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

(Teilrevision Stand 1. April 2019)

---

1. Abschnitt: Allgemeine Bestimmungen ... 3

Artikel 1 Zweck ... 3

Artikel 2 Begriffe ... 3

Artikel 3 Geltungsbereich ... 4

2. Abschnitt: Zuständigkeiten ... 5

Artikel 4 Abteilung Informatikdienste, Informatiksupportgruppen und CSCS ... 5

Artikel 5 Chief Information Security Officer (CISO) ... 6

Artikel 6 IT-Betreiber, System- und Netzanschlussverantwortliche ... 6

Artikel 7 Präsenz im Intranet / Internet ... 6

3. Abschnitt: Nutzung ... 7

Artikel 8 Nutzungszweck und Nutzungsbefugnis ... 7

Artikel 8bis Private Nutzung ... 7

Artikel 9 Nutzung von IKT-Mitteln ausserhalb der ETH Zürich ... 8

Artikel 10 Private Nutzung von ETH Zürich lizenzierter Software ... 8

Artikel 11 Datenschutz ... 8

Artikel 12 Kopien von Software ... 9

Artikel 13 Nutzung elektronischer Kommunikationsmittel ... 9

4. Abschnitt: Sicherheitsmassnahmen ... 9

Artikel 14 Systeme mit normalem Schutzbedarf ... 9

Artikel 14bis Zugriffsschutzmassnahmen ... 10

Artikel 15 Systeme mit hohem Schutzbedarf ... 10

Artikel 15bis Integrität des IKT-Netzwerks ... 11

5. Abschnitt: Verantwortlichkeit und Haftung ... 11

Artikel 16 Verantwortlichkeit ... 11

Artikel 17 Haftung ... 11

6. Abschnitt: Missbrauch ... 11

Artikel 18 Protokollierung/Feststellung von Missbräuchen ... 11

Artikel 19 Missbräuchliche Nutzung ... 12

Artikel 20 Konsequenzen von Missbräuchen ... 13

7. Abschnitt: Besondere Vorschriften ... 14

Artikel 21 Besondere Vorschriften und Weisungen 14

8. Abschnitt: Schlussbestimmungen 15

Artikel 22 Vollzug 15

Artikel 23 Aufhebung bisherigen Rechts und Inkrafttreten 15

Anhang 17

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

(BOT)

vom 19. April 2005 (Stand 1. April 2019[2])

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[3],

v e r o r d n e t :

1. Abschnitt: Allgemeine Bestimmungen

Artikel 1 Zweck

[1]Die Informations- und Kommunikationsmittel (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[4]

[1]*IKT-Mittel* (Ressourcen) umfasst alle Mittel der Informations- und Telekommunikationstechnologie, die im Eigentum der ETH Zürich sind . Es handelt sich insbesondere um Systeme, Einrichtungen und Dienste der ETH Zürich, die zur elektronischen Bearbeitung von Daten eingesetzt werden (z.B. Datenverarbeitungsanlagen, Netzwerkkomponenten, Datenspeicher, Drucker, Scanner, Telekommunikationsnetze und auf diesen Mitteln laufende Software oder Schliesssysteme). 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[5].

[2]Unter *Systeme* sind Hard- und Software zu verstehen, einschliesslich portable Systeme.

---

[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] Anpassung an die Weisung Informationssicherheit an der ETH Zürich vom 9. April 2018 (RSETHZ 203.25) gemäss Beschluss der Schulleitung vom 9. April 2018 (SLB 09.04.18-09.04 und SLB 26.03.19-07.01).

[3] RSETHZ 201.021

[4] Fassung gemäss Schulleitungsbeschluss vom 17. September 2013, in Kraft seit 1. Oktober 2013; Redaktionelle Anpassung in Kraft seit 1.1.2019.

[5] Voraussichtlich Art. 36i ETH-Gesetz (Stand Revision ETH-Gesetz vom Dezember 2018).

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

[4] *Benutzer* sind alle Angehörigen der ETH Zürich (Art. 13 ETH-Gesetz) und Dritte (z.B. Gäste[6], 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), die zur Nutzung von IKT-Mitteln der ETH Zürich berechtigt sind.

