Weisung für den Betrieb von Systemen (WBS)

(vom 27.10.2006, Stand 5.11.2024[1])

Die Zentrale Informatik,

gestützt auf § 6 Abs. 2 Bst. g des Reglements über den Einsatz von Informatikmitteln an der Universität Zürich vom 29.11.2022, Stand 5.11.2024 (REIM),

erlässt folgende Weisung:

1 Grundsätzliches

Die Weisung für den Betrieb von Systemen (WBS) legt Minimalstandards für den Betrieb der Informatikmittel der UZH fest.

1.1 Geltungsbereich

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

Ausnahmen von dieser Weisung bedingen ein alternatives Sicherheitskonzept gemäss REIM §13.

1.2 Begriffe

Die im Reglement über den Einsatz von Informatikmitteln (REIM) definierten Begriffe gelten analog.

2 Organisatorische und technische Vorgaben

Nachfolgende Kapitel beschreiben detaillierte organisatorische und technische Vorgaben zur Sicherstellung des Betriebs von Informatikmitteln der UZH.

2.1 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) 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 Zentralen Informatik ist zu beachten.

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

[1] Die Weisung wurde per 5.11.2024 ins neue UZH Corporate Design überführt und an die Struktur der Weisung über die Netzwerksicherheit (WNS) angeglichen. In der Vergangenheit war diese Weisung als «Normen für den Betrieb von Systemen (NBS)» bezeichnet. Inhaltlich wurden keine Änderungen vorgenommen.

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.

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 E-Mail oder der Webseite verdächtig ist.

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

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.

2.2 Zugang zu Systemen und Vertraulichkeit

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

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) 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.

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.

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

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.

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.

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.

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.

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.

2.3 Datensicherheit

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

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.

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

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

2.4 Verfügbarkeit

Bezüglich Verfügbarkeit werden die folgenden Bedingungen erfüllt:

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.

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.

3 Schlussbestimmungen

3.1 Inkrafttreten

Die Weisung für den Betrieb von Systemen (WBS) ist seit 27.10.2006 in Kraft und ist bis auf Widerruf gültig.

3.2 Übergangsfrist

Für Umsetzung und Einhaltung dieser Weisung besteht eine Übergangsfrist von 12 Monaten ab Inkrafttreten.