

Benutzungsordnung für Telematik an der ETH Zürich (BOT) und Anhang vom 19. April 2005

1.	Abschnitt: Allgemeine Bestimmungen.....	1
	Artikel 1 Zweck.....	1
	Artikel 2 Begriffe.....	1
	Artikel 3 Geltungsbereich.....	2
2.	Abschnitt: Zuständigkeiten	2
	Artikel 4 Infrastrukturbereich Informatik	2
	Artikel 5 IT-Sicherheitsbeauftragte(r).....	2
	Artikel 6 System- und Netzanschlussverantwortliche	3
	Artikel 7 Erscheinungsbild und Präsenz im Internet	3
3.	Abschnitt: Nutzung.....	3
	Artikel 8 Nutzungszweck und Nutzungsbefugnis	3
	Artikel 9 Nutzung von Telematik-Mitteln ausserhalb der ETH Zürich	4
	Artikel 10 Private Nutzung von ETH Zürich lizenzierter Software.....	4
	Artikel 11 Datenschutz.....	4
	Artikel 12 Kopien von Software	5
	Artikel 13 Nutzung elektronischer Kommunikationsmittel	5
4.	Abschnitt: Sicherheitsmassnahmen.....	5
	Artikel 14 Allgemeine Sicherheitsmassnahmen.....	5
	Artikel 15 Besondere Sicherheitsmassnahmen	5
5.	Abschnitt: Verantwortlichkeit und Haftung.....	6
	Artikel 16 Verantwortlichkeit	6
	Artikel 17 Haftung.....	7
6.	Abschnitt: Missbrauch	7
	Artikel 18 Protokollierung/Feststellung von Missbräuchen	7
	Artikel 19 Missbräuchliche Nutzung.....	8
	Artikel 20 Konsequenzen von Missbräuchen.....	9
7.	Abschnitt: Besondere Vorschriften.....	9
	Artikel 21 Besondere Vorschriften und Weisungen	9
8.	Abschnitt: Schlussbestimmungen.....	10
	Artikel 22 Vollzug	10
	Artikel 23 Aufhebung bisherigen Rechts und Inkrafttreten	10
	Anhang.....	11

Benutzungsordnung für Telematik an der ETH Zürich (BOT der ETH Zürich)

vom 19. April 2005

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 2003¹,

verordnet:

1. Abschnitt: Allgemeine Bestimmungen

Artikel 1 Zweck

¹Die Telematik-Mittel der Eidgenössischen Technischen Hochschule Zürich sollen in optimaler Weise für die Erfüllung der Aufgaben der ETH Zürich eingesetzt werden.

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

Artikel 2 Begriffe

¹*Telematik-Mittel* (Ressourcen) sind alle Geräte, Einrichtungen und Dienste der ETH Zürich, die zur elektronischen Bearbeitung von Daten eingesetzt werden, wie Hardware, Software, Netzwerke, Daten, Dokumentationen, Beratung und Schulung sowie nicht ETH Zürich-eigene Geräte (z.B. private Laptops) im Datennetz² der ETH Zürich.

²Unter *Anwendung* ist jeder Einsatz von Telematik-Mitteln zu verstehen.

³*Daten* bedeuten Personen- und Sachdaten.

⁴*Benutzer* sind alle Angehörigen der ETH Zürich (Art. 13 ETH-Gesetz) und Dritte (z.B. Gäste, Kongressteilnehmer, angeschlossene Organisationen, Bibliothekskunden an den öffentlichen Arbeitsplätzen) die zur Nutzung von Telematik-Mitteln der ETH Zürich berechtigt sind.

⁵*Elektronische Kommunikationsmittel* beinhalten Telefon, Fax, E-Mail, SMS, Instant Messaging, Videokonferenzsysteme und ähnliches.

⁶*Benutzereinheit* ist jede Organisationseinheit der ETH Zürich (z.B. Departemente, Institute, Professuren, Infrastrukturbereiche, Stabsstellen).

¹ RSETHZ 201.021

² Details dazu sind unter folgender Web-Adresse zu finden:
http://www.id.ethz.ch/services/list/netzwerk/used_ipnetze/index

Artikel 3 Geltungsbereich

Diese Verordnung gilt sowohl für jede Benutzung und Mitbenutzung aller ETH Zürich-eigenen Telematik-Mittel, als auch für nicht ETH Zürich-eigene Geräte, die aber im Datennetzwerk der ETH Zürich betrieben werden, und zwar durch **ETH Zürich-Angehörige** oder **Dritte**.

