Reglement über den Einsatz von Informatikmitteln an der Universität Zürich (REIM)

(vom 30. November 2017)

Die Universitätsleitung beschliesst:

1. Teil: Grundlagen

§ 1. Zweck

[1]Dieses Reglement dient dazu, die Sicherheit beim Einsatz von Informatikmitteln zu gewährleisten, indem es

1. die Verantwortlichkeiten festlegt,
2. die Nutzungsbedingungen regelt und
3. die Massnahmen gegen und bei Missbrauch bestimmt.

[2]Der Einsatz von Informatikmitteln an der Universität Zürich unterliegt den Bestimmungen in diesem Reglement.

§ 2. Geltungsbereich

[1]Dieses Reglement findet Anwendung für die Benutzung von Informatikmitteln der Universität durch ihre Angehörigen sowie durch Dritte. Als Dritte gelten zum Beispiel Kursbesuchende, Kongressteilnehmende, Nachdiplom-Studierende, Bibliotheksbenutzende und Mieter von Räumen der Universität oder von Räumen, die mit dem Netzwerk der Universität versorgt sind.

[2]Das Universitätsspital (USZ) ist für seinen Bereich für den Erlass entsprechender Vorschriften selbst zuständig. Aus Sicht der IT-Sicherheitsstelle wird das USZ jedoch als Benutzereinheit im Sinne dieses Reglements behandelt.

§ 3. Begriffe

Benutzung
ist jeder Einsatz von Informatikmitteln.

Informatikmittel
sind alle Geräte, Einrichtungen und Dienste, die zur elektronischen Bearbeitung von Daten eingesetzt werden, wie Hardware, Software, Netzwerke und Netzwerkgeräte, die für die Universität Zürich verwendeten Adressierungselemente (z.B. IP-Adressen) sowie die gespeicherten Daten selbst.

Angehörige der Universität
umfasst den Lehrkörper, den Mittelbau, die Studierenden sowie das administrativ-technische Personal gemäss Universitätsgesetz und Universitätsordnung.

Endbenutzende
sind diejenigen Benutzenden, welche einen Computer verwenden und keine Einrichtungs- und Unterhaltsarbeiten des Computersystems vornehmen.

Systemadministrierende
sind die Benutzenden eines Computersystems, welche daran Einrichtungs- und Unterhaltsarbeiten vornehmen.

Benutzereinheiten
sind Dekanate, Institute, Kliniken, Seminare, Abteilungen der Zentralen Dienste, Bibliotheken,

Kompetenzzentren, universitäre Vereine und teilweise Spin-Off-Firmen in den Räumlichkeiten der Universität, die bei der Zentralen Informatik als Dienstleistungsnehmende registriert sind.

Dezentrale IT-Verantwortliche
sind die IT-Verantwortlichen der Benutzereinheiten.

Isolation vom Netzwerk
bezeichnet in diesem Dokument die Trennung eines Computers vom Netzwerk (z. B. durch Ausstecken des Datenkabels).

Starke Passwörter
sind mindestens 8 Zeichen lang, haben aus jeder der vier Buchstabengruppen Grossbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen (wie Satzzeichen u.ä.) mindestens ein Element und dürfen keine erkennbare Konstruktionsregel aufweisen.

Persönliche Passwörter
sind einer Person zugeteilt oder werden von ihr bestimmt.

Gruppen-Passwörter
sind Passwörter, die aus organisatorischen Gründen einer Gruppe bekannt sein müssen.

Peer-to-Peer-Programme
sind Programme, die sowohl Server- als auch Client-Funktionen wahrnehmen.

2. Teil: Organisation und Verantwortung

§ 4. Endbenutzende und Systemadministratoren

[1]Die Endbenutzenden sind für den Einsatz und die Systempflege ihrer Informatikmittel verantwortlich. Die Benutzereinheiten können die Verantwortung für die Systempflege ganz oder teilweise von ihren Endbenutzenden auf die IT-Verantwortlichen übertragen.

[2]Diesem Reglement unterstehen auch als Systemadministrierende beigezogene externe Fachleute oder Firmen.

[3]Bei schwerwiegenden Störungen des Computers müssen die Endbenutzenden den Computer ausser Betrieb nehmen oder isolieren und die Systemadministrierenden beiziehen.