[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[7] errichtete zentrale oder dezentrale Organe der ETH Zürich (z.B. Departemente, Institute, Abteilungen[8], Stabsstellen, selbständige Professuren) sowie Lehr- und Forschungseinrichtungen ausserhalb der Departemente gemäss Art. 61 OV (z.B. CSCS).

[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 namentlich personenbezogene Auswertung* meint die Protokollierungsanalyse pseudonymisierter, bestimmbarer Personen. Das Pseudonym muss die Identität der betroffenen Person in der Phase der nichtpersonenbezogenen Überwachung schützen.

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

[11] *System- und Netzanschlussverantwortliche* sind die in Artikel 3 der *Standards für Verantwortlichkeiten und Systempflege*[9] definierten Fachpersonen.

[12] *Chief Information Security Officer (CISO)* ist die Person, die gemäss Art. 5 Weisung Informationssicherheit an der ETH Zürich[10] 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.[11]

Artikel 3 Geltungsbereich[12]

Diese Verordnung gilt sowohl für jede Benutzung und Mitbenutzung aller ETH Zürich-eigenen IKT-Mittel, 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.**

[6] Vgl. Weisung des Vizepräsidenten für Personal und Ressourcen vom 13. November 2018 betreffend den Gast-Aufenthalt an der ETH Zürich (RSETHZ 515.2).
[7] RSETHZ 201.021
[8] Redaktionelle Anpassung.
[9] RSETHZ 203.23
[10] RSETHZ 203.25
[11] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[12] Fassung gemäss Schulleitungsbeschluss vom 17. September 2013, in Kraft seit 1. Oktober 2013.

2. Abschnitt: Zuständigkeiten

Artikel 4 Abteilung[13] 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 Abteilung Informatikdienste ist im Bereich der IT-Sicherheit insbesondere zuständig für[15]:

a) die technischen Massnahmen im Bereich der Sicherheit der IKT-Mittel und Services, die durch die Informatikdienste für die zentralen und dezentralen Organisationseinheiten der ETH Zürich erbracht werden, einschliesslich der Abklärung und Dokumentation von Sicherheitsmängeln, der Information darüber sowie deren Behebung bzw. Umgehung; [16]

b) die Instruktion und Information der Benutzer;

c) die technische Überwachung der Einhaltung der *Standards für Verantwortlichkeiten und Systempflege*[17] sowie die Einhaltung der IT-Best Practice Rules gemäss Art. 15 Abs. 3;

d) die Koordination bei technischen und organisatorischen Neuerungen;

e) die Bereitstellung der notwendigen Verschlüsselungstechniken (Art. 13 Abs. 2);

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

g) das Erteilen von Genehmigungen gemäss Art. 15bis;

h) die Entgegennahme von Meldungen der Benutzer betreffend Sicherheitsproblemen (Art. 14 und 15);

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;

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;

k) die Feststellung, Dokumentation und Behebung von Sicherheitsmängeln (Art. 14 Abs. 2) in den zentralen Organisationseinheiten;

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

m) *aufgehoben*[21]

[13] Redaktionelle Anpassung.
[14] Fassung gemäss Schulleitungsbeschluss vom 17. September 2013, in Kraft seit 1. Oktober 2013.
[15] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[16] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[17] RSETHZ 203.23
[18] RSETHZ 203.25
[19] RSETHZ 203.25
[20] Ersatz eines Ausdrucks: im ganzen Erlass wird die Funktionsbezeichnung «IT-Sicherheitsbeauftragte» durch «CISO» ersetzt (vgl. Art. 2 Abs. 12).
[21] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.

[2] Die Informatiksupportgruppen in den Departementen sind, mit Ausnahme der in den Buchstaben g, i, k und l beschriebenen Aufgaben, 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 g und k beschriebenen Aufgaben, für die Erbringung von Leistungen auf dem Gebiet des Hochleistungsrechnens zuständig.

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

[1] Die 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 IT-Betreiber, System- und Netzanschlussverantwortliche[24]

[1] Für jedes System, welches im Datennetz der ETH Zürich betrieben wird, gibt es eine zuständige Person.

