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

(vom 29.11.2022)

Die Universitätsleitung,

gestützt auf § 31 Abs. 4 des Universitätsgesetzes vom 15. März 1998[1],

beschliesst:

A. Grundlagen

§ 1. Gegenstand und Zweck

Dieses Reglement regelt:

1. die Verantwortlichkeiten innerhalb der UZH für den gesetzeskonformen Betrieb und die Nutzung von Informatikmitteln der UZH;
2. die Nutzungsbedingungen für die Informatikmittel der UZH;
3. die Überwachung der Informatikmittel der UZH zur Verhinderung von Missbrauch, zur Gewährleistung des sicheren Betriebs und zur Ressourcenplanung;
4. die Massnahmen im Falle von Missbrauch der Informatikmittel der UZH;
5. die Auswertung von Protokollen und die Bearbeitung von personenbezogenen Daten im Rahmen der Überwachung von Informatikmitteln der UZH oder bei Verdacht auf Nichteinhaltung des vorliegenden Reglements;
6. die Nutzung von privaten elektronischen Geräten zu dienstlichen oder schulischen Zwecken, insbesondere den Zugriff auf Netzwerkdienste und das Verarbeiten und Speichern organisations- oder unternehmensinterner Daten (*«Bring your own Device»*).

§ 2. Geltungsbereich

[1]Dieses Reglement gilt für alle Angehörigen und Organisationseinheiten der UZH.

[2]Das Reglement gilt auch für Dritte, denen Zugriff auf Informatikmittel der UZH gewährt wird. Dazu gehören u.a. externe Fachpersonen oder Firmen, die als Systemadministrierende beigezogen werden.

§ 3. Begriffe

Angehörige der UZH
Das Universitätspersonal (Professorenschaft, Mittelbau und administratives und technisches Personal), die Lehrpersonen gemäss §§ 12d und 12e des Universitätsgesetzes (UniG) und die Studierenden gemäss § 13 Abs. 1-3 UniG.

Benutzende
Alle natürlichen Personen, die als Angehörige der UZH, als Dritte oder als Angehörige eines Dritten Informatikmittel der UZH benutzen.

BYOD-Gerät
UZH-fremde resp. private Endgeräte wie Notebooks, Tablets oder Smartphones, die mit dem Netzwerk der UZH verbunden werden («bring your own device»).

Dritte
Natürliche oder juristische Personen, die nicht Angehörige der UZH sind, wie beispielsweise:

a. Lieferant:innen, Dienstleister:innen, Besucher:innen der UZH-Räumlichkeiten, Auditor:innen, Kursbesucher:innen, Kongressteilnehmer:innen, assoziierte Institute, Benutzer:innen von Bibliotheken und Mieter:innen von Räumen, die mit Informatikmitteln der UZH ausgestattet sind.

b. externe Fachpersonen oder Firmen, die für Entwicklungen, Betrieb oder Unterhaltsarbeiten an Informatikmitteln der UZH beigezogen werden.

Informatikmittel der UZH
Alle Geräte, Einrichtungen und Dienste, welche durch die UZH zur Verfügung gestellt werden und die zur elektronischen Bearbeitung von Daten oder für die Kommunikation eingesetzt werden. Unter den Begriff der Informatikmittel der UZH fallen daher insbesondere von der UZH zur Verfügung gestellte:

a. Hardware wie Computer, Drucker, Telefone, mobile Geräte (Notebooks, Smartphones, Tablets etc.) und Geräte, die Teil des Internet of Things sind;
b. Software (Anwendungen, Betriebssysteme, Apps etc.);
c. Dateiablagen und Datenbanken;
d. E-Mail und andere digitale Kommunikationsmittel;
e. Audio-, Video- und andere Multimediageräte;
f. Cloud Services;
g. Webbasierte Plattformen;
h. Netzwerke und Netzwerkgeräte;
i. Zugangspunkte (Accesspoints) zum Internet;
j. Adressierungselemente (z.B. IP-Adressen).

Informationen der UZH
Alle Daten, welche in Erfüllung einer öffentlichen oder nicht-öffentlichen Aufgabe oder im Auftrag der UZH aufgezeichnet werden, unabhängig von ihrer Darstellungsform und ihrem Informationsträger und auch dann, wenn sie noch nicht fertiggestellt sind oder ausschliesslich dem persönlichen Gebrauch dienen.

IT-Sicherheit
Funktionssicherheit (fehlerfreies Funktionieren und Zuverlässigkeit) von Anwendungen und IT-Systemen.

IT-Störung / IT-Notfall
Eine IT-Störung ist eine Situation, in der bestimmte Bereiche, Prozesse oder Ressourcen nicht wie vorgesehen funktionieren, ohne dass schwerwiegende Schäden entstehen.

Ein IT-Notfall ist eine Situation, in der wesentliche Bereiche, Prozesse oder Ressourcen nicht wie vorgesehen funktionieren, so dass sofort oder innert kurzer Zeit schwerwiegende Schäden entstehen oder entstehenden können.

IT-Verantwortliche
Die IT-Verantwortlichen sind die von den Organisationseinheiten bezeichneten Mitarbeitenden, die für IT-Belange in ihrer jeweiligen Organisationseinheit verantwortlich sind. Weitere Angaben zu den Aufgaben und Verantwortlichkeiten sind in § 5 enthalten.

Organisationseinheit
Abteilungen, Fakultäten, Institute und alle weiteren organisatorischen Einheiten der UZH sowie Dritte, die rechtlich selbständig sind und denen Zugang zu Informatikmitteln der UZH gewährt wird.

