Merkblatt „Informatik-Einsatz“ für Mitarbeitende

1 Rechte

Als Mitarbeitende der Universität gehören Sie zu einer Organisationseinheit der Universität. Je nach Anstellungsbedingungen dürfen oder müssen Sie eigene oder Ihnen zur Verfügung gestellte Informatikmittel für Ihre Arbeit einsetzen. Das ist insbesondere auch das Netzwerk der Universität und die zur Verfügung gestellten Anwendungen. Eine private Nutzung ausserhalb der eigentlichen Arbeitszeit ist zugelassen, wenn sie unbedeutend und nicht kommerziell ist. Sie dürfen Server oder Peer-to-Peer-Programme nur im Auftrag der Organisationseinheit für Ihre Arbeit betreiben. Mit der Nutzung der universitären Informatikmittel akzeptieren Sie, dass das Netzwerk überwacht wird und dass technische Massnahmen die Nutzung auf bestimmte Verfahren einschränken können.

2 Missbrauch

Im Zusammenhang mit der Universität gelten zusätzlich zu den gesetzlichen Vorgaben die Universitätsordnung, das Reglement für den Einsatz von Informatikmitteln an der Universität und die Normen für den Betrieb von Systemen an der Universität[1]. Im Rahmen Ihrer Anstellung können weitere Bestimmungen gelten. Sie dürfen also unter anderem mit Informatikmitteln nicht,

2.1 das Netzwerk der Universität absuchen oder unberechtigt in ein System einzudringen versuchen,

2.2 schädlichen Programmcode erstellen oder verbreiten,

2.3 Daten oder Software widerrechtlich herunterladen, kopieren oder installieren,

2.4 die Immaterialgüterrechte von Dritten (Copyright) verletzen,

2.5 andere Personen mit E-Mail oder Webseiten verunglimpfen, schädigen oder belästigen,

2.6 E-Mail-Absenderadressen oder IP-Adressen vortäuschen,

2.7 Daten mit rechtswidrigem, pornografischem, rassistischem, sexistischem oder Gewalt verherrlichendem Inhalt nutzen, verarbeiten, speichern oder übermitteln.

3 Verantwortung für das System

Sie sind grundsätzlich verantwortlich für das Computersystem, das Sie im Zusammenhang mit der Universität verwenden. Wird Ihnen ein Computersystem durch die Organisationseinheit zur Verfügung gestellt, wird diese in der Regel die Verantwortung für das unveränderte oder nach lokaler Anleitung betriebene System übernehmen.

Auch wenn Sie jemanden beauftragen, Ihr eigenes System einzurichten und zu pflegen, bleiben Sie gegenüber der Universität für dessen oder deren Leistung verantwortlich.

4 Schutz der Systeme vor Schadprogrammen und vor Missbrauch durch Dritte

Computersysteme dürfen nur dann mit dem Netzwerk der Universität verbunden sein, wenn sie

1 Siehe http://www.id.uzh.ch/dl/sicher/Vorschriften.html und http://www.rd.uzh.ch/rechtssammlung/richtlinien.html

4.1 bezüglich der vom Hersteller empfohlenen Systemwartung auf dem neuesten Stand sind,

4.2 einen Virenschutz eingerichtet haben, der ebenfalls in jeder Beziehung auf dem neuesten Stand gehalten wird,

4.3 wenn alle über das Netzwerk zugänglichen Benutzer-Konti über ein starkes Passwort oder ein noch besseres Verfahren geschützt sind, und sie

4.4 soweit bekannt frei von Schadprogrammen sind.

Verzichten Sie auf das Anklicken von Verweisen und das Öffnen von Anhängen, sobald der Inhalt der E-Mail oder der Webseite verdächtig ist!

5 Zugangsschutz

Die Passwörter Ihres ITIM-Kontos und der im ITIM verwalteten Konti sind persönlich und dürfen niemandem zugänglich gemacht oder mitgeteilt werden. Sie sollten für ITIM ein eigenes Passwort wählen. Wenn Sie den Verdacht haben, dass ein Passwort einer anderen Person bekannt wurde, müssen Sie es umgehend überall dort ändern, wo Sie es eingerichtet haben. Bewahren Sie das ITIM-Passwort an einem sicheren Ort auf, da Sie damit Ihre anderen Passwörter neu setzen können.

Richten Sie Ihren eigenen PC so ein, dass der Bildschirm nach maximal 20 Minuten ohne Eingabe automatisch gesperrt wird. Lösen Sie die Sperrung immer von Hand aus, wenn Sie den PC an unsicherem Ort eingeschaltet verlassen. Auch zum Schutz des PCs vor Ort sind starke Passwörter nötig.

Starke Passwörter sind mindestens 8 Zeichen lang, haben von jeder der vier Buchstabenklassen (Grossbuchstaben, Kleinbuchstaben, Ziffern und Satzzeichen) mindestens einen Vertreter und haben keine erkennbare Konstruktionsregel.

6 Datensicherung und Verfügbarkeit

Überprüfen Sie die Sicherung Ihrer Daten regelmässig und machen Sie sich bewusst, welche Auswirkungen der plötzliche Verlust Ihrer gewohnten Informatikmittel auf Ihre Arbeit hätte.

7 Hilfe

Bei allen Problemen wenden Sie sich an die IT-Verantwortliche oder den IT-Verantwortlichen Ihrer Organisationseinheit oder eine von ihr oder ihm bezeichnete Person. Wenn Sie Missbräuche durch Universitätsangehörige feststellen, melden Sie diese Ihrem Vorgesetzten.