[2] Jede Organisationseinheit bestimmt für alle ihre Systeme eine/n oder mehrere Systemverantwortliche/n (System-Administrator/in) für die technischen und betrieblichen Belange im Zusammenhang mit der Benutzung der IKT-Mittel sowie eine/n Netzanschlussverantwortliche/n.

[3] Der IT-Betreiber[25] legt aufgrund der Meldungen der zuständigen Information Security Officer (ISO)[26] fest, welche Systeme Daten mit hohem Schutzbedarf im Sinne von Art. 16 und 23 Abs. 1 Weisung Informationssicherheit an der ETH Zürich bearbeiten (Art. 15 Abs. 1). Für Systeme, die nicht von einem IT-Betreiber betreut werden, übernimmt der/die Systemverantwortliche diese Aufgabe.

[4] Die/der Systemverantwortliche löscht vor Weitergabe oder Entsorgung die auf den nicht mobilen Datenträgern (Harddisk u.ä.) vorhandenen Daten der ETH Zürich (Anhang zur BOT Ziffer 1 Abs. 7).

[5] Die weiteren Aufgaben des/der Systemverantwortlichen und des Netzanschlussverantwortlichen sind in Ausführungsbestimmungen wie den *Standards für Verantwortlichkeiten und Systempflege*[27] sowie in den *Regeln zur Überwachung der Telematik-Nutzung an der ETH Zürich* im Anhang dieser Benutzerordnung geregelt.

[6] Bei nicht ETH-eigenen Systemen ist der Benutzer mit Administratorenrechten gleichzeitig auch der Systemverantwortliche.

Artikel 7 Präsenz im Intranet / Internet[28]

[1] Für den Auftritt der ETH Zürich und ihrer Organisationseinheiten im Internet bzw. Intranet ist die Hochschulkommunikation zuständig. Sie erlässt dafür die entsprechenden Ausführungsbestimmungen.[29]

---

[22] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[23] RSETHZ 203.25
[24] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[25] gemäss Art. 3 Abs. 4 Weisung Informationssicherheit an der ETH Zürich (RSETHZ 203.25).
[26] gemäss Art. 6 Weisung Informationssicherheit an der ETH Zürich.
[27] RSETHZ 203.23
[28] Fassung gemäss Schulleitungsbeschluss vom 17. September 2013, in Kraft seit 1. Oktober 2013.
[29] 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).

[2] Dabei trägt die Hochschulkommunikation den Bestimmungen der Behindertengleichstellung[30] angemessen Rechnung.

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

3. Abschnitt: Nutzung

Artikel 8 Nutzungszweck und Nutzungsbefugnis[31]

[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.

[3-4] *aufgehoben*

[5] Veränderungen durch die Benutzer an den von der ETH Zürich zur Verfügung gestellten IKT-Mitteln, insbesondere Eingriffe in und Veränderungen an Software und die Ausschaltung, Umgehung oder Entfernung von Sicherheitsvorkehrungen, sind nur mit schriftlicher Zustimmung des zuständigen Systemverantwortlichen erlaubt. Ausgenommen sind Veränderungen im Rahmen der ordentlichen Nutzung der IKT-Mittel.

[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 einem ETH Gebäude. Allfällige Kosten werden den betreffenden Kunden verrechnet.[32]

[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 gelten ferner Art. 134 Finanzreglement der ETH Zürich[33] sowie Ziff. 8 der Wegleitung für die Inventarführung an der ETHZ[34] vom Januar 2019.[35.]

Artikel 8bis Private Nutzung[36]

[1] Die Nutzung von IKT-Mitteln der ETH Zürich, insbesondere E-Mail und Internet für private Zwecke ist grundsätzlich erlaubt, soweit sie nicht übermässig ist, die Erfüllung der Arbeits- oder Studienpflichten nicht beeinträchtigt oder verletzt, nicht gegen die schweizerische Rechtsordnung (insbesondere gegen Bestimmungen des Strafgesetzbuches) oder Rechte Dritter (Persönlichkeitsrechte, Urheberrechte) verstösst, keinen kommerziellen Charakter hat und für die ETH Zürich nicht rufschädigend ist.