Peer-to-Peer-Kommunikation
Dezentrale Kommunikation, bei der jeder Computer über die nötigen Voraussetzungen verfügt und eine Kommunikationssitzung starten kann. Im Gegensatz zum Client-Server-Modell, bei dem der Client eine Dienstanforderung stellt und der Server die Anfrage beantwortet, kann jeder Knoten gleichzeitig sowohl als Client als auch als Server arbeiten.

Systemadministrierende
Benutzende mit Administratorenrechten, welche an den von ihnen betreuten IT-Systemen Einrichtungs- und Unterhaltsarbeiten vornehmen können. Weitere Angaben zu den Aufgaben und Verantwortlichkeiten sind in § 4 enthalten.

Zentrale Informatik
Die Zentrale Informatik ist eine Abteilung der Zentralen Dienste der UZH. Weitere Angaben zu den Aufgaben und Verantwortlichkeiten sind in § 6 enthalten.

B. Organisation und Verantwortung

§ 4. Benutzende und Systemadministrierende

[1]Die Benutzenden sind für den ordnungsgemässen Einsatz der ihnen zur Verfügung gestellten Informatikmittel der UZH und der von ihnen eingesetzten BYOD-Geräte verantwortlich. Die Organisationseinheiten können die Verantwortung für die Systempflege von Informatikmitteln der UZH ganz oder teilweise von ihren Benutzenden auf die IT-Verantwortlichen übertragen.

[2]Die Systemadministrierenden sind für die Konfiguration, den Betrieb, die Überwachung und die Pflege der von ihnen betreuten Informatikmittel der UZH verantwortlich.

§ 5. Organisationseinheiten und IT-Verantwortliche

[1]Jede Organisationseinheit ist für ihre Informatikmittel, die technischen und betrieblichen Belange im Zusammenhang mit Informatikmitteln und die Einhaltung dieses Reglements verantwortlich. Zur Erfüllung dieser Aufgaben bezeichnet sie eine sachkundige IT-Verantwortliche oder einen sachkundigen IT-Verantwortlichen und meldet diese oder diesen bei der Zentralen Informatik an. Die Funktion der oder des IT-Verantwortlichen kann nicht an Dritte delegiert werden.

[2]Die IT-Verantwortlichen sind gemeinsam mit der Zentralen Informatik für den Betrieb der Informatikmittel der UZH verantwortlich. Die IT-Verantwortlichen sind primär für die Informatikmittel ihrer jeweiligen Organisationseinheit zuständig[1].

[3]Die von der Zentralen Informatik herausgegebenen Richtlinien für die IT-Verantwortlichen[2] regeln Rechte und Pflichten der IT-Verantwortlichen und deren Zusammenarbeit mit der Zentralen Informatik.

[4]Im Auftrag der Organisationseinheiten dürfen die IT-Verantwortlichen:

a. die zugeteilten Netzwerkbereiche und Informatikmittel ihrer jeweiligen Einheit mit dem Ziel kontrollieren, das ordnungsgemässe Funktionieren und die Sicherheit dieser Informatikmittel zu gewährleisten;

b. Server und Peer-to-Peer-Kommunikation einrichten oder einrichten lassen.

[5]Jede Organisationseinheit führt ein Inventar über die in ihrem Bereich betriebenen Informatikmittel der UZH.

§ 6. Zentrale Informatik der UZH

[1]Die Zentrale Informatik ist gemeinsam mit den IT-Verantwortlichen für den Betrieb der Informatikmittel der UZH verantwortlich.

[2]Die Zentrale Informatik ist insbesondere zuständig für:

a. den Aufbau und Betrieb der zentralen IT-Systeme, des Netzwerks der UZH und der strategischen Anwendungen;

b. das Angebot von Beratung und Unterstützung für die angebotenen IT-Dienstleistungen;

c. das Angebot von Beratung und Unterstützung in IT-Sicherheitsbelangen;

d. den Erlass einer Weisung für die Protokollierungen von Systemvorgängen *(«Logfile-Policy»)*;

e. den Erlass der *«Weisung über die Netzwerksicherheit (WNS)»;*

f. den Erlass von weiteren IT-Sicherheitsregelungen;

g. den Erlass von weiteren Ausführungsbestimmungen, insbesondere technischer Natur (z.B. *«Weisung für den Betrieb von Systemen»*).

[1] https://t.uzh.ch/1nO
[2] https://t.uzh.ch/1nP

[3]Das Netzwerk der UZH wird grundsätzlich von der Zentralen Informatik zur Verfügung gestellt. Es liegt in ihrer Verantwortung, einschränkende Massnahmen für die Benutzung des Netzwerks umzusetzen oder anzuordnen, sofern diese im Gesamtinteresse der UZH sind. Insbesondere ist die Zentrale Informatik berechtigt, rechtlich unzulässige Aktivitäten im Netzwerk technisch zu verhindern.

[4]Die Zentrale Informatik kann angemessene Massnahmen zur Eindämmung von Missbrauch und Schadprogrammen, wie z.B. Firewalls, Spamfilter, Anti-Spoofing-Filter, Virenschutz oder Monitoring-Systeme an strategischen Punkten im Netzwerk umsetzen oder anordnen.

§ 7. IT-Sicherheitsstelle

[1]Die IT-Sicherheitsstelle der UZH ist eine Stelle der Zentralen Informatik.

[2]Die IT-Sicherheitsstelle ist verantwortlich für die generelle Überwachung des Netzwerks der UZH, insbesondere was das Feststellen von IT-Sicherheitsmängeln betrifft. Sie schlägt Sicherheitsmassnahmen vor und gibt Sicherheitsempfehlungen ab, um die IT-Anwendungen und -Systeme (inkl. Netzwerke) vor äusseren Einwirkungen und vor unbefugtem Zugriff zu schützen. Sie kann für die Abklärung von IT-Sicherheitsmängeln die IT-Verantwortlichen und externe Fachpersonen beiziehen.