2. Abschnitt: Zuständigkeiten

Artikel 4 Infrastrukturbereich Informatik

¹Der Infrastrukturbereich Informatik (IB-Informatik) der ETH Zürich ist insbesondere zuständig für:

- a) die technischen Massnahmen im Bereich der TelematikSicherheit, einschliesslich der Abklärung und Dokumentation technischer Mängel, der Information darüber, der Koordination der Bestrebungen zu deren Behebung bzw. Umgehung;
- b) die Instruktion und Information der Benutzer;
- c) die technische Überwachung der Einhaltung der *Standards für Verantwortlichkeiten und Systempflege*³;
- d) die Koordination bei technischen und organisatorischen Neuerungen;
- e) die Bereitstellung der notwendigen Verschlüsselungstechniken (Art. 13 Abs. 2);
- f) die Entgegennahme der Meldung der Systemverantwortlichen betreffend Anwendungen mit erhöhtem Schutzbedarf sowie die Führung des entsprechenden Inventars (Art. 6 Abs. 3);
- g) das Erteilen von Genehmigungen (Art. 15 Abs. 8);
- 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 und den Fachhochschulen;
- k) die Unterstützung der/des IT-Sicherheitsbeauftragten bei der Wahrnehmung von deren/dessen Aufgaben gemäss den Regeln zur *Überwachung der Telematik-Nutzung an der ETH Zürich* im Anhang.

Artikel 5 IT-Sicherheitsbeauftragte(r)

¹Die Schulleitung bestimmt die/den IT-Sicherheitsbeauftragte/n für Telematik-Mittel. Er/Sie berichtet direkt an den Präsidenten.

²Dieser sollte über eine möglichst hohe IT-Fachkompetenz verfügen.

³Die/der IT-Sicherheitsbeauftragte ist insbesondere zuständig für:

- a) die Feststellung, Dokumentation und Behebung von Sicherheitsmängeln (Art. 15 Abs. 3 lit. d; Art. 17 Abs. 2). Dazu verfügt er über entsprechende organisatorische Weisungsbefugnisse;
- b) die Koordination und Beaufsichtigung der Sicherheitsmassnahmen;
- c) die Abklärung bei Verdacht auf Missbrauch einschliesslich der Sammlung von Beweisdaten (Art. 18ff.);

³ RSETHZ 203.23

- d) die Sanktionen bei Missbrauch (Art. 20) sowie;
- e) für Tätigkeiten im Rahmen der Überwachung gemäss den Regeln zur *Überwachung der Telematik-Nutzung an der ETH Zürich* im Anhang.

Artikel 6 System- und Netzanschlussverantwortliche

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

²Jede Benutzereinheit 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 Telematik-Mittel sowie eine/n Netzanschlussverantwortliche/n.

³Die/der Systemverantwortliche erstellt für ihre/seine Benutzereinheit ein Inventar der Anwendungen mit erhöhtem Schutzbedarf zuhanden des IB-Informatik.

⁴Die weiteren Aufgaben des/der Systemverantwortlichen und des Netzanschlussverantwortlichen sind in den *Standards für Verantwortlichkeiten und Systempflege*⁴ sowie in den Regeln zur *Überwachung der Telematik-Nutzung an der ETH Zürich* im Anhang dieser Benutzerordnung geregelt.

⁵Bei nicht ETH-eigenen Geräten ist der Benutzer gleichzeitig auch der Systemverantwortliche.

Artikel 7 Erscheinungsbild und Präsenz im Internet

¹Für das Erscheinungsbild der ETH Zürich im weltweiten und ETH Zürich-internen Netz (Internet/Intranet) ist der Infrastrukturbereich Corporate Communications zuständig. Er erlässt dafür die entsprechenden Ausführungsbestimmungen.⁵

²Dabei trägt die Corporate Communications den Bestimmungen der Behindertengleichstellung⁶ angemessene Rechnung.

³Kommerzielle 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

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

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

³Die Nutzung von Telematik-Mitteln für private Zwecke ist erlaubt, soweit sie nicht übermässig ist und die Erfüllung der Arbeits- oder Studienpflichten nicht beeinträchtigt.