---

[30] Behindertengleichstellungsgesetz vom 13. Dezember 2002 (BehiG; SR **151.3**); Behindertengleichstellungsverordnung, vom 19 November 2003 (BehiV; SR **151.31**).
[31] Fassung gemäss Schulleitungsbeschluss vom 17. September 2013, in Kraft seit 1. Oktober 2013.
[32] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[33] Finanzreglement der ETH Zürich vom 1. Januar 2019 (RSETHZ 245).
[34] abrufbar unter ETH Zürich > Finanzen und Controlling > Downloads (zuletzt 21.01.2019).
[35] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[36] Neu eingefügt gemäss Schulleitungsbeschluss vom 17. September 2013, in Kraft seit 1. Oktober 2013.

[2] 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.

[3] 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.

[4] 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[37]. 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.[38]

Artikel 9 Nutzung von IKT-Mitteln ausserhalb der ETH Zürich

[1] Erbringt eine Mitarbeiterin oder ein Mitarbeiter die Arbeitsleistung im Einvernehmen mit der zuständigen Stelle zu Hause[39], so kann dies unter entsprechender Nutzung von IKT-Mitteln der ETH Zürich erfolgen.

[2] Der Einsatz von portablen ETH Zürich eigenen Systemen wie Laptops, Smartphone etc. ausserhalb des ETH Zürich Campus ist erlaubt. Dabei sind die IT Best Practice Rules zu beachten.[40]

Artikel 10 Private Nutzung von ETH Zürich lizenzierter Software[41]

aufgehoben

Artikel 11 Datenschutz[42]

[1] Die Bearbeitung von Personendaten[43] ist nur im Rahmen der gesetzlichen Zwecke der ETH Zürich sowie nach Massgabe der Datenschutzbestimmungen[44] erlaubt.

[2] Die Bekanntgabe von Personendaten der ETH Zürich an Dritte zur Autorisierung und Authentisierung von elektronischen Services ist erlaubt, jedoch nur soweit es sich nicht um besonders schützenswerte Daten[45] handelt und diese Personendaten für die Benutzung dieser Services notwendig sind.

---

[37] Erläuterndes Hilfsblatt der Abt. Informatikdienste unter https://idesnx.ethz.ch/SpecialInfo/Heimnutzung_SW.pdf, zuletzt abgerufen 1. Oktober 2018. Massgebend sind die jeweiligen Lizenzbedingungen.

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

[39] Gemäss Art. 43 Abs. 3 Personalverordnung ETH-Bereich (PVO-ETH; SR **172.220.113**).

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

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

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

[43] 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.

[44] 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).

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

[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 in jedem Fall die Vorgaben des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDOEB) zu beachten.[46]

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

Artikel 12 Kopien von Software[47]

aufgehoben

Artikel 13 Nutzung elektronischer Kommunikationsmittel[48]

[1] Die Vertraulichkeit des Nachrichtenversands über elektronische Kommunikationsmittel ist nicht gewährleistet.

[2] Berufs-, Amts- und Geschäftsgeheimnisse oder andere vertrauliche Informationen[49] aus dem Bereich der ETH Zürich (z.B. aus Personalakten) sind mittels sicheren IKT-Mitteln zu übermitteln, insbesondere mit geeigneter Verschlüsselungstechnik, sofern verfügbar.

[3] Die elektronischen Kommunikationsmittel der ETH Zürich dürfen nicht anonym, unter einem Pseudonym oder unter falschem Absender benutzt werden. [50]

4. Abschnitt: Sicherheitsmassnahmen

Artikel 14 Systeme mit normalem Schutzbedarf[51]

[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] Die Systemverantwortlichen von solchen Systemen sind für die Einhaltung der aktuell geltenden IT Best Practice Rules der Informatikdienste zuständig. Sie melden Sicherheitsprobleme, Defekte etc. unverzüglich an die zuständigen Stellen bei den Informatikdiensten oder den Informatiksupportgruppen.

[3] *aufgehoben*

[46] Stellungnahme des EDOEB vom November 2012 zu Analysetools für Webseiten (www.edoeb.admin.ch). Bei Fragen sind der Rechtsdienst oder die HK zu kontaktieren.
[47] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[48] Redaktionelle Anpassung, in Kraft seit 1. April 2019.
[49] Vgl. Art. 16 und 23 Abs. 1 Weisung Informationssicherheit an der ETH Zürich (RSETZH 203.25); Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[50] Fassung gemäss Schulleitungsbeschluss vom 17. September 2013, in Kraft seit 1. Oktober 2013.
[51] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.