[3]Die IT-Sicherheitsstelle beanstandet IT-Sicherheitsmängel direkt bei den zuständigen Benutzenden, Systemadministrierenden oder IT-Verantwortlichen. Führt diese Beanstandung nicht zu einer Behebung des IT-Sicherheitsmangels, informiert die IT-Sicherheitsstelle die Leitung der jeweiligen Organisationseinheit.

[4]Die IT-Sicherheitsstelle kann die Isolation von Informatikmitteln, welche am Netzwerk der UZH angeschlossen sind, anordnen oder selbst durchführen.

[5]Die IT-Sicherheitsstelle stellt operative Anforderungen bezüglich der IT-Sicherheit (IT- Grundschutz) und kann deren Umsetzung jederzeit überprüfen.

[6]Die IT-Sicherheitsstelle berät die Organisationseinheiten in Fragen der IT-Sicherheit und gibt Empfehlungen ab.

[7]Die IT-Sicherheitsstelle unterstützt bei Bedarf die Organisationseinheiten bei IT-Sicherheitsvorfällen. Sie ist dafür verantwortlich, externe IT-Sicherheitsspezialisten aufzubieten und ihren Einsatz zu koordinieren.

[8]Die IT-Sicherheitsstelle vertritt die Interessen der UZH gegenüber den Internet-Betreibern. Die Organisationseinheiten und Benutzenden/Systemadministrierenden sind dazu verpflichtet, die IT-Sicherheitsstelle bei der Bearbeitung von Beanstandungen durch die Internet Community zu unterstützen.

§ 8. IT-Notfallmanagement

[1]Benutzende sind verpflichtet, alle wesentlichen beobachteten oder vermuteten IT-Notfälle und Informationssicherheitsvorfälle dem IT Service Desk unverzüglich zu melden.

[2]Der IT Service Desk überprüft die Meldung und bestimmt, ob es sich um eine IT-Störung oder um einen IT-Notfall handelt. Bei einem IT-Notfall informiert der IT Service Desk umgehend das IT-Notfallmanagement der Zentralen Informatik. Die Rollen und Verantwortlichkeiten des IT-Notfallmanagements sind im IT-Notfallhandbuch der Zentralen Informatik definiert[3].

[3]Die IT-Verantwortlichen sind für die Behebung von lokalen IT-Störungen verantwortlich. Sie stellen bei einem IT-Notfall den Kontakt und die Zusammenarbeit mit dem IT-Notfallmanagement der Zentralen Informatik sicher.

[4]Die IT-Notfallmanager:in behandelt den IT-Notfall gemäss dem im IT-Notfallhandbuch dokumentierten Prozess.

[5]Die IT-Notfallmanager:in hat die Kompetenz, Massnahmen zu erlassen, welche für die Notfallbewältigung und die Wiederherstellung des Normalbetriebs notwendig sind.

[3] https://t.uzh.ch/1nQ

C. Nutzung von Informatikmitteln der UZH

§ 9. Erlaubte Nutzungszwecke

[1]Die Informatikmittel der UZH sind im Wesentlichen zur Erfüllung universitärer Aufgaben einzusetzen. IT-Dienste, welche Ressourcen (Netzwerke, Bandbreite, Strom, Kühlung etc.) der UZH stark beanspruchen, sind in Zusammenarbeit mit den zuständigen Stellen der zentralen Dienste zu planen. In jedem Fall ist auch die Zentrale Informatik zu informieren.

[2]Die Informatikmittel der UZH sind von den Benutzenden dazu zu verwenden, ihre jeweiligen Aufgaben innerhalb der UZH zu erfüllen.

[3]Die Benutzung der Informatikmittel der UZH für private nicht-kommerzielle Zwecke ist erlaubt, sofern sie nur in geringem Umfang stattfindet und:

a. weder dieses Reglement noch die schweizerische Rechtsordnung, noch Rechte von Drittpersonen verletzt (z.B. Persönlichkeitsrechte, Urheberrechte);
b. keinen Massenversand von E-Mails beinhaltet;
c. die Erfüllung der Arbeitspflichten nicht beeinträchtigt oder verletzt;
d. keine technischen Störungen verursacht;
e. die Nutzungs- und Lizenzbedingungen der genutzten Dienste und Programme nicht verletzt;
f. allgemein benutzte Informatikmittel der UZH nicht unverhältnismässig beansprucht (Netzwerke, Bandbreite, Internet-Zugang etc.).

[4]Um die Aufgabenerfüllung des einzelnen Informatikmittels der UZH sicherzustellen, kann die Leitung einer Organisationseinheit zusätzliche Nutzungsvorschriften erlassen und insbesondere die Nutzung für private nicht-kommerzielle Zwecke weiter einschränken oder ganz untersagen.

[5]Die Benutzung von Informatikmitteln der UZH für private kommerzielle Zwecke ist untersagt. Die Universitätsleitung kann eine kommerzielle Nutzung zur Erfüllung nicht-universitärer Aufgaben ausnahmsweise zulassen. Für assoziierte Institute gelten die Bestimmungen der Assoziierungsvereinbarung.

§ 10. Rechtmässige Nutzung

[1]Untersagt sind der Konsum und die Nutzung, Verarbeitung, Speicherung, Übermittlung oder Weiterverbreitung von rechtswidrigen, pornographischen, rassistischen, sexistischen oder Gewalt verherrlichenden Inhalten, insbesondere von entsprechenden Internetangeboten, E-Mails, Mitteilungen in Nachrichtendiensten, Bild- oder Tonaufnahmen oder sonstigen Abbildungen.

