# Norm 01

**Normen für den Betrieb von Systemen an der Universität Zürich**

## 1. Gültigkeit dieser Norm

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, vertretbare alternative Sicherheitskonzepte aufgezeigt, festgehalten und umgesetzt werden.

## 2. Normen

### *1. Bekämpfung des Missbrauchs durch Dritte*

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 SicherheitsUpdates 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. Zugang zu Systemen und Vertraulichkeit*

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.

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 Benutzendenund 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.

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. Datensicherheit*

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. Verfügbarkeit

Bezüglich Verfügbarkeit werden die folgenden Bedingungen erfüllt:

4.1 Die reguläre Systemwartung ist so geplant, dass sie einerseits sorgfältig durchgeführt werden kann, anderseits 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.