Artikel 14bis Zugriffsschutzmassnahmen[52]

[1] Die Benutzer sind – unabhängig vom Schutzbedarf gemäss Weisung Informationssicherheit an der ETH Zürich - für die Geheimhaltung der persönlichen Zugriffsberechtigungsmittel und Identifikationsmethoden wie Passwörter, PINs, Private Keys, Chip-Karten, physische Schlüssel, Tokens etc. zuständig. Deren Bekanntgabe oder das Zugänglichmachen für andere Benutzer ist untersagt. Dies betrifft insbesondere die Konfiguration von persönlichen Zugangsdaten zu ETH-Services auf Systemen, die nicht von der ETH Zürich betrieben werden (z.B. Mailgateway für Mobiltelefone, externer Mailserver, der Mails von ETH-Mailserver herunterlädt, u.ä.).

[2] Besteht die Vermutung, dass ein Zugangsberechtigungsmittel oder eine Identifikationsmethode Unbefugten bekannt oder zugänglich gemacht wurde oder von diesen genutzt wird, muss der Benutzer die Zugangsberechtigung umgehend sperren lassen und den Vorfall der/dem Systemverantwortlichen melden.

[3] Die zuständigen Stellen der Informatikdienste, die Informatiksupportgruppen und das CSCS 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] Der/die Systemverantwortliche legt die Bestimmungen bezüglich Zugangsberechtigungsmittel und Identifikationsmethoden fest (z.B. Wechsel von Passwörtern). Bei erhöhtem Schutzbedarf müssen die Bestimmungen entsprechend verschärft werden.

Artikel 15 Systeme mit hohem Schutzbedarf[53]

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

[1bis] *aufgehoben*

[2] 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] Die zuständigen Systemverantwortlichen müssen entsprechende IT Best Practice Rules der Informatikdienste einhalten.

[4-9] aufgehoben

[10] Der Verlust oder die 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.[54] Bei Datenverlust ist der/die zuständige Vorgesetzte und der/die CISO zu informieren. Bei Diebstahl zusätzlich die Abteilung SGU. Im Übrigen sind die IT Best Practice Rules der Informatikdienste einzuhalten.

[52] Neu eingefügt mit Schulleitungsbeschluss vom 17. September 2013, in Kraft seit 1. Oktober 2013; Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[53] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[54] vgl. auch Anhang zur BOT Ziffer 1 Abs. 7.

Artikel 15bis Integrität des IKT-Netzwerks[55]

Das IKT-Netzwerk der ETH-Zürich darf von Benutzern oder Dritten nicht eigenmächtig erweitert oder verändert werden[56]. Ausnahmen bedürfen der schriftlichen Zustimmung der Informatikdienste.

5. Abschnitt: Verantwortlichkeit und Haftung

Artikel 16 Verantwortlichkeit[57]

[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 sowie Anordnungen der/des CISO sind für alle Benutzer verbindlich. Jeder Benutzer hat diese Anordnungen einzuhalten[58].

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

[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.[59]

6. Abschnitt: Missbrauch

Artikel 18 Protokollierung/Feststellung von Missbräuchen[60]

[1] Die IKT-Mittel protokollieren die wichtigsten auf ihnen durchgeführten Aktivitäten.

---

[55] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[56] 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.
[57] Fassung gemäss Schulleitungsbeschluss vom 17. September 2013, in Kraft seit 1. Oktober 2013.
[58] Fassung gemäss Schulleitungsbeschluss vom 17. September 2013, in Kraft seit 1. Oktober 2013.
[59] SR **170.32**
[60] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.

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

[2bis] Die Protokollierung der geschäftlichen E-Mails betrifft u.a. die Betreffzeile, Datum, Zeit, Absender- und Empfängeradressen. Private E-Mails sind von den Nutzern ausdrücklich durch die Vermerkoption „PRIVAT" zu kennzeichnen oder entsprechend getrennt abzulegen.

[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 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] Die Benutzer und Systemverantwortlichen sind verpflichtet, bei der Aufklärung von Fällen missbräuchlicher und rechtswidriger Nutzung und von Schadensfällen mitzuwirken.

