| UniversitätsSpital Zürich | | Spitaldirektion | |
|---|---|---|---|
| Dokumentenart | Weisung ICT | Version | 03.09.2015 |
| Erlassen durch | SDI | Gültig ab | 06.11.2015 |
| Geltungsbereich | USZ | Ersetzt | 01.04.2014 |
| Erstellt durch | ICT | Kurztitel | WE_Benutzung Informatikmittel |

# Weisung über die Benutzung der Informatikmittel im USZ

## 1. Ziel

Die Weisung für die Benutzung der Informatiksysteme und -anwendungen regelt den Umgang und die Nutzung der zur Verfügung stehenden Informatikmittel. Sie stellt eine Präventivmassnahme dar, um Missbräuche einzuschränken und die Sicherheit der Systeme und Anwendungen zu erhöhen.

## 2. Definition

Informatikmittel umfassen Informatiksysteme und Informatikanwendungen.

Informatiksysteme sind sämtliche Geräte und Einrichtungen sowie die dazugehörende Infrastruktur und Software, die zur elektronischen Bearbeitung von Daten eingesetzt werden.

Informatikanwendungen umfassen Programme, welche die Nutzung von Informatiksystemen für die Erfüllung oder Unterstützung bestimmter Aufgaben ermöglichen einschliesslich netzbasierter Anwendungen für Datenaustausch via Internet (z.B. WWW), Social Media und elektronische Kommunikationsdienste (z.B. E-Mail, Instant Messaging und SMS).

## 3. Geltungsbereich

Diese Weisung gilt für alle Mitarbeitenden, Dienstleistenden, Zuliefernden und Assoziierte, welche Informatiksysteme und -anwendungen des USZ nutzen (sog. 'Benutzende').

## 4. Allgemeine Pflichten der Benutzenden

Die Benutzenden sind verpflichtet, die gesetzlichen Vorgaben und die in dieser Weisung präzisierten Regelungen einzuhalten. Sie haben die Kenntnisnahme dieser Weisung unterschriftlich zu bestätigen.

Die Benutzenden sind verpflichtet, die ihnen zur Verfügung gestellten Informatikmittel recht- und zweckmässig einzusetzen und Informationen, insbesondere schützenswerte Informationen wie Mitarbeiter- und Patientendaten, nicht an unberechtigte Adressaten weiterzuleiten oder diesen zugänglich zu machen.

Die Benutzenden melden alle sicherheitsrelevanten Ereignisse sowie Schäden und Verlust von Hardware und Software der Hotline der Direktion ICT.

Benutzende erhalten für den Zugriff auf die Applikationen und Systeme persönliche Benutzerkontos mit persönlichem Passwort oder funktionelle Kontos. Sie sind für die mit ihrem Konto erfolgten Zugriffe verantwortlich. Auf gemeinsam benutzten Systemen ("Stations-PC") haben sich Benutzende nach Abschluss der Tätigkeiten von der Arbeitssitzung abzumelden ("Logout").

## 5. Passwortregeln

Passwörter sind vertraulich zu behandeln. Benutzende dürfen Passwörter nicht aufschreiben, unverschlüsselt auf Systemen speichern oder Dritten bekannt geben. Insbesondere darf das USZ-Passwort nicht auch für weitere, nicht USZ-zugehörige Dienste verwendet werden. Das Passwort muss bei entsprechender Aufforderung geändert werden. Passwörter müssen neben Buchstaben auch Zahlen und, wenn möglich, Sonderzeichen (z.B. '%@', etc.) enthalten.

## 6. Datenschutz und Informationssicherheit

Die Benutzenden haben zu verhindern, dass Unbefugte Zutritt zu den Arbeitsräumlichkeiten haben. Halten sich externe Personen in den Arbeitsräumen auf, ist dafür zu sorgen, dass diese keinen unbefugten Zugang zu Informationen erhalten.

Der Arbeitsplatz ist bei Abwesenheit so zu hinterlassen, dass keine vertraulichen oder schutzbedürftigen Unterlagen und Datenträger offen zugänglich sind. Ausdrucke mit vertraulichen Informationen sind umgehend aus dem Drucker zu entfernen.

Aus Sicherheitsgründen ist ebenfalls vorzusehen, dass Daten auf dem USZ-Netzwerklaufwerk gespeichert werden.

Benutzer von Einzelplatzsystemen sind selbst für die Datensicherung und die datenschutzgerechte Aufbewahrung der dazu verwendeten Datenträger verantwortlich.

Die dienstliche Nutzung von externen Dienstleistungen wie Google, Yahoo, Hotmail, Dropbox etc. für den Austausch oder die Speicherung von Geschäftsdaten ist nicht erlaubt.

Für den sicheren Datenaustausch grosser Dateien steht im USZ über https://transfer.usz.ch ein Server zur Verfügung.

