ETH-Angehörigen genommen werden (Art. 18 Abs. 2bis BOT). Wenn ein E-Mail nicht gemäss Art. 8bis Abs. 3 in einem «Privat»-Ordner gespeichert ist[106], wenn kein Unterscheidungsvermerk zwischen privaten und geschäftlichen E-Mails besteht und die private Natur aufgrund der Adressierungselemente nicht erkennbar und nicht anzunehmen ist, darf die ETH Zürich davon ausgehen, dass das E-Mail geschäftlich ist. Im Zweifelsfalle ist die Natur des E-Mails mit dem ETH-Angehörigen zu klären.

[3] Anlässlich der stichprobenweisen Überprüfung festgestellte Missbräuche oder ein entsprechender Verdacht sind von den Systemverantwortlichen und Service-Vermittelnden umgehend der/dem CISO mitzuteilen.

4. Sichernde und vorsorgliche Massnahmen

[1] Liegt aufgrund der nicht personenbezogenen Stichproben ein konkreter Verdacht eines Missbrauchs im Sinne von Art. 19 vor, der die Gefahr einer erheblichen Beeinträchtigung der ordentlichen Nutzung von IKT-Mitteln der ETH Zürich oder einer Schädigung der ETH Zürich, von deren Angehörigen oder von Dritten mit sich bringt, so ist die/der CISO zur Anordnung der folgenden sichernden und vorsorglichen Massnahmen befugt[107]:

a) Sperrung des Zugangs zu IKT-Mitteln, von denen ein festgestellter Missbrauch ausgeht oder die davon betroffen sind;

b) Blockierung von Daten sowie deren Sicherung und Aufbewahrung zu Beweiszwecken.

[102] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.
[103] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.
[104] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.
[105] Redaktionelle Berichtigung vom 15. Juli 2019 (Ersatz von «Artikel» durch «Ziffer» [dieses Anhangs]).
[106] Fassung gemäss Schulleitungsbeschluss vom 7. April 2022, in Kraft seit 1. Mai 2022
[107] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.

[2] Die in Abs. 1 erwähnten Massnahmen können in dringenden Fällen auch von der/vom ITSO ID angeordnet werden, wobei die/der CISO umgehend zu informieren ist und über die Aufrechterhaltung der getroffenen Massnahmen entscheidet.

5. Personenbezogene Auswertungen der Aufzeichnungen[108]

[1] Die/der CISO entscheidet bei nach einer nicht personenbezogenen Auswertung von Aufzeichnungen festgestellten *Missbräuchen* im Sinne von Art. 19 BOT oder beim Vorliegen eines konkreten Verdachts auf solche Missbräuche nach den folgenden Grundsätzen über die personenbezogene Auswertung von aufgezeichneten Daten:

a) Aufgrund der Schwere des Missbrauchs, gemeinsam mit dem/der direkten Vorgesetzten (Mitarbeiter) sowie dem Leiter/der Leiterin HR bzw. dem /der zuständigen Personalchef/Personalchefin oder der Studiendirektorin/ dem Studiendirektor bzw. dem Rektor/der Rektorin (Studierende), ob die personenbezogene Auswertung zur Identifikation der verantwortlichen Person sofort oder erst nach wiederholter Feststellung eines Missbrauchs erfolgen soll.

b) Weitere Auswertungen erfolgen in jedem Fall nur, nachdem die betroffene Person über den Missbrauchsverdacht informiert worden ist.[109]

c) Liegt beim in Frage stehenden Missbrauch der konkrete Verdacht auf das Vorliegen **strafbarer Handlungen** nach dem schweizerischen Strafgesetzbuch vor, so sind die entsprechenden Beweise bestehend aus Protokollierungen und eventuellen Backups zu sichern. **Weitere personenbezogene Auswertungen sind in diesen Fällen nicht zulässig und obliegen alleine der zuständigen Strafjustizbehörde.** Der Entscheid, ob Anzeige gegen die diese Person erstattet wird, liegt im Falle von fehlbaren Mitgliedern des Lehrkörpers oder Mitarbeitenden der ETH Zürich beim Präsidenten.[110]

d) *aufgehoben*

[2] Auswertungen zur Analyse und Behebung von *technischen Störungen* der IKT-Mittel und Abwehr konkreter Bedrohungen dieser Infrastruktur sind nur zulässig, wenn sie für die Suche nach der Ursache oder die Beseitigung der Störung oder für die Abwehr einer konkreten Bedrohung erforderlich sind, namentlich wenn

a) die Nutzung der IKT-Mittel wegen eines Defekts oder einer ausserordentlichen Beanspruchung durch einen einzelnen Nutzer verunmöglicht oder stark eingeschränkt ist; oder

b) die unmittelbare Gefahr einer Schädigung der IKT-Mittel oder der Daten der Nutzer besteht (Verbreitung von Schadprogrammen).[111]

6. Sanktionen

Die Zuständigkeit zur Sanktionierung von festgestellten Missbräuchen gegenüber den fehlbaren Benutzern richtet sich nach Art. 20 BOT.

[108] Fassung gemäss Schulleitungsbeschluss vom 11. Mai 2021, in Kraft seit 1. Juni 2021.

[109] 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**).

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

[111] Art. 57o Abs. 1 Bst. b Regierungs- und Verwaltungsorganisationsgesetz (RVOG; SR **172.010**) i.V. mit Art. 12 Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen vom 22. Februar 2012 (SR **172.010.442**).

7. Vertraulichkeit

[1] Die gemäss Ziffer 1 dieses Anhangs aufgezeichneten Daten sind vertraulich zu behandeln und die Systemverantwortlichen und Service-Vermittelnden haben die entsprechenden Massnahmen zu treffen, damit Angehörige der ETH Zürich und Dritte weder unbefugt Kenntnis davon noch Zugang dazu erhalten.

[2] Über das Ergebnis der stichprobenweisen Überprüfungen und personenbezogener Auswertungen sowie über sichernde und vorsorgliche Massnahmen ist von den damit befassten Personen strengstes Stillschweigen zu wahren. Auskünfte dürfen nur dann und nur insoweit erteilt werden, als dies gemäss den vorliegenden sowie allfälligen weiteren Bestimmungen zulässig ist.

8. Fernmeldeüberwachung

[1] Die/der CISO ist zuständig für den Kontakt zum vom Bund betriebenen «Dienst Überwachung Post- und Fernmeldeverkehr» (Dienst ÜPF). Der Dienst ÜPF betreibt die Auswertung des Post- und Fernmeldeverkehrs zur Klärung von schweren Straftaten. Die/der CISO und andere Stellen der ETH Zürich informieren unverzüglich den Rechtsdienst, wenn sie vom Dienst ÜPF oder von Strafverfolgungsbehörden im Zusammenhang mit der Überwachung des Fernmeldeverkehrs kontaktiert werden.

[2] Die Vorbereitungen und Durchführung der Überwachung richtet sich namentlich nach den Artikeln 4, 18 ff., 28 sowie Art. 51 ff. Verordnung über die Überwachung des Post- und Fernmeldeverkehrs vom 15. November 2017 (VüPF; SR **780.11**).