[4]Endbenutzende, die keiner Benutzereinheit angehören, dürfen keine Server und keine Peer-to-Peer-Programme einrichten oder einrichten lassen und betreiben. Sie dürfen nur Systeme ohne besondere Sicherheitsanforderungen im Sinne von §12 betreiben. Die Zentrale Informatik kann Ausnahmen von Peer-to-Peer-Programmen publizieren und Vorschriften für deren Betrieb erlassen.

§ 5. Benutzereinheiten

[1]Die Benutzereinheiten setzen Informatikmittel für die Tätigkeit ihrer Endbenutzenden, für Betriebsabläufe (z.B. Drucker, Fileserver, Forschungsrechner) und für allgemeine Informatikdienstleistungen (z.B. Webauftritt) ein.

[2]Jede Benutzereinheit ist für diese Informatikmittel, die technischen und betrieblichen Belange im Zusammenhang mit Informatikmitteln und die Einhaltung dieses Reglements verantwortlich. Zur Erfüllung dieser Aufgaben bezeichnet sie eine qualifizierte IT-Verantwortliche oder einen qualifizierten IT-Verantwortlichen und meldet diese oder diesen bei der Zentralen Informatik an.

[3]Die von der Zentralen Informatik im Web publizierten Guidelines für die dezentralen IT-Verantwortlichen regeln Rechte und Pflichten der IT-Verantwortlichen und deren Zusammenarbeit mit der Zentralen Informatik. Im Auftrag der Benutzereinheiten dürfen die IT-Verantwortlichen

1. die zugeteilten Netzwerkbereiche und eigenen Computer mit dem Ziel kontrollieren, das ordnungsgemässe Funktionieren und die Sicherheit dieser Informatikmittel zu gewährleisten,

2. Server und Peer-to-Peer-Programme einrichten oder einrichten lassen.

[4]Die IT-Verantwortlichen der Benutzereinheiten sorgen dafür, dass sich von einer IP-Adresse ihres Netzwerkbereichs auf die Person zurückschliessen lässt, von welcher der entsprechende Computer verwendet wurde oder, z. B. im Falle von Schulungsräumen, zumindest der konkret benützte Computer eruiert werden kann. Es ist sicherzustellen, dass entsprechende Rückschlüsse über einen Zeitraum von einem halben Jahr erfolgen können. Dies gilt auch bei temporär und automatisch zugeteilten IP-Adressen.

[5]Jede Benutzereinheit führt ein Inventar über die in ihrem Bereich betriebenen Informatikgeräte.

§ 6. Zentrale Informatik

[1]Die Zentrale Informatik ist alleine oder in Absprache mit dem Rechtsdienst insbesondere zuständig für

1. den Aufbau und Betrieb der zentralen Informatikmittel, das Netzwerk und das zentrale Angebot der Informatikdienstleistungen an die Studierenden und die Benutzereinheiten,
2. das Angebot von Beratung und Unterstützung in Sicherheits-Belangen der IT,
3. den Erlass des IT-Sicherheitsreglements der Universität,
4. den Erlass der Regelungen für die Protokollierungen von Systemvorgängen (Logfile-Policy),
5. den Erlass von technischen Ausführungsbestimmungen.

[2]Die Zentrale Informatik kann einschränkende Massnahmen für die Benutzung des Netzwerks verfügen. Insbesondere ist sie berechtigt, unzulässige Aktivitäten im Netzwerk technisch zu verhindern.

[3]Die Zentrale Informatik kann angemessene Massnahmen zur Eindämmung von Missbrauch und Schadprogrammen, wie Firewalls, Spamfilter, Anti-Spoofing-Filter oder Virenschutz an strategischen Punkten im Netzwerk einsetzen.

§ 7. IT-Sicherheitsstelle

[1]Die IT-Sicherheitsstelle der Universität ist eine Stabsstelle der Zentralen Informatik.

[2]Die IT-Sicherheitsstelle vertritt die Interessen der Universität gegenüber den Internet-Betreibern. Die Benutzereinheiten und Endbenutzenden sind dazu verpflichtet, die IT-Sicherheitsstelle bei der Bearbeitung von Beanstandungen der Internet Community zu unterstützen.

