Universität Zürich[UZH]

Geheimhaltungserklärung vom Mai 2016

Für wen gilt diese Geheimhaltungserklärung?

Die vorliegende Geheimhaltungserklärung ist durch alle Personen zu unterzeichnen, welche in Ausübung ihrer Tätigkeit, ihres Studiums oder ihres Auftrags Zugriff auf solche Informationen der UZH haben, die einer Geheimhaltungspflicht oder einem besonderen Schutz unterliegen.

Solche Personen sind z.B.:

- von der UZH beauftragte externe Personen / Mitarbeitende von beauftragten Unternehmen / Mitarbeitende von beauftragten öffentlichen Organen; oder
- an der UZH tätige studentische Hilfskräfte, Praktikantinnen und Praktikanten sowie Assistentinnen und Assistenten ohne Anstellungsverhältnis; oder
- Teilnehmende von Lehrveranstaltungen oder Forschungsvorhaben der Humanmedizin / Zahnmedizin / Psychologie, soweit nicht ausgeschlossen werden kann, dass die oder der jeweilige Teilnehmende im Rahmen der Lehrveranstaltung Kenntnis von Patientendaten erlangt.

Die Geheimhaltungserklärung ist nicht durch solche Personen zu unterzeichnen, deren Tätigkeit auf einer Anstellung der UZH beruht.

Verpflichtete Person

Nachname	
Vorname	
Geburtsdatum	
Soweit zutreffend Name und Anschrift des beauftragten Unternehmens bzw. des beauftragten öffentlichen Organs	

Welche Tatsachen sind geheim zu halten / Was ist geschützt?

1. Die UZH ist eine **öffentlich-rechtliche Anstalt des Kantons Zürich** mit eigener Rechtspersönlichkeit. Als solche muss sie sicherstellen, dass alle Personen (z.B. Mitarbeitende, Studierende und Auftragnehmer), welche in Ausübung ihrer Tätigkeit, ihres Studiums oder ihres Auftrags Zugriff auf Informationen der UZH haben, die Geheimhaltungspflichten oder einem besonderen Schutz unterliegen, dem Kontroll- und Weisungsrecht der UZH unterstellt und darauf hingewiesen werden, dass sie das Amtsgeheimnis, soweit erforderlich das Berufsgeheimnis, das Fabrikations- oder Geschäftsgeheimnis sowie datenschutzrechtliche Pflichten bei der Bearbeitung von Personendaten zu wahren haben.

2. Das **Amtsgeheimnis** ist eine gesetzliche Geheimhaltungspflicht, welche für alle Mitglieder einer Behörde und damit auch für alle Mitarbeitenden der UZH gilt. Es untersagt die Bekanntgabe von Tatsachen, die weder öffentlich bekannt noch allgemein zugänglich sind, sondern einem Mitarbeitenden der UZH bei der Erfüllung seiner amtlichen oder dienstlichen Tätigkeit anvertraut worden sind oder von denen der Mitarbeitende bei dieser Gelegenheit Kenntnis erlangt hat. Das Amtsgeheimnis gilt auch für solche Auftragnehmer, die eine Bearbeitung von Informationen im Auftrag der UZH durchführen. Dies liegt darin begründet, dass die Auftragnehmer mit der Annahme des Auftrags zu Hilfspersonen der UZH werden und in dieser Funktion dieselbe Geheimhaltungspflicht wie die Mitarbeitenden der UZH zu wahren haben. Das Amtsgeheimnis ist nicht nur gegenüber Privatpersonen und der Presse zu wahren, sondern auch im Verhältnis zu anderen Behörden, welche die Informationen nicht zur Erfüllung ihrer gesetzlichen Aufgaben benötigen und die auch keine Aufsicht über die UZH ausüben. Das Amtsgeheimnis besteht auch nach Beendigung der amtlichen oder dienstlichen Tätigkeit weiter.