[2]Die Abteilung Recht und Datenschutz kann in begründeten Einzelfällen Ausnahmen bewilligen, insbesondere für Forschung und Lehre, zur Erfüllung anderer Aufgaben der Universität oder in Zusammenhang mit künstlerischen Darstellungen. Der/die Gesuchsteller:in hat das Bewilligungsgesuch schriftlich, mit Begründung und mit einem Visum der Institutsleitung bei der Zentralen Informatik einzureichen. Die Zentrale Informatik prüft das Gesuch und leitet es mit einer Empfehlung an die Abteilung Recht und Datenschutz weiter. Diese prüft das Gesuch aus juristischer Sicht und entscheidet über die Bewilligung. Die Bewilligung kann mit Auflagen verbunden werden.

[3]Beim Herunterladen, Nutzen, Vervielfältigen oder Zurverfügungstellen von Software und anderen urheberrechtlich geschützten Werken ist den urheberrechtlichen Vorgaben, den jeweiligen Lizenzbestimmungen und allfälligen beschaffungsrechtlichen Vorgaben vollumfänglich Rechnung zu tragen.

§ 11. Bearbeitung von Personendaten und anderen Informationen

[1]Die Bearbeitung von Personendaten ist nur nach Massgabe der anwendbaren Datenschutzbestimmungen[4] erlaubt.

[2]Mit Informatikmitteln der UZH erstellte, empfangene oder versandte Informationen (einschliesslich E-Mails) gelten als dienstliche Informationen, sofern deren private Natur aus deren Bezeichnung oder Ablage nicht eindeutig erkennbar ist.

[3]Dienstliche Informationen, die weder öffentlich bekannt noch allgemein zugänglich sind, unterstehen grundsätzlich dem Amtsgeheimnis und gegebenenfalls zusätzlich einem Berufsgeheimnis (z.B. für Ärzte, Zahnärzte oder Psychologen) oder einem Fabrikations- und Geschäftsgeheimnis.

[4]Dienstliche E-Mails dürfen nicht auf ein privates E-Mail-Konto um- oder weitergeleitet werden.

[5]Das Speichern von vertraulichen oder geheimen Informationen auf Informatikmitteln der UZH oder auf BYOD-Geräten, die geschäftlich genutzt werden, ist nur in den von der UZH dafür vorgesehenen Anwendungen erlaubt (z.B. Outlook Mailclient, Microsoft O365, UZH-Laufwerke). Vorgängig sind die technischen Richtlinien der Zentralen Informatik auf den Geräten durch die Benutzenden zu akzeptieren. Das Synchronisieren ist nur mit einer von der UZH unterstützten Verwaltungsmethode erlaubt[5].

D. Vorgaben zur Gewährleistung der IT-Sicherheit

§ 12. Vorgaben zum Grundschutz der Informatikmittel der UZH

[1]Die Informatikmittel der UZH sind vor Missbrauch sowie unautorisiertem Zugriff bestmöglich zu schützen. Insbesondere ist dafür Sorge zu tragen, dass ein Angriff auf weitere Geräte im Netzwerk der UZH und die Ausbreitung von schädlichen Programmcodes verhindert wird.

[2]Die Benutzenden überprüfen sämtliche verschlüsselten E-Mails und Attachments, die von ihnen entschlüsselt werden, vor Gebrauch auf Malware. Sie stellen auch sicher, dass von ihnen versandte, verschlüsselte E-Mails und Attachments vorgängig überprüft wurden.

[3]Bei Störungen eines Informatikmittels der UZH oder BYOD-Geräts, welche weitere Informatikmittel der UZH negativ beeinflussen und zu weiteren Schäden führen können, sind die Benutzenden verpflichtet, das Informatikmittel oder BYOD-Gerät sofort ausser Betrieb zu nehmen oder zu isolieren und unverzüglich die IT-Verantwortlichen beizuziehen. Diese ziehen bei Bedarf die Systemadministrierenden und weitere Fachpersonen bei.

[4]Bei Verdacht auf Schwachstellen und mögliche IT-Sicherheitsvorfälle (z.B. Virenbefall) ist der IT Service Desk zwingend zu informieren. Alle wesentlichen beobachteten oder vermuteten IT-Notfälle und Informationssicherheitsvorfälle sind unverzüglich dem IT Service Desk zu melden.

[5]Sicherheitseinstellungen von Informatikmitteln der UZH (Virenschutz, Browser-Konfiguration, System-Konfiguration, IT-Grundschutz etc.) dürfen durch die Benutzenden nicht verändert werden. Derartige Konfigurationsänderungen erfolgen ausschliesslich durch die zuständigen IT-Verantwortlichen oder die Zentrale Informatik. Diese Bestimmung gilt auch für Benutzende mit lokalen Administrationsrechten. Auf BYOD-Geräten sind die Sicherheitseinstellungen gemäss Vorgaben in diesem Reglement durch die Benutzenden vorzunehmen.

§ 13. Anschluss von Informatikmitteln und Installation von Software

[1]An Informatikmittel der UZH dürfen ausschliesslich Informatikmittel und BYOD-Geräte für den erlaubten Anwendungszweck angeschlossen und betrieben werden. Die Organisationseinheiten können für Informatikmittel in ihrem Zuständigkeitsbereich die Details regeln.