[3]Sie ist zuständig für die generelle Überwachung des Universitätsnetzwerks, insbesondere was die Suche nach Sicherheitsmängeln betrifft. Sie schlägt Sicherheitsmassnahmen vor und gibt Sicherheitsempfehlungen ab.

[4]Die IT-Sicherheitsstelle beanstandet Sicherheitsmängel und leichte Missbräuche direkt bei den zuständigen Endbenutzenden oder IT-Verantwortlichen. Führt diese Beanstandung nicht zu einer Beendigung des Fehlverhaltens, kann die Leitung der Benutzereinheit informiert werden. Die IT-Sicherheitsstelle kann für die Abklärung von Sicherheitsmängeln die Verantwortlichen und externe Hilfen beiziehen.

[5]Die IT-Sicherheitsstelle kann die Isolation von Computern vom Netzwerk anordnen oder notfalls erzwingen.

[6]Die IT-Sicherheitsstelle meldet schwere Missbräuche dem Sicherheitsdienst, dieser leitet unter Beizug des Rechtsdienstes die notwendigen Massnahmen ein.

3. Teil: Einsatz von Informatikmitteln

§ 8. Bedingungen

[1]Die universitären Informatikmittel, insbesondere auch das Netzwerk, sind zur Erfüllung universitärer Aufgaben einzusetzen. IT-Dienste, welche Infrastrukturleistungen (Netzwerkbandbreite, Strom, Kühlung, etc.) der Universität stark beanspruchen, sind in Zusammenarbeit mit den zuständigen Stellen der Zentralen Dienste zu planen. In jedem Fall ist auch die Zentrale Informatik zu informieren. Eine kommerzielle Nutzung zur Erfüllung nicht-universitärer Aufgaben durch Mieter von Räumen der Universität ist nur nach schriftlicher Einwilligung der Universitätsleitung zulässig.

[2]Der Einsatz von Informatikmitteln für private nicht-kommerzielle Zwecke ist grundsätzlich gestattet, soweit dieser in geringem Rahmen geschieht. Um die Aufgabenerfüllung des einzelnen Informatikmittels sicherzustellen, kann die Leitung einer Benutzereinheit für diese zusätzlichen Nutzungsvorschriften erstellen und insbesondere die private Nutzung einschränken oder verbieten.

[3]Der Einsatz von Informatikmitteln für private kommerzielle Nutzung ist untersagt.

[4]Unzulässig sind allgemein jegliche Form des Konsums von rechtswidrigen, pornographischen, rassistischen, sexistischen oder Gewalt verherrlichenden Inhalten. Ausnahmen können im begründeten Einzelfall bei nachweislich genehmigten Zwecken, z. B. für Forschung, Lehre, Kunst, Ausbildung oder offizielle Aufgaben, gemacht werden. Unter Konsum wird Nutzung, Verarbeitung, Speicherung, Übermittlung und/oder Weiterverbreitung insbesondere von Internetangeboten, E-Mails, Mitteilungen in Nachrichtendiensten, Bild-/Tonaufnahmen oder sonstigen Abbildungen verstanden.

[5]Ausleihe, Vermietung und Verkauf der Informatikmittel sind bewilligungspflichtig. Die Bewilligung wird durch die Leitung der Benutzereinheit erteilt.

§ 9. Bewilligungspflichtige Anwendungen

[1]Im Zusammenhang mit dem öffentlichen Webauftritt der Universität Zürich gibt es eine Bewilligungspflicht. Zuständig dafür ist die Abteilung Kommunikation.