Artikel 19 Missbräuchliche Nutzung[61]

[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. 261[bis] StGB);

b) Die Herstellung, die Anleitung zur Herstellung oder absichtliche Verbreitung von schädlichen Programmen oder Programmteilen im Sinne von Art. 144[bis] 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. 143[bis] 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[62] erlaubt sein, sofern vorgängig

[61] Fassung gemäss Schulleitungsbeschluss vom 17. September 2013, in Kraft seit 1. Oktober 2013.
[62] z.B. Information Security Lab, D-INFK

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 für den Netzbereich zuständigen Systemverantwortlichen und der ID Network Security Group 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 elektronischen Kommunikationsmitteln mit vorgetäuschten oder irreführenden Absenderangaben (inkl. technischer Adresse);

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-interne Massenversande im Sinne von Art. 11 Abs. 3 dieser Benutzerordnung sind 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.

[4] Die Kenntnis schwerer oder wiederholter missbräuchlicher Nutzung verpflichtet die direkten Vorgesetzten sowie die System- bzw. Netzwerkverantwortlichen zur Meldung an die/den CISO.

Artikel 20 Konsequenzen von Missbräuchen

[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; [63]

b) Vorsorgliche Sperrung des Zugangs zu IKT-Mitteln[64], 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. Diese Sanktionen sind mittels Verfügung anzuordnen. Sie fallen dahin, wenn nicht innerhalb von drei Monaten ein Disziplinarverfahren eingeleitet oder Strafanzeige erstattet wird. Mit Abschluss des Disziplinarverfahrens wird über allfällige Sanktionen neu entschieden.

[63] Fassung gemäss Schulleitungsbeschluss vom 9. April 2018, in Kraft seit 1. April 2019.
[64] vgl. Anhang Ziffer 4

[3] Die Massnahmeverfügungen gemäss Absatz 2 können innert 30 Tagen nach ihrer Eröffnung bei der ETH-Beschwerdekommission angefochten werden.

[4] Gegen fehlbare Benutzer können zudem disziplinarische Massnahmen[65] ergriffen, ein Zivilverfahren (Schadenersatzklage) eingeleitet oder Strafanzeige erstattet werden[66]. Bei schwerem Missbrauch (Art. 19 Abs. 3) wird in jedem Fall ein Disziplinarverfahren eingeleitet. Besonders schwere Fälle 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[67]. Für Mitarbeitende gilt jede Art des Missbrauchs als Verletzung der arbeitsrechtlichen Pflichten.[68]

[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.

7. Abschnitt: Besondere Vorschriften

Artikel 21 Besondere Vorschriften und Weisungen[69]

[1] Im Übrigen sind von den Benutzern, 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[70];

c) Wegleitung für die Inventarführung an der ETHZ vom Januar 2019[71];

d) Standards für Verantwortlichkeiten und Systempflege[72];

e) Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen;[73]

f) Art. 36a bis Art. 36e ETH-Gesetz[74] (Personalinformationssysteme, Studieninformationssysteme; Umgang mit Personendaten in Forschungsprojekten) sowie

[65] 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**).
[66] Das Vorgehen richtet sich nach Art. 22a Bundespersonalgesetz (BPG; SR **172.220.1**).
[67] Disziplinarordnung ETH Zürich vom 4. November 2004 (SR **414.138.1).**
[68] 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.
[69] Fassung gemäss Schulleitungsbeschluss vom 17. September 2013 in Kraft seit 1. Oktober 2013.
[70] 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.
[71] Wegleitung für die Inventarführung an der ETHZ vom Januar 2019; abrufbar unter ETH Zürich > Finanzen und Controlling > Downloads (zuletzt 21.01.2019).
[72] Standards für Verantwortlichkeiten und Systempflege vom 6. Februar 2003 (RSETHZ 203.23).
[73] Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen vom 22. Februar 2012 (SR **172.010.442**).
[74] ETH Gesetz (SR **414.110)**

g) IT-Best Practice Rules der Informatikdienste[75]

8. Abschnitt: Schlussbestimmungen

Artikel 22 Vollzug[76]

aufgehoben

Artikel 23 Aufhebung bisherigen Rechts und Inkrafttreten[77]