---

[4] Hierbei sind insbesondere die folgenden Bestimmungen zu beachten: *«Gesetz über die Information und den Datenschutz» (IDG, LS 170.4), «Verordnung über die Information und den Datenschutz» (IDV, LS 170.41)* sowie *«Verordnung über die Informationsverwaltung und -sicherheit» (IVSV, LS 170.8) sowie die «Weisung zur Klassifizierung von Informationen» der UZH.*

[5] Detaillierte Informationen unter: https://t.uzh.ch/1iu

[2]Für die Informatikmittel der UZH sind die Sicherheitsanforderungen bezüglich:

a. Vertraulichkeit;
b. Unversehrtheit (Integrität) und
c. Verfügbarkeit

durch die IT-Verantwortlichen festzulegen und mit geeigneten IT-Sicherheitsmassnahmen und unter der Berücksichtigung der «*Weisung für den Betrieb von Systemen»* sicherzustellen.

[3]Die Bestimmungen dieses Reglements und der «*Weisung für den Betrieb von Systemen»* sind einzuhalten. Für IT-Systeme, welche die erwähnten Bestimmungen nicht vollumfänglich erfüllen können, müssen von den Verantwortlichen vertretbare alternative Sicherheitskonzepte resp. kompensierende Massnahmen zur Risikominimierung schriftlich festgehalten und umgesetzt werden. Diese Dokumentationspflicht kann bei gemeinsam gepflegten Informatikmitteln der UZH durch summarische bzw. tabellarische Aufstellungen erfüllt werden.

[4]Die Installation von privat lizenzierter Software auf Informatikmitteln der UZH ist grundsätzlich untersagt. Ausnahmen bedürfen der Bewilligung durch die Zentrale Informatik oder die IT-Verantwortlichen.

§ 14. Physischer Schutz der Informatikmittel

[1]Informatikmittel der UZH sind stets vor Diebstahl oder Manipulation zu schützen. Sie müssen sicher aufbewahrt werden. Insbesondere in frei zugänglichen Räumlichkeiten sind Informatikmittel vor Fremdzugriffen und Diebstahl angemessen zu schützen.

[2]Verlorene oder gestohlene Informatikmittel der UZH sowie BYOD-Geräte mit betrieblichen Daten der UZH sind unverzüglich dem zuständigen IT-Verantwortlichen und der vorgesetzten Stelle zu melden. Diese entscheiden über weitere Massnahmen.

[3]Ausleihe, Vermietung und Verkauf der Informatikmittel der UZH müssen von der Leitung der Organisationseinheit bewilligt werden.

[4]Sollen Datenträger entsorgt werden, muss vorher sichergestellt werden, dass die abgespeicherten Restinformationen nicht in falsche Hände gelangen können. Hierzu muss der Datenträger sicher gelöscht oder physikalisch vernichtet werden. Dabei ist das Merkblatt *«Vernichten elektronischer Daten»* der Datenschutzbeauftragten des Kantons Zürichs zu berücksichtigen.

§ 15. Schutz des Netzwerks der UZH

[1]Alle an das Netzwerk der UZH angeschlossenen Informatikmittel der UZH und BYOD-Geräte müssen (soweit für das jeweilige Gerät verfügbar bzw. konfigurierbar) über die folgenden, minimalen Sicherheitsstandards verfügen:

a. Aktueller Virenscanner;
b. Aktuelle Softwareversionen (Anwendungen und Betriebssystem), insbesondere in Bezug auf Sicherheitspatches und Signaturen für Virenscanner;
c. Bei Informatikmitteln der UZH und BYOD-Geräten, die von Mitarbeitenden genutzt werden, ein automatisches Logout sowie ein separates Benutzerprofil ohne Administrationsrechte, welches zur Erledigung der täglichen Arbeit verwendet wird;
d. Zugang geschützt durch ein starkes Passwort gemäss *«Weisung für den Betrieb von Systemen»*.

[2]BYOD-Geräte dürfen gemäss den Vorgaben der Zentralen Informatik oder der IT-Verantwortlichen nur an speziell dafür vorgesehenen Netzwerken der UZH angeschlossen werden. Dabei ist der Zugriff der BYOD-Geräte so zu steuern, dass die Regelungen des vorliegenden Reglements eingehalten werden.

[3]Im Netzwerk der UZH dürfen nur durch die Zentrale Informatik autorisierte WLAN-Installationen und DSL-Anschlüsse eingesetzt werden. Ausnahmen sind nur mit schriftlicher Erlaubnis der Zentralen Informatik zulässig.

[4]Das Verbinden des Netzwerks der UZH mit Fremdnetzen ist nur in Ausnahmefällen mit schriftlicher Erlaubnis der Zentralen Informatik zulässig. Einzelheiten werden in der *«Weisung über die Netzwerksicherheit (WNS)»* geregelt.

[5]Organisationseinheiten, welche eigene Netzwerke oder Netzwerkesegmente betreiben, benötigen eine schriftliche Ausnahmebewilligung der Zentralen Informatik. Sie sind verpflichtet, die Vorgaben gemäss *«Weisung über die Netzwerksicherheit (WNS)»* einzuhalten.

§ 16. Protokollierung und Überwachung

[1]Das Netzwerk der UZH und einzelne IT-Dienste werden durch die Zentrale Informatik überwacht. Die Nutzung des Netzwerks sowie der mit dem Netzwerk der UZH verbundenen Informatikmittel werden protokolliert. Die Protokollierung dient dem Schutz der IT-Systeme und der Erkennung des Missbrauchs von Informatikmitteln der UZH durch Benutzende sowie der Betriebssicherung und der Ressourcenplanung.