Bewilligungspflichtig sind ausserdem

1. Die Verbindungen mit universitätsfremden Netzwerken, wie Modemleitungen oder Tunnelverbindungen von ausserhalb der Universität ins Netzwerk der Universität, die nicht an einem entsprechenden Dienst der Zentralen Informatik, wie Modem-Einwahl, VPN-Server, enden. Zuständig ist die IT-Sicherheitsstelle.
2. Die Massenversände per E-Mail an Angehörige der Universität. Die Universitätsleitung beauftragt eine Abteilung der UZH mit der Betreuung von Massenversänden. Die von dieser Abteilung bewilligten Versände (Umfragen, universitäre Veranstaltungen etc.) werden von der Zentralen Informatik ausgeführt, ohne dass die Antragstellenden in den Besitz der E-Mail-Adressen der Zielgruppen gelangen. Von der Bewilligungspflicht ausgenommen sind Versände durch Universitätspersonal betreffend Angelegenheiten, die unmittelbar mit der Aufrechterhaltung des Betriebes von Lehre, Forschung und Zentralen Diensten zusammenhängen.
3. Das Einrichten eines Computers mit einer statischen IP-Adresse. Zuständig ist die für den örtlich gültigen Netzwerknummernbereich zuständige Benutzereinheit.

§ 10. Nicht erlaubte Anwendungen

Untersagt ist

1. Das Betreiben von Mail-Servern, welche von ausserhalb der Universität direkt ansprechbar sind oder die Mailserver ausserhalb des Universitätsnetzwerks direkt kontaktieren. Vorbehalten ist das Weiterbetreiben der bisher betriebenen und bei der Zentralen Informatik registrierten Mailserver einzelner Benutzereinheiten.

2. Das Betreiben von Kommunikationsleitungen oder Tunnelverbindungen, welche an Endpunkten sowohl innerhalb als auch ausserhalb der Universität eine Vermittlungsfunktion ins örtliche Internet ausführen und somit eine weitere Datenverbindung ins Internet darstellen.
3. Das Weiterbetreiben von Netzwerk-Diensten von welchen bekannt ist, dass damit in schwerwiegender Weise Missbrauch betrieben wird, und das ungeschützte Weiterbetreiben von Computern, bei denen unbefugte Dritte Administratorenrechte erlangt haben oder sie sonst wie in störender oder gefährdender Weise missbrauchen konnten.
4. Untersagt ist grundsätzlich die Publikation von Webseiten, die den Webbrowser der Aufrufenden ohne deren bewusste Entscheidung dazu bringen, Seiten oder Dienste von ausserhalb der UZH nachzuladen. Insbesondere verboten sind das Einbetten von Bildern, Scripts, Iframes und Applets mit Angabe einer fremden Datenquelle und das Einbetten von Scripts oder Applets, die Entsprechendes bewirken. Ausnahmen sind nur möglich, wenn der Datenschutz gewährleistet ist, insbesondere durch Abschluss eines entsprechenden Vertrages.
5. Untersagt ist das Anbieten von Webseiten oder Netzwerkdiensten ohne inhaltliche Kontrolle, welche das anonyme Auftreten von Dritten ermöglichen.

§ 11. Datenschutz

[1]Jeglicher Einsatz von Informatikmitteln, der die Privatsphäre anderer Personen verletzt, ist untersagt. Personendaten dürfen nur soweit erfasst, verarbeitet und weitergegeben werden, als dies zur Ausführung der anvertrauten Aufgabe innerhalb der Universität notwendig ist. Die einschlägigen Datenschutz- und Archivierungsbestimmungen sind einzuhalten.

[2]Die Benutzerinnen und Benutzer von Informatikmitteln sind dafür verantwortlich, dass Daten nicht durch unbefugte Dritte missbräuchlich verwendet werden.

§ 12. Sicherheitsvorschriften

[1]Die Systeme sind so zu pflegen, dass sie vor Missbrauch durch Dritte bestmöglich geschützt sind. Insbesondere ist dafür Sorge zu tragen, dass ein Angriff auf weitere Computer im Netzwerk und die Ausbreitung von schädlichen Programmcodes möglichst wirksam verhindert wird.

[2]Passwörter und PINs müssen geheim gehalten werden. Die Benutzerinnen und Benutzer sind für Wahl, Vertraulichkeit und Qualität ihrer Passwörter verantwortlich. Persönliche Authentisierungsmittel (wie z.B. Passwörter, Zertifikate, Hardware Token und Badges) und Schlüssel dürfen nicht an Dritte weitergegeben werden. Passwörter, die durch die Benutzerinnen und Benutzer im Rahmen ihrer Aktivitäten im Umgang mit Systemen der Universität Zürich eingesetzt werden, dürfen nicht für Zugriffe auf andere Systeme (z.B. im privaten Bereich oder für externe Systeme und Services im Internet welche nicht in Verbindung mit Tätigkeiten an der UZH stehen) verwendet werden.