⁴ RSETHZ 203.23

⁵ ETH Zürich Internetrichtlinien vom 1.5.1999 (RSETHZ 203.22)

⁶ Behindertengleichstellungsgesetz, BehiG, vom 13. Dezember 2003 (SR 151.3); Behindertengleichstellungsverordnung, BehiV, vom 19 November 2003 (SR 151.31)

⁴Die private Nutzung von Telematik-Mitteln der ETH Zürich darf nicht zu einer technischen Störung oder Beeinträchtigung der Nutzung für die gesetzlichen Zwecke der ETH Zürich oder zu einer unverhältnismässigen Beanspruchung oder Belastung von allgemein genutzten Ressourcen (Netzwerke, Internetzugang etc.) führen.

⁵Veränderungen durch die Benutzer an den von der ETH Zürich zur Verfügung gestellten Telematik-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 Telematik-Mittel.

⁶Eine kommerzielle Nutzung z.B. im Rahmen von Spin-Off-Verträgen ist nur nach schriftlicher Einwilligung der Vizepräsidentin/des Vizepräsidenten für Forschung, die/der auch das Entgelt festsetzt, zulässig.

⁷In Bezug auf die Aussonderung von Telematik-Mitteln gilt ferner die Weisung über das Inventarwesen an der ETH Zürich vom 1.1.2004⁷

Artikel 9 Nutzung von Telematik-Mitteln ausserhalb der ETH Zürich

¹Erbringt eine Mitarbeiterin oder ein Mitarbeiter die Arbeitsleistung im Einvernehmen mit der zuständigen Stelle zu Hause⁸, so kann dies unter entsprechender Nutzung von Telematik-Mitteln der ETH Zürich erfolgen.

²Der Einsatz von portablen ETH Zürich-eigenen Geräten wie Laptops und Organizer ausserhalb des ETH Zürich Campus ist, vorbehältlich abweichender besonderer Anordnungen, erlaubt.

Artikel 10 Private Nutzung von ETH Zürich lizenzierter Software

¹Die private Nutzung von an der ETH Zürich-lizenzierter Software ist erlaubt, für Mitarbeiterinnen und Mitarbeiter der ETH Zürich in einem mindestens 50%ige Anstellungsverhältnis sowie für an der ETH Zürich immatrikulierte Studierende, soweit dies der jeweilige Lizenzvertrag⁹ zulässt.

²Die Einräumung des Rechts, die Software auf einem privaten Computer zu installieren, ist vom jeweiligen Lizenzvertrag abhängig.

³Die gleichzeitige Nutzung von an der ETH Zürich-lizenzierter Software auf dem Privat- und Bürocomputer ist untersagt, ausser die Lizenzbestimmungen erlauben dies explizit.

Artikel 11 Datenschutz

¹Die Bearbeitung von Personendaten¹⁰ ist nur im Rahmen der gesetzlichen Zwecke der ETH Zürich sowie nach Massgabe der Datenschutzbestimmungen¹¹ erlaubt.

⁷ RSETHZ 220

⁸ Gemäss Art. 43 Abs. 3 PVO (SR 172.220.113)

⁹ Die entsprechende Zusammenstellung befindet sich auf:
<http://www.id.ethz.ch/services/list/einkauf/heimnutzung>

¹⁰ Personendaten sind gemäss Legaldefinition des Datenschutzgesetzes vom 19. Juni 1992 (SR 235.1) alle Angaben, die sich auf eine bestimmte oder bestimmbar natürliche oder juristische Person beziehen

¹¹ Datenschutzgesetz vom 19. Juni 1992 (SR 235.1); Datenschutzverordnung vom 14. Juni 1993 (SR 235.11); Art. 59 f. Personalverordnung ETH-Bereich (SR 172.220.113)

²Die Bekanntgabe von Personendaten an Dritte zur Autorisierung und Authentisierung von elektronischen Services ist erlaubt, jedoch nur soweit es sich nicht um besonders schützenswerte Daten¹² handelt und diese Personendaten für die Benutzung dieser Services notwendig sind.

Artikel 12 Kopien von Software

Das vollständige oder teilweise Kopieren von an der ETH Zürich-lizenzierte Software (Programmen und Dokumentation), gleich welcher Herkunft, ist untersagt, soweit nicht Lizenzbestimmungen oder das Urheberrechtsgesetz¹³ dies ausdrücklich erlauben.

Artikel 13 Nutzung elektronischer Kommunikationsmittel

¹Die Vertraulichkeit von Nachrichten über elektronische Kommunikationsmittel ist nicht gewährleistet.