[2]Im Rahmen der Protokollierung werden auch Internet-Zugriffe und der E-Mail-Verkehr protokolliert. Es besteht keine Möglichkeit, E-Mails bezüglich Protokollierung speziell behandeln zu lassen; die E-Mails können jedoch verschlüsselt werden.

[3]Weitere Bestimmungen zur Protokollierung sind in der von der Zentralen Informatik erlassenen Weisung «*Logfile-Policy*» enthalten.

[4]Eine personenbezogene Auswertung der Protokolle kann erfolgen:

a. im Fall eines Missbrauchsverdachts. Die Voraussetzungen und Zuständigkeiten richten sich in diesem Fall nach § 26.

b. durch die Zentrale Informatik zur Gewährleistung der Sicherheit und Funktionsfähigkeit der Informatikmittel der UZH, wobei die Benutzenden vorgängig über die personenbezogene Auswertung zu informieren sind. Eine Auswertung ohne vorgängige Information ist zulässig, soweit dies zur IT-Störungsbehebung unumgänglich ist.

[5]Zum Zweck der Kontrolle der Einhaltung des vorliegenden Reglements sind die Organisationseinheiten berechtigt, anonymisierte Berichte über die Nutzung der Informatikmittel der UZH zu erstellen. Die Berichte dürfen keine Rückschlüsse auf einzelne Benutzende zulassen. Ergibt sich aufgrund eines anonymisierten Berichts ein Verdacht auf Missbrauch von Informatikmitteln der UZH, ist nach § 26 vorzugehen.

[6]Die Zentrale Informatik und die IT-Verantwortlichen der Organisationseinheiten sorgen dafür, dass sich von einer IP-Adresse ihres Netzwerkbereichs auf die Person zurückschliessen lässt, von welcher das entsprechende Gerät verwendet wurde oder (z. B. im Falle von Schulungsräumen) zumindest das benützte Gerät eruiert werden kann. Sie stellen sicher, dass solche Rückschlüsse über den in der *«Logfile-Policy»* geforderten Zeitraum erfolgen können. Dies gilt auch bei temporär und automatisch zugeteilten IP-Adressen.

[7]Die Protokollierungen und anonymisierten Berichte werden nach spätestens 12 Monaten gelöscht, sofern sie nicht für die Ahndung eines Missbrauchs oder aufgrund gesetzlicher Anforderungen länger aufbewahrt werden müssen.

§ 17. IT-Störungsbehebung

[1]Zur Behebung einer IT-Störung kann die Zentrale Informatik alle zur Aufrechterhaltung bzw. Wiederherstellung des rechtmässigen Zustandes erforderlichen Massnahmen treffen, wie:

a. Ermittlung der Störungsursache in Zusammenarbeit mit dem IT-Verantwortlichen oder der Leitung der Organisationseinheiten;

b. Aufforderung der verantwortlichen Benutzenden zur Behebung des störenden Zustands;

c. Setzung von Fristen zur Wiederherstellung des rechtmässigen Zustands;

d. Sperrung eines Kontos bis zur sicheren Rückgabe an den rechtmässigen Benutzenden;

e. Sperrung eines Kontos zur Einholung einer schriftlichen Zusicherung der Einhaltung dieses Reglements;

f. Sperrung von Diensten oder Services zum Schutz der IT-Infrastruktur oder von Angehörigen der UZH.

[2]Wird bei einer IT-Störungsbehebung festgestellt, dass ein Verdacht auf Missbrauch von Informatikmitteln der UZH besteht, ist gemäss den Bestimmungen in §26 vorzugehen.

§ 18. Vorgaben zum Betrieb von dezentralen IT-Systemen

[1]Benutzende, die nicht UZH-Angehörige sind, dürfen keine Informatikmittel mit erhöhten Sicherheitsanforderungen, insbesondere keine Server und keine Peer-to-Peer-Kommunikation, einrichten oder einrichten lassen und betreiben. Die Zentrale Informatik kann Ausnahmeregelungen für einzelne Peer-to-Peer-Kommunikation und Vorschriften für deren Betrieb erlassen.

[2]Bei Mailservern ist ein expliziter Schutz vor Malware, unerwünschter Software und Spam einzusetzen. Dabei müssen alle ein- und ausgehenden E-Mails inklusive deren Anhänge, unabhängig vom Absender, überprüft werden, da Malware in verschlüsselten E-Mails oder Dateien durch ein Virenschutzprogramm nicht erkannt werden kann.

[3]Die *«Weisung über die Netzwerksicherheit (WNS)»* und die *«Verordnung über die Informationsverwaltung und -sicherheit des Kantons Zürich (IVSV)»* sind einzuhalten.

E. Benutzerberechtigungen und Passwörter

§ 19. Zugangsberechtigungen

[1]Der Zugang zu Informationen und Anwendungen auf Informatikmitteln der UZH ist vor Unberechtigten zu schützen. Es gelten insbesondere folgende Regelungen:

a. Zugriffe auf Informatikmittel der UZH haben sich ausnahmslos nach den Interessen der UZH zu richten und dürfen nur auf den zugelassenen Zugriffswegen auf autorisierte Inhalte erfolgen;

b. Es werden den Benutzenden nur die notwendigen Zugriffsrechte eingeräumt, damit diese die ihnen zugeteilten Aufgaben erledigen können (Least-Privilege-Prinzip);

c. Der Zugriff durch die Benutzenden ist nur gestattet, wenn die Informationen unmittelbar für die Erfüllung einer konkreten Aufgabe der Benutzenden benötigt werden (Need-to-know-Prinzip).