[1] Folgende Erlasse werden aufgehoben:

a) Die Benutzungsordnung für Telematik (BOT) vom 12. Januar 1999 (RSETHZ 203.21);

b) Regeln für die Benutzung von ETH Zürich-Informatikmitteln „zuhause" vom 12. September 1995 (SLB 120913-95);

c) Weisungen zur Computerbenützung durch Studierende vom 20. Oktober 1992/CAZ;

d) Grundsätze für die Verwendung von Software beim Einsatz von Informatikmitteln im Unterricht an der ETH Zürich vom 20. Juli 1987 (RSETHZ 305.50);

e) Informatik-Netz der ETH Zürich vom 13. September 1977 (RSETHZ 222.01);

f) Reglement über die Verwendung von Unterrichts-Software an der ETH Zürich vom 15. September 1987 (RSETHZ 305.52);

g) Benützungsordnung für Unterrichtscomputer der ETH Zürich vom 15. September 1987 (RSETHZ 305.51);

h) Richtlinien für die Dozenten betreffend Unterrichts-Software vom 26. April 1988 (RSETHZ 305.53).

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

Zürich, 19. April 2005

Im Namen der Schulleitung:

Der Präsident: Kübler

Der Delegierte: Kottusch

Teilrevision vom 26. März 2019, im Namen der Schulleitung:

[75] IT-Best Practice Rules der Informatikdienste vom August 2013 (Stand 23. Mai 2018); abrufbar unter ETH Zürich> Services&Ressourcen > IT Services > Dokumente&Publikationen > Rechtliches (zuletzt 21.01.2019).

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

[77] Redaktionelle Anpassung, in Kraft seit 1. April 2019.

Der Präsident
Joël Mesot

Die Generalsekretärin
Katharina Poiger Ruloff

Anhang[78]

Regeln zur Überwachung der Nutzung von IKT-Mitteln an 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[79]:

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:[80]

a. Daten gemäss Abs. 2 Bst. a: bis zur Archivierung der zugrundeliegenden Informationen durch das ETH-Archiv[81]; 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. Die Mitarbeitenden der ETH Zürich sind für die Aufbewahrung bzw. Löschung ihrer elektronischen Post verantwortlich.

---

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

[79] Aufzeichnung zu den Zwecken gemäss Art. 57l Regierungs- und Verwaltungsorganisationsgesetz (RVOG; SR **172.010**); redaktionelle Anpassung in Kraft seit 1.1.2019.

[80] 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**).

[81] Die ETH-Bibliothek hat für die ETH Zürich und den ETH-Rat die Funktion eines öffentlichen Archivs gemäss Archivierungsgesetz (BGA; SR **152.1**, RSETHZ 420.1).

[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[82].

[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.[83]

[8] Für die Aufbewahrung von Forschungsdaten gilt Artikel 11 der Richtlinien für Integrität in der Forschung und gute wissenschaftliche Praxis an der ETH Zürich.[84]

2. Zuständigkeiten

2.1 IT-Betreiber und Systemverantwortliche 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 Netzanschlussverantwortliche

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

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.

2.4 IT Security Officer Informatikdienste (ITSO ID)

Soweit nicht in Art. 8 Weisung Informationssicherheit an der ETH Zürich[85] 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[86] geregelt, obliegen der/dem CISO namentlich folgende Aufgaben:

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

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

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

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

[83] 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**).

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

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

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

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

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

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

3. Nicht namentlich personenbezogene Stichproben

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

[1bis] Nicht namentlich personenbezogene (anonyme, pseudonyme) Auswertungen der Daten gemäss Art. 1 Abs. 2 lit. b 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 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 umgehend der/dem CISO mitzuteilen.

4. Sichernde und vorsorgliche Massnahmen

[1] Liegt aufgrund der nicht namentlich 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:

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.

[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. Namentlich personenbezogene Auswertungen der Aufzeichnungen

[1] Die/der CISO entscheidet bei nach einer nicht namentlich 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.[87]

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.[88]

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).[89]

6. Sanktionen

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

7. Vertraulichkeit

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

---

[87] 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**).

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

[89] 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**).

[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**).