²Das Versenden von Berufs-, Amts- und Geschäftsgeheimnissen oder anderen vertraulichen Informationen (z.B. aus Personalakten) aus dem Bereich der ETH Zürich mittels elektronischen Kommunikationsmitteln darf nur mit geeigneter Verschlüsselungstechnik erfolgen.

³Die elektronischen Kommunikationsmittel der ETH Zürich dürfen nicht anonym oder unter einem Pseudonym benutzt werden.

4. Abschnitt: Sicherheitsmassnahmen

Artikel 14 Allgemeine Sicherheitsmassnahmen

¹Anwendungen oder Systeme mit **normalem Schutzbedarf** sind solche, für die keine besonderen Schutzmassnahmen nötig sind.

²Die Systemverantwortlichen von Anwendungen oder Systemen in dieser Kategorie sind für die folgenden Sicherheitsmassnahmen selbst verantwortlich: Installation und Aktivierung der neusten Antivirus-Software; Installation der Sicherheits-Updates der Betriebssysteme; regelmässige bedarfsgerechte Sicherstellung der Daten; sofortige Meldung von Sicherheitsproblemen, Defekte, etc. an den IB-Informatik.

³Die Benutzer von Anwendungen oder Systemen in dieser Kategorie sind für die Geheimhaltung der Zugriffsinformationen zuständig.

Artikel 15 Besondere Sicherheitsmassnahmen

¹Anwendungen oder Systeme mit **erhöhtem Schutzbedarf** sind solche mit Daten, deren Verlust die gesetzlichen Zwecke der ETH Zürich wesentlich beeinträchtigen oder bedeutende Wiederherstellungskosten verursachen.

²Anwendungen oder Systeme mit erhöhtem Schutzbedarf müssen mit verschärften Mitteln gegen den Zugriff durch Unbefugte geschützt werden. Dies betrifft sowohl den Zugang zu Applikationen und Daten als auch den physischen Zugriff zu den Rechnern selber.

¹² Daten im Sinne von Art. 3 lit. c Datenschutzgesetz (SR 235.1)

¹³ Art. 24 Urheberrechtsgesetz vom 9. Oktober 1992 (SR 231.1)

³Zugangsberechtigungsverfahren und Identifikationsmethoden wie Passwörter, PINs, Chip-Karten, physische Schlüssel, Tokens etc. sind vertraulich zu behandeln. Insbesondere sind bei erhöhtem Schutzbedarf folgende Punkte situationsgerecht anzuwenden:

- a) Verschärfter Passwortschutz mit regelmässiger Kontrolle;
- b) Logout beim Verlassen des Arbeitsplatzes;
- c) sofortige Meldung von Sicherheitsproblemen;
- d) periodische Kontrolle durch den/die IT-Sicherheitsbeauftragte/n;
- e) Datenschutz durch Verschlüsselung der Datenübermittlung;
- f) Erstellen eines Konzeptes zur Datensicherung;
- g) Bestimmung der Stellvertretung des/der Systemverantwortlichen;
- h) Notfallstrategie bei längerem Systemausfall;
- i) Sicherstellung der Datenträger ausserhalb des Standortes ihrer Verarbeitung;
- j) Zutrittsschutz zum Beispiel durch Personenliste, Drehkreuz, Identifikation durch Badge, Photo oder magnetische Karte.

⁴Die Bekanntgabe oder das Zugänglichmachen von persönlichen Zugangsberechtigungsverfahren und Identifikationsmethoden an andere Benutzer ist grundsätzlich untersagt.

⁵Innerhalb von Stellvertretungsregelungen im Rahmen des Pflichtenheftes der jeweiligen Benutzer ist die Bekanntgabe oder das Zugänglichmachen unter Mitteilung an die/den Systemverantwortliche/n gestattet, soweit dies für die Stellvertretung unentbehrlich ist und keine zumutbare Alternative besteht.

⁶Der/die Systemverantwortliche der Benutzereinheiten legt die Bestimmungen bezüglich Zugangsberechtigungsverfahren und Identifikationsmethoden fest (z.B. Wechsel von Passwörtern). Bei erhöhtem Schutzbedarf müssen die Bestimmungen entsprechend verschärft werden.

⁷Besteht die Vermutung, dass ein Zugangsberechtigungsverfahren oder eine Identifikationsmethode Unbefugten bekannt oder zugänglich wurde oder von diesen genutzt wird, muss der Benutzer dies umgehend der/dem Systemverantwortlichen melden.