Schützenswerte Daten, insbesondere Personal- oder Patientendaten, dürfen nur soweit eingesehen, verwendet, verarbeitet und weitergegeben werden, als dies für die Auftragserfüllung unbedingt erforderlich ist. Patienten- und Personendaten sowie Geschäftsdaten dürfen nicht für private Zwecke vom Arbeitsplatz entfernt werden. Eine Weitergabe von schützenswerten Daten an Dritte (Dienstleister, Zulieferer und Assoziierte) erfordert die vorgehende Zustimmung durch die verantwortliche Stelle (Dateninhaber oder Rechtsdienst, siehe USZ Informationssicherheitsweisung).

Datenzugriffe werden zentral protokolliert. Unberechtigte Zugriffe werden nachverfolgt und haben personalrechtliche Konsequenzen. Dies gilt insbesondere auch für das Klinikinformationssystem (KISIM).

Es dürfen keine Auskünfte über die im USZ eingesetzten Systeme an unbekannte Personen oder Firmen gegeben werden. Anfragen dieser Art sind an die Direktion ICT weiterzuleiten.

## 7. Hard- und Software

Es darf nur Hard- und Software verwendet werden, die das USZ offiziell beschafft hat, und die Direktion ICT zur Installation freigegeben hat. Auf begründeten Antrag ist der Zugang auf ICT Dienstleistungen mit einem privaten Gerät über die Virtual Desktop Infrastruktur (VDI) möglich.

Die Kontrolle und der Unterhalt der über das USZ beschafften Hard- und Software obliegen ausnahmslos der Direktion ICT. Die Benutzenden dürfen Informatiksysteme, die am Netzwerk angeschlossen sind, nicht gleichzeitig mit einem Netz oder System ausserhalb des USZ-Netzwerkes verbinden. Nur die Direktion ICT darf Geräte in die Reparatur oder zur Entsorgung geben. Sie stellt sicher, dass keine schützenswerten Daten auf diesem Weg das USZ verlassen. Änderungen an Systemeinstellungen (Installation, Deinstallation, Änderung der Konfiguration etc.) dürfen nur durch die Direktion ICT vorgenommen werden.

Festinstallierte Systemkomponenten und Peripheriegeräte dürfen nur auf Anweisung und in Abstimmung mit der Direktion ICT vom Arbeitsplatz entfernt und gezügelt werden.

Private Geräte dürfen nicht für dienstliche Aufgaben eingesetzt und ans Netzwerk angeschlossen werden.

Die Synchronisation von USZ E-Mail-, Kalender- und Kontaktdaten mit privaten Mobilgeräten ist erlaubt.

## 8. Virenschutz

Die Benutzenden dürfen die Virenschutzsoftware und deren laufende Aktualisierung nicht ausschalten, blockieren oder umkonfigurieren. Die Benutzenden mit Einzelarbeitsplätzen sind dafür verantwortlich, dass auch auf diesen Systemen der Virenschutz nach den Vorgaben der Direktion ICT aktuell gehalten wird. Im Zweifelsfalle soll die Hotline der Direktion ICT informiert werden.

Die Direktion ICT bietet eine Dienstleistung an, durch welche mobile Datenträger vor einem Einsatz an einem USZ-Gerät auf Viren geprüft werden können.

## 9. E-Mail

E-Mails sind mit der gleichen Sorgfalt zu behandeln wie der entsprechende Schriftverkehr. Schützenswerte Daten, wie Patienten- oder Personendaten dürfen vom USZ als Absender und Initiant der E-Mail-Kommunikation nur verschlüsselt an Empfangende versandt werden. Wenn jedoch die E-Mail-Kommunikation nicht vom USZ initiiert wird und der Geheimnisherr dem USZ bereits schützenswerte Daten unverschlüsselt schickt, geht das USZ davon aus, dass der Geheimnisherr diese Art der Kommunikation explizit wünscht bzw. konkludent damit einverstanden ist, dass das USZ ebenfalls in einer unverschlüsselten E-Mail eine entsprechende Antwort geben oder die erfragten Informationen, sofern es sich dabei um unwesentliche und wenig umfangreiche Daten handelt, übermitteln darf. Das USZ klärt den Absender der E-Mail vorab in geeigneter Weise über die fehlende Vertraulichkeit der unverschlüsselten E-Mail-Kommunikation auf.

Das automatische Umleiten (Forwarding) von E-Mails an Adressen ausserhalb des USZ, insbesondere an private E-Mail-Kontos, ist nicht erlaubt. Die Umleitung von E-Mails an die UZH ist vom Forwarding-Verbot ausgenommen. Ebenfalls zu unterlassen ist die Weiterleitung an interne Stellvertreter. Bei Abwesenheit ist die Funktion des Abwesenheitsassistenten zu nut-

zen, um Absendende einzuladen, selbst die entsprechenden Nachrichten den Stellvertretenden nochmals zu senden. Bei unvorhersehbarer Abwesenheit und bei Unerreichbarkeit des Mitarbeitenden ist das USZ ermächtigt, den Abwesenheitsassistenten zu aktivieren.

Das Versenden oder Weiterleiten von E-Mails mit rechtswidrigem, pornografischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt, mit unnötig grossem Verteiler, mit grossen Datenmengen oder mit der Aufforderung zum Weiterversand im Schneeballsystem (Kettenbriefe) ist verboten.