[3]Wo Passwörter verwendet werden, sind starke persönliche Passwörter oder starke Gruppen-Passwörter einzusetzen. Persönliche Passwörter dürfen keiner anderen Person mitgeteilt oder zugänglich gemacht werden. Für Gruppenpasswörter ist ein Passwort-Verantwortlicher bestimmt, der alle Gruppenmitglieder persönlich kennt und das Passwort jederzeit, insbesondere auf Anweisung der IT-Sicherheitsstelle, ändern kann.

Für jeden Computer sind die Sicherheitsanforderungen bezüglich

1. Vertraulichkeit und Zugangsschutz,
2. Datensicherheit und
3. Verfügbarkeit

festzulegen und mit geeigneten Massnahmen sicherzustellen.

[4]Es sind die *Normen für den Betrieb von Systemen an der Universität Zürich* einzuhalten. Für Systeme, welche erhöhte Sicherheitsanforderungen haben oder die aufgrund der besonderen Umstände die Normen nicht in allen Punkten erfüllen können, müssen vertretbare alternative Sicherheitskonzepte

schriftlich festgehalten und umgesetzt werden. Die hier geforderte Dokumentationspflicht kann bei gemeinsam gepflegten Computern durch summarische bzw. tabellarische Aufstellungen erfüllt werden.

[5] Es sind nur Zugriffe im Rahmen der erhaltenen Zugriffsberechtigungen mit den zugeteilten Identifikations- und Authentisierungsmitteln erlaubt. Benutzerinnen und Benutzer sind für ihre Zugriffe auf IT-Systeme und Anwendungen verantwortlich, sowie für Zugriffe durch Dritte, welche aufgrund von fahrlässigem Verhalten der Benutzerinnen und Benutzer erfolgen. Stellen Benutzerinnen und Benutzer fest, dass sie Zugriff auf Informationen haben die nicht zur Erfüllung ihrer Tätigkeiten erforderlich sind, oder decken einen Missbrauch der eigenen Identifikationsmittel auf, so ist dies umgehend der vorgesetzten Stelle und dem IT–Service Desk oder der IT–Sicherheitsstelle zu melden.

§ 13. Überwachung

[1]Das Netzwerk der Universität und einzelne IT-Dienste werden überwacht. Im Vordergrund der Überwachung stehen die Erkennung des Missbrauchs von Informatikmitteln durch Dritte und die Bedürfnisse der Ressourcenplanung.

[2]Es besteht keine Möglichkeit, E-Mail als privat zu bezeichnen und bezüglich Protokollierung speziell behandeln zu lassen; die E-Mails können jedoch verschlüsselt werden.

[3]Weitere Bestimmungen sind in den von der Zentralen Informatik erlassenen Regelungen für die Protokollierung von Systemvorgängen (Logfile-Policy) enthalten.

4. Teil: Missbrauch und Folgen von Missbrauch

§ 14. Missbrauch

[1]Die Verletzung von Bestimmungen dieses Reglements oder anderer universitärer Reglemente durch den Einsatz oder die Benutzung von Informatikmitteln der Universität stellen einen Missbrauch dar und gegen den Verursacher dieser Verletzungen können Massnahmen ergriffen werden.

[2]Insbesondere sind die folgenden Handlungen missbräuchlich:

1. Nutzung, Verarbeitung, Speicherung, Übermittlung oder Weiterverbreitung von Daten, insbesondere von E-Mails oder Internetseiten, mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder Gewalt verherrlichendem Inhalt.
2. Der Einsatz von E-Mail oder Webseiten zur Belästigung, Verunglimpfung oder Schädigung anderer Personen.
3. Widerrechtliches Herunterladen, Kopieren oder Installieren von Daten und Software jeglicher Art.
4. Verwenden der Informatikmittel in einer Weise, welche die Verletzung von Immaterialgüterrechten Dritter zur Folge hat.
5. Nichtbeachtung der Gesetzgebung zum Schutz von Personendaten.
6. Erstellen oder Verbreiten von schädlichen Programmcodes (z. B. Viren, Trojaner, Würmer).
7. Das unberechtigte Absuchen (Scannen) des Netzwerks innerhalb und ausserhalb der Universität; berechtigt sind nur die IT-Verantwortlichen der Benutzereinheiten für die ihnen zugeteilten Netzwerkbereiche sowie die IT-Sicherheitsstelle für das gesamte Netzwerk der Universität.
8. Der Versuch, unberechtigt in ein Computersystem einzudringen oder höhere als die zugeteilten Berechtigungen zu erlangen.
9. Verwenden von vorgetäuschten IP-Adressen oder E-Mail-Absender-Adressen.
10. Versenden von Massen-E-Mails mit Ausnahme der gemäss § 9 Ziff. 2 erlaubten Anwendungen.
11. Betreiben von Servern in einer Weise, die Missbrauch durch anonyme Dritte, anonyme Versände von Spam-Mails, Hackerangriffe oder illegalen Datenaustausch begünstigen.

12. Betrieb von gehackten oder befallenen Systemen am Netzwerk.

§ 15. Massnahmen bei Missbrauch oder Missbrauchsverdacht

[1]Die Universitätsleitung weist die Mitarbeitenden darauf hin, dass der Internet-Zugriff oder E-Mail-Verkehr protokolliert wird. Er kann personenbezogen ausgewertet werden, wenn

1. bei Internet-Zugriffen Missbräuche von erheblicher Tragweite vorliegen oder
2. beim E-Mail-Verkehr ein konkreter Verdacht auf Missbrauch besteht.

[2]Nach erfolgter Abmahnung durch die Vorgesetzte oder den Vorgesetzten kann der Sicherheitsdienst bei der Zentralen Informatik personenbezogene Berichte über die Internet-Zugriffe oder den E-Mail-Verkehr beantragen.

[3]Personenbezogene Berichte dürfen für höchstens drei Monate erstellt werden.

[4]Die Zentrale Informatik stellt dem Sicherheitsdienst die Berichte zu.

[5]Bei begründetem Verdacht auf Missbrauch entscheidet der Sicherheitsdienst, ob er Antrag stellt, dass gegen die betreffende Person ein Administrativ- oder Disziplinarverfahren eingeleitet wird oder ob er diesen nur abmahnt. Wird keine Untersuchung eingeleitet sind die personenbezogenen Daten zu vernichten.

[6]Zur Behebung eines Missbrauchs kann die Zentrale Informatik, insbesondere die IT-Sicherheitsstelle, alle zur Aufrechterhaltung bzw. Wiederherstellung des rechtmässigen Zustandes erforderlichen Massnahmen treffen, wie:

1. Meldung des Verstosses an den Sicherheitsdienst,
2. Ermittlung der Störungsursache in Zusammenarbeit mit dem IT-Verantwortlichen oder der Leitung der Benutzereinheit;
3. Aufforderung der verantwortlichen Benutzenden zur Behebung des störenden Zustands;
4. Setzung von Fristen zur Wiederherstellung des rechtmässigen Zustands;
5. Sperrung eines Kontos bis zur sicheren Rückgabe an den rechtmässigen Benutzer,
6. Sperrung eines Kontos zur Einholung einer schriftlichen Zusicherung der Einhaltung dieses Reglements.

[7]Bei begründetem Verdacht auf Missbrauch kann die Zentrale Informatik Anschlüsse oder Dienste vorsorglich sperren oder sperren lassen. Sie sorgen dafür, dass die fraglichen Daten gesucht und aufbewahrt werden.

[8]Rechtswidrige und missbräuchliche Daten können von der Universität blockiert und zu Beweiszwecken aufbewahrt werden. Wird von einem Verfahren wegen Missbrauch abgesehen oder ist ein Verfahren abgeschlossen, werden sie gelöscht.

5. Teil: Schlussbestimmung

§ 16. Inkrafttreten

Das vorliegende Reglement tritt am 30. November 2017 in Kraft.

Zürich, 31. Oktober 2017

Im Namen der Universitätsleitung

Der Rektor:	Die Generalsekretärin:
Prof. Dr. Michael Hengartner	Dr. Rita Stöckli