⁸Die Einrichtung und die Benutzung von Direktanschlüssen an ETH Zürich-fremde Kommunikationsnetze sowie das Einrichten von Direktanschlüssen an ETH Zürich-eigene Kommunikationsnetze (z.B. durch Modems) bedürfen einer schriftlichen Zustimmung des IB-Informatik.

⁹Zugriffsschutzmechanismen im Internet und Intranet (z.B. IP-Beschränkungen) dürfen durch Such- oder Beschleunigungsmechanismen (proxy- und cache-engines) nicht unberechtigterweise ausser Kraft gesetzt werden.

5. Abschnitt: Verantwortlichkeit und Haftung

Artikel 16 Verantwortlichkeit

¹Jeder Benutzer ist persönlich dafür verantwortlich, dass seine Benutzung der Telematik-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.

²Nimmt der Benutzer ohne schriftliche Zustimmung des/der zuständigen Vorgesetzten oder Dozierenden kostenpflichtige Leistungen Dritter in Anspruch, so hat er alle damit im Zusammenhang stehenden Kosten selber zu tragen.

Artikel 17 Haftung

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

²Technische und betriebliche Anordnungen des IB-Informatik, der/des Systemverantwortlichen der Benutzereinheiten oder der/des IT-Sicherheitsbeauftragten sind für alle Benutzer verbindlich. Jeder Benutzer hat diese Anordnungen einzuhalten.

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

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

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

⁶Im Übrigen gilt für Mitarbeitende der ETH Zürich bei der Benutzung der Telematik-Mittel in Erfüllung öffentlichrechtlicher Aufgaben des Bundes das Verantwortlichkeitsgesetz.¹⁴

6. Abschnitt: Missbrauch

Artikel 18 Protokollierung/Feststellung von Missbräuchen

¹Aufzeichnungen über die Nutzung der Telematik-Mittel sind zulässig für Randdaten (Adressierungsdaten im Kopf von elektronischen Nachrichten, Information zum Sessionsaufbau gem. technischem Kommunikationsprotokoll und ähnliches), insbesondere betreffend Nutzung der Server-Systeme der ETH Zürich und des ein- und ausgehenden Datenverkehrs, sowie für Rechnungsdaten und Daten zur Kontrolle der Einhaltung von Lizenzbedingungen.

²Zur Kontrolle der Einhaltung der Bestimmungen dieser Benutzungsordnung sind auf Anordnung der/des IT-Sicherheitsbeauftragten stichprobenweise anonyme Überprüfungen der Protokollierungen zulässig.

³Bei festgestellten Missbräuchen im Sinne von Art. 19 oder beim Vorliegen des Verdachts auf solche Missbräuche können die Aufzeichnungen vom IT-Sicherheitsbeauftragten zur Ermittlung der fehlbaren Personen gemäss den hierfür in den *Regeln zur Überwachung der Telematik-Nutzung an der ETH Zürich* im Anhang geltenden Grundsätzen personenbezogen ausgewertet werden.

⁴Einzelheiten zur Aufzeichnung des Nutzerverhaltens, Zuständigkeiten, Protokollierung von Missbräuchen, Aufbewahrung der Nutzungsdaten und deren Auswertung sind im Anhang zu dieser Benutzungsordnung geregelt.

⁵Die Benutzer und Systemverantwortlichen sind verpflichtet, bei der Aufklärung von Fällen missbräuchlicher und rechtswidriger Nutzung und von Schadensfällen mitzuwirken.

¹⁴ SR 170.32

Artikel 19 Missbräuchliche Nutzung

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

²Als missbräuchlich gelten insbesondere die folgenden Verhaltensweisen:

- a) Die Verarbeitung, Speicherung oder Übermittlung von Material mit widerrechtlichem oder unsittlichem Inhalt, wie z.B. Gewaltdarstellungen, Pornographie (Art. 197 des Schweizerischen Strafgesetzbuches StGB), 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 Forschung¹⁵ erlaubt sein, sofern vorgängig die schriftliche Zustimmung der Schulleitung oder der von dieser als zuständig erklärten Stelle eingeholt worden ist; Scanning nach Verwundbarkeiten in einem abgegrenzten Bereich mit dem Ziel, diese zu beseitigen, sind durch die für den Netzbereich verantwortlichen Systemverantwortlichen erlaubt.
- d) Datendiebstahl (Art. 143 StGB) und Datenbeschädigung (Art. 144bis Ziff. 1 StGB);
- e) Die Nutzung von Telematik-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) oder von unverlangten Werbe-E-Mails (Spam);
- 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 des IB-Informatik und der jeweiligen Systemverantwortlichen;

³Als schwerer Missbrauch gelten:

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

⁴Die Kenntnis schwerer oder wiederholter missbräuchlicher Nutzung verpflichtet die direkten Vorgesetzten, sowie die System- bzw. Netzwerkverantwortlichen zur Meldung an die/den IT-Sicherheitsbeauftragte/n.