3. Das **Berufsgeheimnis** ist eine gesetzliche Geheimhaltungspflicht, welche für bestimmte Berufsgruppen, die auch an der UZH vorhanden sind, und deren Hilfspersonen gilt. Zu diesen Berufsgruppen zählen z.B. Ärzte, Zahnärzte und Psychologen. Hilfspersonen sind alle Personen, die Angehörige der vorbenannten Berufsgruppen bei deren Berufstätigkeit unterstützen (z.B. Pflegefachpersonen, Assistentinnen und Assistenten, Sekretariatsangestellte). Das Berufsgeheimnis untersagt die Bekanntgabe von Tatsachen, welche den Angehörigen der Berufsgruppen infolge ihres Berufes anvertraut worden sind oder welche sie oder ihre Hilfspersonen bei dessen Ausübung wahrgenommen haben. Bereits die Tatsache, dass zwischen einer Person und einem Angehörigen der Berufsgruppe ein Behandlungsverhältnis besteht, unterliegt der Geheimhaltung. Die gleiche Geheimhaltungspflicht gilt für Personen, welche im Rahmen der Forschung am Menschen nach dem Humanforschungsgesetz (d.h. Forschung zu Krankheiten des Menschen sowie zu Aufbau und Funktion des menschlichen Körpers, z.B. Anatomie, Physiologie und Genetik) ein Berufsgeheimnis erfahren haben. Auch für Studierende gilt das Berufsgeheimnis, soweit sie als Hilfspersonen der vorbenannten Berufsgruppen oder forschend nach dem Humanforschungsgesetz tätig sind und aus diesem Anlass eine Tatsache erfahren haben, welche den Angehörigen der Berufsgruppen infolge ihres Berufes anvertraut worden ist oder welche die Studierenden in Ausübung ihrer Hilfstätigkeit oder bei ihrer Forschungstätigkeit wahrgenommen haben. Diese Geheimhaltungspflicht ist auch gegenüber Kommilitoninnen und Kommilitonen zu wahren, soweit diese durch gemeinsam besuchte Veranstaltungen nicht auch Kenntnis von diesen Tatsachen erhalten haben. Das Berufsgeheimnis besteht auch nach Beendigung der Berufsausübung oder des Studiums weiter.

4. Das **Fabrikationsgeheimnis** und das **Geschäftsgeheimnis** sind gesetzliche Geheimhaltungspflichten, welche für diejenigen Personen gelten, welche gesetzlich oder vertraglich zur Geheimhaltung verpflichtet sind, bspw. durch den Arbeitsvertrag oder durch einen Auftrag. Sie untersagen die Bekanntgabe von Tatsachen, die in einem unternehmerischen Zusammenhang stehen, nur einem begrenzten Personenkreis bekannt oder zugänglich sind und an deren Geheimhaltung der Geheimnisherr ein schützenswertes Interesse hat. Die UZH ist durch diese Geheimhaltungspflichten dann geschützt, wenn sie privatwirtschaftlich tätig wird, z.B. bei Weiterbildungsprogrammen, Auftragsforschung für Unternehmen der Wirtschaft, Beratungstätigkeiten, Erstellen von Gutachten. Fabrikationsgeheimnisse betreffen den Produktionsvorgang; hierzu zählen z.B. Herstellungs- und Konstruktionsverfahren, Know-how und Forschungsergebnisse. Geschäftsgeheimnisse betreffen die nichttechnische, kaufmännische Ebene; hierzu zählen z.B. Einkaufs- und Bezugsquellen und Vertragspartner. Das Fabrikations- und Geschäftsgeheimnis bestehen auch nach Beendigung des Vertragsverhältnisses weiter.