Die Nutzung des USZ Outlook Web Mail Zugangs ist nur auf USZ-Informatikgeräten, einem Gerät der UZH oder der ETH oder auf privaten Geräten der Benutzenden, die über einen aktuellen Virenschutz verfügen und regelmässig gewartet (Updates) werden, erlaubt.

## 10. Private Nutzung von Internet oder E-Mail

Die zurückhaltende Nutzung der Informatikmittel des USZ für private Zwecke ist grundsätzlich gestattet, soweit dadurch Systemressourcen wie Speicher und Übertragungskapazität nicht im Übermass belastet werden.

Die private Nutzung soll ausserhalb der Arbeitszeit erfolgen. Während der Arbeitszeit ist sie auf ein Minimum zu beschränken. Die Auftragserfüllung darf nicht beeinträchtigt werden. Die private Nutzung der USZ-Informatiksysteme zugunsten Dritter oder zu kommerziellen Zwecken ist nicht erlaubt.

Der Zugriff auf Internet-Seiten mit rechtswidrigem, pornografischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt ist untersagt.

Dienstliche E-Mail-Adressen dürfen nicht für private Zwecke im Internet abgelegt werden.

## 11. Missbrauch der Internet- und E-Mail-Dienste

Die Direktion ICT kann jederzeit Berichte erstellen, die Aufschluss über die verwendeten Internet-Adressen und soweit möglich über Zeitpunkt und Anzahl der Zugriffe und übertragenen Datenmengen geben. Die Kontrolle hat in dieser Phase anonym zu erfolgen.

Werden im Rahmen dieser anonymen Kontrollen Verstösse gegen diese Nutzungsregelung festgestellt, informiert die Direktion ICT das Legal Compliance Office. Liegen bei Internet-Zugriffen Missbräuche von erheblicher Tragweite vor oder besteht beim E-Mail-Verkehr ein konkreter Verdacht auf Missbrauch und erscheint die Zahl der überwachten Personen sowie die Überwachungsdauer im Hinblick auf den allfälligen Missbrauch verhältnismässig, kann die Direktion ICT nach vorgängiger Abmahnung durch die Spitaldirektion die Internet-Zugriffe oder den E-Mail-Verkehr fortan personenbezogen protokollieren und auswerten. Der Überwachungszeitraum darf drei Monate nicht übersteigen. Eine permanente Überwachung ist unzulässig.

Nach Erhalt der Ergebnisse der personenbezogenen Auswertungen entscheidet die Spitaldirektion, ob Sanktionen verhängt werden sollen (Ziffer 13).

Bei Verdacht auf strafrechtlich relevantes Verhalten können die Strafverfolgungsbehörden ohne Vorwarnung die Internetnutzung beziehungsweise den E-Mail-Verkehr einer Person auswerten.

## 12. Beendigung des Anstellungsverhältnisses

Auf den letzten Arbeitstag hin deaktiviert das USZ alle Benutzerkonten der austretenden Mitarbeitenden. Diese haben alle USZ-Informatikmittel dem USZ als Arbeitgeber zurück zu geben bzw. wieder zur Verfügung zu stellen. E-Mails, die nach der Deaktivierung an E-Mail-Adressen gesendet werden, werden ohne Weiterleitung abgewiesen (Zustellfehlerbericht). Abweichende Vereinbarungen im Einzelfall bleiben vorbehalten.

Die Mitarbeitenden sind verpflichtet sicher zu stellen, dass Geschäftsdokumente jederzeit in den Geschäftsverzeichnissen (und weder im persönlichen Mail-Konto noch auf dem persönlichen Laufwerk) abgelegt sind, sodass das USZ auch bei unvorhergesehenen Abwesenheiten sowie nach Austritt Zugriff auf alle Geschäftsdokumente hat. Es ist den austretenden Mitarbeitenden untersagt, Geschäftsdaten mitzunehmen.

Das USZ ist berechtigt, nach Beendigung des Anstellungsverhältnisses sämtliche Daten auf den Privatlaufwerken sowie E-Mail-Konten zu löschen. Besteht die Vermutung, dass sich Geschäftsdokumente darauf befinden, wird der ehemalige (oder abwesende) Mitarbeiter abgemahnt und aufgefordert, die Geschäftsdokumente auf Geschäftsverzeichnisse zu überführen. Verweigert er die Mitwirkung oder ist er unerreichbar, ist das USZ berechtigt, im Sinne einer Ersatzmassnahme auf die privaten Verzeichnisse und E-Mail-Konten zuzugreifen, um die Geschäftsdokumente zu übertragen.

## 13. Sanktionen

Sanktionen werden getroffen, wenn eine Verletzung dieser Nutzungsregelung bzw. missbräuchliche oder gesetzeswidrige Nutzung der Informatikmittel nachweisbar feststeht.

Ein Missbrauch hat personalrechtliche Konsequenzen zur Folge. Bei Verstoss gegen das Strafgesetz und bei Verletzung der Rechte Dritter, insbesondere von Urheberrechten, muss mit straf- bzw. zivilrechtlichen Konsequenzen gerechnet werden. Grundsätzlich haften Benutzende für den Schaden, den er oder sie absichtlich oder grobfahrlässig dem USZ zufügt.