¹⁵ z.B. Information Security Lab, D-INFK

Artikel 20 Konsequenzen von Missbräuchen

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

- a) Vorsorgliche Sperrung des Zugangs zu Telematik-Mitteln¹⁶, die davon betroffen sind;
- b) Blockierung missbräuchlicher und rechtswidriger Daten sowie deren Sicherung und Aufbewahrung zu Beweis Zwecken;
- c) Löschung missbräuchlicher und rechtswidriger Daten, soweit dies aus Sicherheitsgründen erforderlich ist.

²Als Sanktionen gegen Missbräuche können die fehlbaren Benutzer mit der Sperrung des Zugangs zu Telematik-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.

³Die Massnahme Verfügungen gemäss Abs. 2 können innert 30 Tagen nach ihrer Eröffnung bei der ETH-Beschwerdekommision angefochten werden.

⁴Gegen fehlbare Benutzer können zudem disziplinarische Massnahmen¹⁷ ergriffen, ein Zivilverfahren (Schadenersatzklage) eingeleitet oder Strafanzeige erstattet werden. Bei schwerem Missbrauch (Art. 19 Abs. 3) wird in jedem Fall ein Disziplinarverfahren eingeleitet. Besonders schwere Fälle können zur Exmatrikulation oder Entlassung führen.

⁵Ein schwerer Missbrauch durch Studierende gilt als nicht geringfügiger Verstoss im Sinne von Art. 8 der Disziplinarordnung ETH Zürich¹⁸.

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

7. Abschnitt: Besondere Vorschriften

Artikel 21 Besondere Vorschriften und Weisungen

¹Im Übrigen sind von den Benutzern, soweit sie ihre Tätigkeit oder die von ihnen genutzten Telematik-Mittel betreffen, die folgenden Vorschriften in ihrer jeweils aktuellen Fassung zu beachten:

- a) Allfällige besondere Weisungen der jeweiligen Benutzereinheiten betreffend Nutzung einzelner Systeme, insbesondere bezüglich Datenschutz und Datensicherheit;
- b) Ausführungsbestimmungen über den Auftritt der ETH Zürich im Internet (ETH Zürich Internet-Richtlinien) vom 1.5.1999 (Stand Juli 2003) (RSETHZ 203.22);
- c) Weisung der Finanzabteilung der ETH Zürich über das Inventarwesen an der ETH Zürich vom 1.1.2004 (RSETHZ 220);
- d) Standards für Verantwortlichkeiten und Systempflege vom 6.2.2003 (RSETHZ 203.23).

¹⁶ vgl. auch Ziffer 4 Anhang

¹⁷ 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 (SR 172.220.113)

¹⁸ SR 414.138.1

8. Abschnitt: Schlussbestimmungen

Artikel 22 Vollzug

Die Einheiten der ETH Zürich, namentlich der Infrastrukturbereich Informatik, die Abteilung Sicherheit und Umweltschutz, der Infrastrukturbereich ETH-Bibliothek, das CSCS sowie der Infrastrukturbereich Corporate Communications, können gestützt auf diese Verordnung in ihrem Kompetenzbereich zusätzliche Regeln erlassen.

Artikel 23 Aufhebung bisherigen Rechts und Inkrafttreten

¹Folgende 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 „zu Hause“ 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) Benutzungsordnung 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).

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

Zürich, 19. April 2005

Im Namen der Schulleitung

Der Präsident: Kübler

Der Delegierte: Kottusch

Anhang

Regeln zur Überwachung der Nutzung von Telematik-Mitteln an der ETH Zürich

1. Aufzeichnung von Daten

¹Die ETH Zürich ist dafür besorgt, dass die technischen Schutzmassnahmen zur Verhinderung technischer Störungen regelmässig dem neuesten Stand der Technik angepasst werden.

²Bei technischen Störungen können Protokollierungen beigezogen werden, um deren Ursache zu klären.