5. Zusätzlich zu den vorbenannten Geheimhaltungspflichten müssen öffentliche Organe des Kantons Zürich wie die UZH bestimmte **Verpflichtungen des Gesetzes über die Information und den Datenschutz des Kantons Zürich** (IDG) beachten, damit bei der Bearbeitung von Personendaten nicht die Persönlichkeitsrechte der betroffenen Personen (z.B. Mitarbeitende, Studierende, Versuchspersonen oder Auftragnehmer) verletzt werden. Personendaten sind Informationen, welche sich auf eine bestimmte oder (über Zusatzinformationen) bestimmbare natürliche oder juristische Person beziehen, wie z.B. Name, Adresse, Foto, Personal-, Matrikel-, Patienten-, Telefonnummer oder E-Mail-Adresse. Der Begriff des Bearbeitens umfasst jeden Umgang mit Informationen, wie das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Einsicht gewähren, Weitergeben, Veröffentlichen oder Vernichten. Die UZH darf Personendaten nur bearbeiten, soweit dies zur Erfüllung ihrer in § 2 Universitätsgesetz des Kantons Zürich (UniG) gesetzlich umschriebenen Aufgaben geeignet und erforderlich ist. Personendaten müssen durch angemessene organisatorische und technische Massnahmen vor zufälligen, unberechtigten oder unrechtmässigen Zugriffen, Veränderungen oder Offenlegungen und vor Verlusten sowie Zerstörung geschützt werden. Daraus folgt auch, dass ein Zugriff auf Personendaten ausschliesslich denjenigen Personen erteilt werden darf, die aufgrund ihrer Funktion und Aufgabe auf die Personendaten zugreifen müssen. Weitergehende Restriktionen, wie z.B. besondere Informationspflichten oder der Vorbehalt einer Einwilligung der betroffenen Person, gelten je nach Sachverhaltskonstellation für die Bearbeitung von besonderen Personendaten. Besondere Personendaten sind Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht. Hierzu gehören Informationen über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten und Tätigkeiten, die Gesundheit, die Intimsphäre, die Rassenzugehörigkeit oder die ethnische Herkunft, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen oder Sanktionen. Zu den besonderen Personendaten gehören auch Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit natürlicher Personen (Persönlichkeitsprofil) erlauben.

Die unterzeichnende Person verpflichtet sich hinsichtlich aller Informationen und Personendaten, die ihr im Rahmen ihrer Tätigkeit bei der UZH zugänglich werden wie folgt:

- Alle Informationen und Personendaten sowie die eingesetzten Informatikmittel wie Programme, Datenbanken, Netzwerke, Passwörter, Zugriffsregelungen, Sicherheitsmassnahmen etc. werden **ausschliesslich zu den für die Tätigkeit / die Studien / den Auftrag vorgesehenen Zwecken und entsprechend den Weisungen der zuständigen Stelle der UZH bearbeitet**.
- Alle Informationen und Personendaten werden unabhängig davon, auf welchem Datenträger sie sich befinden (z.B. auf Papier, CD, Speicherchip), weder im Original noch als Kopie, weder ganz oder auszugsweise, **in keiner Art und Form, ohne ausdrückliche Zustimmung der zuständigen Stelle der UZH aus den Räumlichkeiten der UZH entfernt oder Dritten zugänglich gemacht**.
- An den Informationen und Personendaten werden **keinerlei Rechte**, insbesondere Eigentums-, Lizenz-, Nachbau-, Nutzungs- oder sonstige Schutzrechte **geltend gemacht.**
- **Bei Beendigung der Tätigkeit** werden **auf Verlangen** der zuständigen Stelle der UZH alle Dokumente, Datenträger oder weitere Unterlagen, die Informationen oder Personendaten der UZH enthalten, inklusive erstellter bzw. entstandener Sicherungskopien, **zurückgegeben oder zerstört**.
- Es werden **alle Unregelmässigkeiten** im Zusammenhang mit der Ausführung der Tätigkeit **ohne Verzug** der zuständigen Stelle der UZH **gemeldet**.

Die unterzeichnende Person verpflichtet sich die vorbenannten Geheimhaltungs-, Datenbearbeitungs- und Sorgfaltspflichten, deren Verletzung auch straf- und/oder zivilrechtliche Folgen begründen kann, einzuhalten und bestätigt, die beigefügten Auszüge aus dem Strafgesetzbuch (Art. 162, 320, 321, 321bis StGB), **aus dem Universitätsgesetz des Kantons Zürich** (§ 1, 2 UniG) **und dem Gesetz über die Information und den Datenschutz des Kantons Zürich** (§ 6, 7, 8, 9, 11, 40 IDG) **zur Kenntnis genommen zu haben.**

_____

(Ort, Datum und Unterschrift)

Auszüge von Gesetzestexten

Art. 162 Schweizerisches Strafgesetzbuch (Verletzung des Fabrikations- oder Geschäftsgeheimnisses)
Wer ein Fabrikations- oder Geschäftsgeheimnis, das er infolge einer gesetzlichen oder vertraglichen Pflicht bewahren sollte, verrät,
wer den Verrat für sich oder einen andern ausnützt,
wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Art. 320 Schweizerisches Strafgesetzbuch (Verletzung des Amtsgeheimnisses)
1. Wer ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Mitglied einer Behörde oder als Beamter anvertraut worden ist, oder das er in seiner amtlichen oder dienstlichen Stellung wahrgenommen hat, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.
Die Verletzung des Amtsgeheimnisses ist auch nach Beendigung des amtlichen oder dienstlichen Verhältnisses strafbar.
2. Der Täter ist nicht strafbar, wenn er das Geheimnis mit schriftlicher Einwilligung seiner vorgesetzten Behörde geoffenbart hat.