[2]Es sind nur Zugriffe im Rahmen der erhaltenen Zugriffsberechtigungen mit den zugeteilten Identifikations- und Authentisierungsmitteln erlaubt. Die Benutzenden sind für ihre Zugriffe auf Informatikmittel der UZH verantwortlich, sowie für Zugriffe durch unberechtigte Dritte, welche aufgrund von fahrlässigem Verhalten der Benutzenden erfolgen.

[3]Stellen Benutzende fest, dass sie Zugriff auf Informationen haben, die nicht zur Erfüllung ihrer Tätigkeiten erforderlich sind, oder decken sie einen Missbrauch der eigenen Authentisierungsmittel auf, so müssen sie dies umgehend der vorgesetzten Stelle und dem IT Service Desk melden.

§ 20. Umgang mit Passwörtern, anderen Authentisierungsmitteln und Schlüsseln

[1]Authentisierungsmittel wie Passwörter, PINs, Zertifikate, Hardware Tokens und Badges sowie Schlüssel dürfen nicht weitergegeben werden. Wo Passwörter verwendet werden, sind starke persönliche Passwörter oder starke Gruppenpasswörter gemäss *«Weisung für den Betrieb von Systemen»* einzusetzen. Passwörter sind verschlüsselt zu speichern.

[2]Die Benutzenden und Systemadministrierenden sind für die Wahl, Vertraulichkeit und Qualität ihrer Passwörter verantwortlich. Passwörter, die durch die Benutzenden im Umgang mit Informatikmitteln der UZH eingesetzt werden, dürfen nicht für Zugriffe auf andere IT-Systeme verwendet werden (z.B. im privaten Bereich oder für externe Systeme und Services im Internet, welche nicht in Verbindung mit Tätigkeiten an der UZH stehen). Passwörter sind unverzüglich zu wechseln, wenn der Verdacht besteht, dass sie unberechtigten Dritten bekannt geworden sein könnten.

[3]Für Gruppenpasswörter ist eine Passwort-verantwortliche Person zu bestimmen, die alle Gruppenmitglieder persönlich kennt und das Passwort jederzeit, insbesondere auf Anweisung der IT-Sicherheitsstelle, ändern kann. Sie stellt sicher, dass die per Gruppenpasswort zugreifende Person oder der zugreifende Computer im Missbrauchsfall identifiziert werden kann.

§ 21. Remote Access für Fernwartung

[1]Der Fernzugriff (Remote Access) auf Informatikmittel der UZH durch Mitarbeitende der UZH sowie Mitarbeitende von Drittfirmen im Auftragsverhältnis erfolgt mit einer starken Authentisierung (mind. Zwei-Faktor-Authentisierung), der Verschlüsselung des Übertragungsweges sowie der Steuerung der Zugriffe über die dafür vorgesehene IT-Infrastruktur der UZH. Mitarbeitende von Drittfirmen haben vorgängig eine Geheimhaltungsvereinbarung zu unterzeichnen.

F. Bewilligungspflichtige und nicht erlaubte Anwendungen

§ 22. Bewilligungspflichtige Anwendungen

[1]Web-Subdomänen im Rahmen des öffentlichen Webauftritts der UZH sind bewilligungspflichtig. Die Bewilligungen werden von der Abteilung Kommunikation erteilt.

[2]Bewilligungspflichtig sind ausserdem:

a. Verbindungen aus universitätsfremden Netzwerken wie DSL-Anschlüssen oder Tunnelverbindungen ins Netzwerk der UZH, die nicht an einem entsprechenden Dienst der Zentralen Informatik enden. Die Bewilligungen werden von der Abteilung IT-Infrastruktur der Zentralen Informatik erteilt.

b. Das Einrichten eines Gerätes mit einer statischen IP-Adresse. Die Bewilligungen werden vom IT-Verantwortlichen erteilt, der für den örtlich gültigen IP-Adressbereich zuständig ist.

c. Massenversände per E-Mail mit dem Adress-Stamm der Universität Zürich. Die Bewilligungen werden vom Rektoratsdienst erteilt. Die 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 in Angelegenheiten, die unmittelbar mit der Aufrechterhaltung des Betriebes der UZH zusammenhängen.

§ 23. Nicht erlaubte Anwendungen

[1]Der Einsatz von Hard- und Softwarekomponenten, welche Informationen der UZH oder Informatikmittel der UZH bedrohen, ist untersagt.

[2]Untersagt sind weiter:

a. das Betreiben von Mailservern, welche von ausserhalb der Universität direkt ansprechbar sind oder Mailserver ausserhalb des Netzwerks der UZH direkt kontaktieren. Vorbehalten bleibt das Weiterbetreiben der bisher betriebenen und bei der Zentralen Informatik registrierten Mailserver einzelner Organisationseinheiten;

b. das Betreiben von Kommunikationsleitungen oder Tunnelverbindungen, welche an Endpunkten sowohl innerhalb als auch ausserhalb des Netzwerks der UZH eine Vermittlungsfunktion ins Internet ausführen;

c. das Weiterbetreiben von Netzwerkdiensten, von welchen bekannt ist, dass damit in schwerwiegender Weise Missbrauch betrieben werden kann, und das ungeschützte Weiterbetreiben von Geräten, bei denen unberechtigte Dritte Administratorenrechte erlangt haben oder sie anderweitig in störender oder gefährdender Weise missbrauchen konnten;

d. die Publikation von Webseiten, die den Webbrowser der Aufrufenden ohne deren bewusste Entscheidung dazu bringen, Seiten oder Dienste von ausserhalb der UZH nachzuladen, insbesondere das Einbetten von Bildern, Scripts, iFrames oder Applets mit oder ohne 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 Vertrages, welcher die Datenschutzbestimmungen bei Auslagerung von IT-Dienstleistungen beinhaltet;