³Aufzeichnungen über die Nutzung der Telematik-Mittel der ETH Zürich sind zulässig für:

- a) Randdaten (Adressierungsdaten im Kopf von elektronischen Nachrichten, Information zum Sessionsaufbau gem. technischem Kommunikationsprotokoll und ähnliches), insbesondere betreffend Nutzung der Server-Systeme der ETH Zürich und des ein- und ausgehenden Datenverkehrs;
- b) Rechnungsdaten im Zusammenhang mit Telematik-Mitteln, die gegen Entgelt zur Nutzung zur Verfügung gestellt werden;
- c) Daten zur Kontrolle der Einhaltung von Lizenzbedingungen (Lizenzserver).

⁴Die einzelnen Benutzereinheiten der ETH Zürich (Departemente, Institute, Professuren, Infrastrukturbereiche, Stabsstellen) können in Ausnahmefällen für die in ihren Verantwortungsbereich fallenden Telematik-Mittel im Einverständnis mit der/dem IT-Sicherheitsbeauftragten schriftliche Weisungen erlassen über die Aufzeichnung, Aufbewahrung und Löschung der Rand-, Rechnungs- und/oder Lizenzdaten. Dabei berücksichtigen sie die Eigenart der betreffenden Telematik-Mittel, deren Nutzungszweck und die Rahmenbedingungen für deren Nutzung. Diese Informationen sind nicht länger als 3 Monate nach Abschluss des relevanten Vorganges aufzubewahren.

⁵Die Weisungen sind den Benutzern in geeigneter Weise bekannt zu machen.

2. Zuständigkeiten

2.1 Systemverantwortliche der Benutzereinheiten

- a) Einrichtung der Telematik-Mittel zur Vornahme der Aufzeichnungen gemäss Ziff. 1 dieses Anhangs.
- b) Vornahme von Stichproben gemäss Ziff. 3 auf Anordnung des IT Sicherheitsbeauftragten.
- c) Unterstützung der/des IT-Sicherheitsbeauftragten bei der Wahrnehmung von deren/dessen Aufgaben gemäss diesen Regelungen.

2.2 Netzanschlussverantwortliche

Unterstützung der/des IT-Sicherheitsbeauftragten bei der Wahrnehmung von deren/dessen Aufgaben gemäss diesen Regelungen.

2.3 IB-Informatik der ETH Zürich

Unterstützung der/des IT-Sicherheitsbeauftragten bei der Wahrnehmung von deren/dessen Aufgaben gemäss diesen Regelungen.

2.4 IT-Sicherheitsbeauftragte/r

- a) Zuständig für den Kontakt mit dem Dienst für Besondere Aufgaben (DBA) im Zusammenhang mit der Überwachung des Fernmeldeverkehrs.
- b) Anordnung der Durchführung von Stichproben gemäss Ziff. 3.
- c) Ergreifung von vorsorglichen Massnahmen gemäss Ziff. 4.
- d) Entscheid über die unmittelbare personenbezogene Auswertung von aufgezeichneten Daten bei konkretem Verdacht auf strafbares Verhalten oder bei anderen Missbräuchen gemäss Ziff. 5 Bst. a.
- e) Befragung von Angehörigen der ETH Zürich betreffend Inhalt elektronischer Nachrichten (z.B. E-Mail) gemäss Ziff. 5 Bst. d.
- f) Anordnung von personenbezogenen Aufzeichnungen in Absprache mit den zuständigen direkten Vorgesetzten (Mitarbeitende) bzw. des Rektors (Studierende) gemäss Ziff. 5 Bst. b.

3. Anonyme Stichproben

¹In Bezug auf die gemäss Ziff. 1 aufgezeichneten Daten können die Systemverantwortlichen auf Anordnung der/des IT-Sicherheitsbeauftragten stichprobenweise anonyme Überprüfungen auf missbräuchliche Nutzungen im Sinne von Art. 19 BOT vornehmen.

²Bei der Überprüfung vom elektronischen Nachrichtenaustausch (z.B. E-Mail) dürfen die Inhalte der überprüften Nachrichten nicht zur Kenntnis genommen werden.

³Anlässlich der stichprobenweisen Überprüfung festgestellte Missbräuche oder ein entsprechender Verdacht sind von den Systemverantwortlichen umgehend der/dem IT-Sicherheitsbeauftragten mitzuteilen.