Art. 321 Schweizerisches Strafgesetzbuch (Verletzung des Berufsgeheimnisses)
1. Geistliche, Rechtsanwälte, Verteidiger, Notare, Patentanwälte, nach Obligationenrecht zur Verschwiegenheit verpflichtete Revisoren, Ärzte, Zahnärzte, Chiropraktoren, Apotheker, Hebammen, Psychologen sowie ihre Hilfspersonen, die ein Geheimnis offenbaren, das ihnen infolge ihres Berufes anvertraut worden ist oder das sie in dessen Ausübung wahrgenommen haben, werden, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.
Ebenso werden Studierende bestraft, die ein Geheimnis offenbaren, das sie bei ihrem Studium wahrnehmen.
Die Verletzung des Berufsgeheimnisses ist auch nach Beendigung der Berufsausübung oder der Studien strafbar.
2. Der Täter ist nicht strafbar, wenn er das Geheimnis auf Grund einer Einwilligung des Berechtigten oder einer auf Gesuch des Täters erteilten schriftlichen Bewilligung der vorgesetzten Behörde oder Aufsichtsbehörde offenbart hat.
3. Vorbehalten bleiben die eidgenössischen und kantonalen Bestimmungen über die Zeugnispflicht und über die Auskunftspflicht gegenüber einer Behörde.

Art. 321bis Schweizerisches Strafgesetzbuch
(Berufsgeheimnis in der Forschung am Menschen)
1 Wer ein Berufsgeheimnis unbefugterweise offenbart, das er durch seine Tätigkeit in der Forschung am Menschen nach dem Humanforschungsgesetz vom 30. September 2012 erfahren hat, wird nach Artikel 321 bestraft.
2 Berufsgeheimnisse dürfen für die Forschung zu Krankheiten des Menschen sowie zu Aufbau und Funktion des menschlichen Körpers offenbart werden, wenn die Voraussetzungen nach Artikel 34 des Humanforschungsgesetzes vom 30. September 2011 erfüllt sind und die zuständige Ethikkommission die Offenbarung bewilligt hat.

§ 1. Universitätsgesetz des Kantons Zürich (Rechtsform)
1 Die Universität ist eine öffentlichrechtliche Anstalt des Kantons mit eigener Rechtspersönlichkeit.
2 Die Universität plant, regelt und führt ihre Angelegenheiten im Rahmen von Verfassung und Gesetz selbstständig.

§ 2. Universitätsgesetz des Kantons Zürich (Zweck und Auftrag)
1 Die Universität leistet wissenschaftliche Arbeit in Forschung und Lehre im Interesse der Allgemeinheit. Sie erbringt in diesem Zusammenhang auch Dienstleistungen.
2 Die Universität vermittelt wissenschaftliche Bildung. Sie schafft damit die Grundlagen zur Ausübung von akademischen Tätigkeiten und Berufen.
3 Die Universität pflegt die akademische Weiterbildung und fördert den wissenschaftlichen Nachwuchs.

§ 6. Gesetz über die Information und den Datenschutz des Kantons Zürich (Bearbeiten im Auftrag)
1 Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen, sofern keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht.
2 Es bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich.

§ 7. Gesetz über die Information und den Datenschutz des Kantons Zürich (Informationssicherheit)
1 Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen.
2 Die Massnahmen richten sich nach den folgenden Schutzzielen:
a. Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen,
b. Informationen müssen richtig und vollständig sein,
c. Informationen müssen bei Bedarf vorhanden sein,
d. Informationsbearbeitungen müssen einer Person zugerechnet werden können,
e. Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.
3 Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik.