G. Massnahmen bei Missbrauch und Missbrauchsverdacht

§ 24. Missbräuchliche Nutzung von Informatikmitteln der UZH

[1]Missbräuchlich ist jede Verwendung von Informatikmitteln der UZH, die gegen dieses Reglement oder gegen die von der Zentralen Informatik erlassenen Ausführungsbestimmungen verstösst, darunter insbesondere Verstösse gegen die Bestimmungen über:

a. die erlaubten Nutzungszwecke und die rechtmässige Nutzung (§§ 9 und 10);

b. den Schutz des Netzwerks der UZH und den Betrieb von dezentralen IT-Systemen (§§ 15 und 18);

c. den Umgang mit Passwörtern, anderen Authentisierungsmitteln und Schlüsseln (§ 20);

d. die bewilligungspflichtigen Anwendungen und die nicht erlaubten Anwendungen (§ 22 und 23).

[2]Missbräuchlich sind weiter:

a. das unbefugte Beschaffen von Daten im Sinn von Art. 143 des Schweizerischen Strafgesetzbuches (StGB; SR 311.0), das unbefugte Eindringen in ein Datenverarbeitungssystem im Sinn von Art. 143bis Abs. 1 StGB und das Beschädigen von Daten im Sinn von Art. 144bis Ziff. 1 StGB;

b. das unautorisierte Absuchen von internen und externen Netzwerken auf Schwachstellen (z.B. Port-Scanning);

c. das Vorkehren und Durchführen von Massnahmen zur Störung von Netzwerken, Servern und anderen Geräten (z.B. Denial-of-Service-Angriffe);

d. das Ausspionieren von Passwörtern und anderen Authentisierungsmitteln;

e. das Versenden von E-Mails oder anderen elektronischen Mitteilungen mit vorgetäuschten oder irreführenden Angaben zum Absender oder zur technischen Adresse des Absenders;

f. das Belästigen oder Irreführen von Personen durch das Senden von E-Mails oder anderen elektronischen Mitteilungen oder durch Telefonanrufe.

§ 25. Folgen von Missbrauch

[1]Bei Missbräuchen durch Angehörige der UZH werden allfällige Massnahmen nach Massgabe der auf das Arbeitsverhältnis anwendbaren Bestimmungen bzw. der Disziplinarverordnung der Universität Zürich (LS 415.33) ergriffen.

[2]Bei Missbräuchen durch Dritte richten sich allfällige Massnahmen nach dem auf das jeweilige Rechtsverhältnis anwendbaren Recht und nach den vertraglichen Vereinbarungen. Die UZH kann die Arbeitgeberin des Dritten (z.B. assoziiertes Institut) über den erfolgten Missbrauch informieren.

[3]Vorbehalten bleiben die Geltendmachung von Schadenersatzansprüchen und die Einleitung eines Strafverfahrens durch die UZH.

§ 26. Vorgehen bei Missbrauchsverdacht

[1]Wird ein Missbrauchsverdacht im Rahmen der Überwachung der Informatikmittel der UZH, bei einer Störungsbehebung oder aufgrund einer Meldung eines Benutzenden festgestellt, wird er der Abteilung Recht und Datenschutz gemeldet.

[2]Die Abteilung Recht und Datenschutz klärt den Missbrauchsverdacht näher ab und leitet die weiteren Schritte ein. Sie ist für den Einbezug anderer zuständiger Stellen verantwortlich.

[3]Bei begründetem Verdacht auf Missbrauch gemäss diesem Reglement kann die IT-Sicherheitsstelle:

a. Anschlüsse oder Dienste vorsorglich sperren oder sperren lassen und missbräuchlich verwendete Daten blockieren. Sie ist verantwortlich dafür, dass die relevanten Systemprotokolle und Daten zu Beweiszwecken sichergestellt und aufbewahrt werden;
b. auf Anordnung der Abteilung Recht und Datenschutz eine rückwirkende personenbezogene Auswertung von Protokollen nach § 16 vornehmen;
c. auf Anordnung der Abteilung Recht und Datenschutz eine zeitlich befristete personenbezogene Protokollierung durchführen. Diese Massnahme wird den betroffenen Benutzenden vorgängig angekündigt, unter vorgängigem Einbezug des direkten Vorgesetzten sowie der Abteilung Personal oder der Abteilung Professuren. Eine personenbezogene Protokollierung ist auf höchstens drei Monate zu befristen.

[4]Die von der IT-Sicherheitsstelle erstellten personenbezogenen Auswertungen und personenbezogenen Protokolle sind streng vertraulich und werden ausschliesslich der Abteilung Recht und Datenschutz bekannt gegeben. Die Abteilung Recht und Datenschutz entscheidet über die weitere Verwendung von beweisrelevanten Informationen.

[5]Bestätigt sich der Missbrauchsverdacht nicht, wird von Massnahmen nach § 25 abgesehen oder sind sämtliche entsprechenden Verfahren rechtskräftig abgeschlossen, werden die personenbezogenen Auswertungen und personenbezogenen Protokolle vernichtet.

H. Schlussbestimmung

§ 27. Aufhebung bisherigen Rechts

Das Reglement über den Einsatz von Informatikmitteln an der Universität Zürich vom 30. November 2017 wird aufgehoben.

§ 28. Inkrafttreten

Das vorliegende Reglement tritt am 1.1.2023 in Kraft.

Zürich, 29.11.2022

Im Namen der Universitätsleitung

Der Rektor:	Die Generalsekretärin:
Michael Schaepman	Rita Stöckli