4. Sichernde und vorsorgliche Massnahmen

¹Liegt aufgrund der anonymen Kontrolle ein konkreter Verdacht eines Missbrauchs im Sinne von Art. 19 BOT vor, der die Gefahr einer erheblichen Beeinträchtigung der ordentlichen Nutzung von Telematik-Mitteln der ETH Zürich oder einer Schädigung der ETH Zürich, von deren Angehörigen oder von Dritten mit sich bringt, so ist die/der IT-Sicherheitsbeauftragte zur Anordnung der folgenden sichernden und vorsorglichen Massnahmen befugt:

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

²Die in Abs. 1 erwähnten Massnahmen können in dringenden Fällen auch vom Leiter der Gruppe Netzwerksicherheit des IB-Informatik der ETH Zürich angeordnet werden, wobei die/der IT-Sicherheitsbeauftragte umgehend zu informieren ist und über die Aufrechterhaltung der getroffenen Massnahmen entscheidet.

5. Personenbezogene Auswertungen

¹Die/der IT-Sicherheitsbeauftragte entscheidet bei festgestellten Missbräuchen im Sinne von Art. 19 BOT oder beim Vorliegen des Verdachts auf solche Missbräuche nach den folgenden Grundsätzen über die personenbezogene Auswertung von aufgezeichneten Daten:

- a) Bei **Missbräuchen** die zugleich zu **technischen Störungen** führen, kann die/der IT-Sicherheitsbeauftragte die personenbezogene Auswertung zur Identifikation der für den Missbrauch verantwortlichen Person sofort anordnen. Liegt beim in Frage stehenden Missbrauch der Verdacht auf das Vorliegen **strafbarer Handlungen** nach dem schweizerischen Strafgesetzbuch (z.B. im Sinne von Art. 197, Art. 259, Art. 261, Art. 261bis StGB, Art. 143bis, Art. 144bis StGB) vor, kann eine Strafanzeige gegen die fehlbare Person erstattet werden. Der Entscheid, ob Anzeige erstattet wird, liegt beim Präsidenten.¹⁹
- b) Wenn ein Missbrauch **keine technische Störung** zur Folge hat, entscheidet der direkte Vorgesetzte (Mitarbeiter) oder der Rektor (Studierende) gemeinsam mit dem IT-Sicherheitsbeauftragten aufgrund der Schwere des Missbrauchs, ob die personenbezogene Auswertung der Protokollierung sofort oder erst nach wiederholter Feststellung eines Missbrauchs erfolgen soll. Die Angehörigen der betroffenen Benutzereinheit sind vorgängig darüber zu informieren. Im Falle des Vorliegens eines **konkreten Straftatverdachtes** erfolgt eine Strafanzeige gegen Unbekannt und die personenbezogenen Auswertungen werden von der Strafjustizbehörde vorgenommen.
- c) Bei Vorliegen von **blößen Fehlmanipulationen**, die zu technischen Störungen führen, ist eine personenbezogene Auswertung der Protokollierungen grundsätzlich untersagt, da kein Missbrauch vorliegt. Diesen Störungen ist mit dem Einsatz angemessener technischer Schutzmassnahmen zu begegnen.
- d) Ist im Zusammenhang mit dem Austausch elektronischer Nachrichten (z.B. E-Mails) das Vorliegen eines Missbrauchs nur unter der Voraussetzung der Kenntnisnahme des Inhalts der relevanten Nachrichten feststellbar, muss die/der IT-Sicherheitsbeauftragte den betreffenden Benutzer über Inhalt und Zweck der relevanten Nachrichten befragen.

6. Sanktionen

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

7. Vertraulichkeit

¹Die gemäss Ziff. 1 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.

²Über 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

¹Zuständig für den Kontakt mit dem Dienst für Besondere Aufgaben (DBA) im Zusammenhang mit der Überwachung des Fernmeldeverkehrs²⁰ im Rahmen der Ermittlung von Straftaten ist der IT-Sicherheitsbeauftragte. Dieser und auch andere Stellen der ETH Zürich informieren unverzüglich den Rechtsdienst, wenn sie vom DBA oder von Strafverfolgungsbehörden im Zusammenhang mit der Überwachung des Fernmeldeverkehrs kontaktiert werden.

²Die Vorbereitungen und Durchführung der Überwachung erfolgt nach Art. 28 und 29 der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs vom 31. Oktober 2001 (VüPF; SR 780.11).

¹⁹ Art. 14 Abs. 2 der Geschäftsordnung der Schulleitung vom 10. August 2004 (RSETHZ 202.3)

²⁰ Art. 28 und 29 der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VüPF; SR 780.11)