§ 8. Gesetz über die Information und den Datenschutz des Kantons Zürich (Gesetzmässigkeit)
1 Das öffentliche Organ darf Personendaten bearbeiten, soweit dies zur Erfüllung seiner gesetzlich umschriebenen Aufgaben geeignet und erforderlich ist.

§ 9. Gesetz über die Information und den Datenschutz des Kantons Zürich (Zweckbindung)
1 Das öffentliche Organ darf Personendaten nur zu dem Zweck bearbeiten, zu dem sie erhoben worden sind, soweit nicht eine rechtliche Bestimmung ausdrücklich eine weitere Verwendung vorsieht oder die betroffene Person im Einzelfall einwilligt.

§ 11. Gesetz über die Information und den Datenschutz des Kantons Zürich (Vermeidung des Personenbezugs)
1 Das öffentliche Organ gestaltet Datenbearbeitungssysteme und -programme so, dass möglichst wenig Personendaten anfallen, die zur Aufgabenerfüllung nicht notwendig sind.
2 Es löscht, anonymisiert oder pseudonymisiert solche Personendaten, sobald und soweit dies möglich ist.

§ 40. Gesetz über die Information und den Datenschutz des Kantons Zürich (Vertragswidriges Bearbeiten von Personendaten)
1 Wer als beauftragte Person gemäss § 6 ohne ausdrückliche Ermächtigung des auftraggebenden öffentlichen Organs Personendaten für sich oder andere verwendet oder anderen bekannt gibt, wird mit Busse bestraft.
2 Die Untersuchung und Beurteilung von Widerhandlungen obliegt den Statthalterämtern.

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

Normen für den Betrieb von Systemen an der Universität Zürich (NBS)

Gültigkeit dieses Dokuments

Dieses Dokument ist eine Ausführungsvorschrift zu den Richtlinien für den Einsatz von Informatikmitteln an der Universität Zürich (REIM) und gilt für dieselben Personen und Anwendungen.

Wenn mit gutem Grund einzelne dieser Normen nicht erfüllt werden, müssen gemäss REIM (§11.) vertretbare alternative Sicherheitskonzepte aufgezeigt, festgehalten und umgesetzt werden.

Normen

1. Zur **Bekämpfung des Missbrauchs durch Dritte** sind die für das System Verantwortlichen verpflichtet, dafür zu sorgen, dass folgende Bedingungen erfüllt werden:

1.1 Ein Virenschutzprogramm ist eingerichtet, und zwar so, dass es laufend automatisch mit den aktuellen Virenbeschreibungen versorgt wird, wenn möglich laufend alle ankommenden Dateien prüft und zusätzlich für vertiefte Prüfungen gestartet werden kann. Das Angebot der Informatikdienste ist zu beachten.

1.2 Das Betriebssystem muss vom Hersteller oder der Distribution unterstützt sein und gewartet werden.

1.3 Das System wird grundsätzlich bezüglich der vom Systemhersteller gelieferten Sicherheits-Updates auf den laufenden Stand gebracht. Wenn nicht im Einzelnen gute Gründe dagegen sprechen ist das automatische Verfahren des Systemherstellers zu verwenden.

1.4 Die Endbenutzer wissen, dass sie auf das Anklicken von Verweisen, auf das Ausfüllen von Formularen und auf das Öffnen von Attachments verzichten müssen, sobald der Kontext der Mail oder der Webseite verdächtig ist.

1.5 Unnötige Netzwerkdienste, welche bei Systemlieferung eingeschaltet sind, werden nach Möglichkeit und bestem Wissen ausgeschaltet.

1.6 Ein neu aufgesetztes System wird erst ans Datennetz angeschlossen, wenn es durch eine Software- oder Hardware-Firewall gut geschützt ist oder alle Servicepakete und Updates eingerichtet sind.

2. Bezüglich **Zugänglichkeit und Vertraulichkeit** sind die für das System Verantwortlichen verpflichtet, dafür zu sorgen, dass folgende Bedingungen erfüllt werden:

2.1 Ein individueller Zugangsschutz vor Ort und für alle Netzwerkverbindungen ist eingerichtet. Alle Benutzenden arbeiten mit eigener persönlicher Identifikation und erhalten die nötigen Daten aufgrund von Datei-Berechtigungen.

2.2 Die individuelle Identifikation ist mit starkem persönlichem Passwort oder einem besseren anerkannten Verfahren eingerichtet. Die Verwendung starker Passwörter ist auch dort vorgeschrieben, wo die Einrichtung schwacher Passwörter technisch nicht verhindert wird.[1)]

2.3 Der Zugangsschutz ist so eingerichtet, dass der oder die Systemadministrierende die einzige Person ist, die über Systemrechte verfügt. Es wird sichergestellt, dass nur die nötigen Benutzenden- und Systemkonti eingerichtet sind.

2.4 Die berechtigten Personen können ihre Daten vor Einsicht durch andere auf den selben Computern tätigen Berechtigten individuell schützen. Die Einsichtnahme geschützter Daten durch den Systemadministrator ist für diesen obwohl verboten nicht technisch verhindert.

---

1) Siehe *Richtlinien für den Einsatz von Informatikmitteln* §3.

2.5 Empfohlen ist die Einrichtung einer Personal Firewall derart, dass nur die nötigen Verbindungen von aussen her möglich sind. Wenn das Betriebssystem eine mitgelieferte Personal Firewall enthält, muss entweder diese oder ein anderes Produkt aktiviert sein.

2.6 Das System ist so eingerichtet, dass eine automatische Sperrung des Bildschirms nach maximal zwanzig Minuten inaktiver Zeit erfolgt. Es sind aber in der Regel keine besonderen Vorkehrungen getroffen, die verhindern, dass eine Person mit physischem Zugang mit verbotenen Mitteln in den Computer eindringen kann.

2.7 Die Zugänglichkeit über das Netzwerk von ausserhalb der Universität ist auf verschlüsselte Protokolle beschränkt, d. h. die IP-Nummer des Systems ist für Transistor, die zentrale Firewall der Universität, in der Standard-Klasse.

2.8 Die Leitung der Organisationseinheit kann im Notfall, z. B. bei plötzlicher Beendigung des Arbeitsverhältnisses im Unfrieden oder durch Tod, den Zugriff auf die Arbeits-Daten der Organisationseinheit mit besonderen Methoden anordnen. Zu diesem Zweck notwendige Vorkehrungen, wie das Deponieren des Systemadministrator-Passworts in einem verschlossenen Kuvert im Tresor, sind vorsorglich getroffen.

2.9 Es werden keine Daten gehalten oder bearbeitet, die geheim sind, d.h. einem Berufsgeheimnis unterstellt sind, im Sinne des Datenschutzgesetzes besonders schützenswerte Personendaten darstellen oder im Rahmen von Dienstreglementen der Organisationseinheiten als geheim klassifiziert sind.

3. Bezüglich **Datensicherheit** sind die für das System Verantwortlichen verpflichtet, dafür zu sorgen, dass folgende Bedingungen erfüllt werden:

3.1 Der Datenbestand der Endbenutzenden wird regelmässig gesichert oder die Endbenutzenden verwenden einen bezeichneten Speicherbereich auf einem Server der Organisationseinheit, wo eine regelmässige Datensicherung durchgeführt wird.

3.2 Der Turnus der Datensicherung ist täglich bis wöchentlich, jedenfalls aber so häufig, dass der durch verloren gegangene Mutationen erzeugte Schaden mit vertretbarem Aufwand durch die Endbenutzer behoben werden kann.

3.3 Die Datensicherung wird nach jeder Verfahrensänderung sowie mindestens einmal alle drei Monate geprüft.

3.4 Bei Beendigung des Arbeitsverhältnisses findet eine Übergabe der Arbeits-Daten an den Arbeitgeber statt.

4. Bezüglich **Verfügbarkeit** werden die folgenden Bedingungen erfüllt:

4.1 Die reguläre Systemwartung ist so geplant, dass sie einerseits sorgfältig durchgeführt werden kann, andererseits die Zweckerfüllung des Systems nicht unnötig beeinträchtigt. Wo die Systempflege nicht durch den Endbenutzer selbst geschieht, werden die Ausfallzeiten vorher vereinbart.

4.2 Die Arbeit mit dem System ist so geplant, dass durch dessen ungeplanten Ausfall kein hoher Schaden entsteht. Die für das Bereitstellen einer Ersatzlösung nötige Zeit und die Kosten sind dabei angemessen berücksichtigt.