USZ Universitäts Spital Zürich		Spitaldirektion	
Dokumentenart	Weisung	Version	03.04.2020
Erlassen durch	SDI	Gültig ab	04.05.2020
Geltungsbereich	USZ	Ersetzt	Weisung über die Benutzung der Informatikmittel im USZ
Erstellt durch	CISO	Kurztitel	WS Nutzung IT-Mittel

Weisung
Informationssicherheit – Nutzung der Informatikmittel am USZ

1. Einführung

Die vorliegende Weisung ergänzt die Weisung «Informationssicherheit – Information Security Management System Governance» und regelt spezifisch den Umgang und die Nutzung der am USZ zur Verfügung stehenden Informatikmittel. Sie konkretisiert die Pflichten der am USZ tätigen Personen, welche Informatikmittel nutzen; unabhängig davon, ob eine Anstellung mit dem USZ oder mit Dritten besteht. Die Klassifizierung von Daten ist in der Weisung «Informationssicherheit – Information Security Management System Governance» geregelt.

Der Begriff Informatikmittel umfasst sämtliche Hard- und Software, welche für die elektronische Bearbeitung von Daten eingesetzt wird und/oder welche die Erfüllung oder Unterstützung von bestimmten Aufgaben ermöglicht. Dies schliesst die Nutzung von Servern, Netzwerken, Clients (PC, Laptops etc.), Peripheriegeräte, Betriebssystemen, Programmen und Anwendungen inkl. Internet, Cloudlösungen, Social Media, E-Mail, Instant Messaging und SMS ein.

2. 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 im Rahmen der Eintrittsformalitäten unterschriftlich zu bestätigen.
- Die Benutzenden sind verpflichtet, die ihnen zur Verfügung gestellten Informatikmittel recht- und zweckmässig einzusetzen und Informationen sowie Daten, insbesondere vertrauliche Daten wie Patienten- und Mitarbeiterdaten, nur in Übereinstimmung mit der USZ Weisung zum Datenschutz zu bearbeiten, an Dritte weiterzuleiten oder diesen zugänglich zu machen.
- Geschäftsdokumente müssen in Geschäftsverzeichnissen abgelegt werden, sodass das USZ auch bei unvorhergesehenen Abwesenheiten sowie nach Austritt Zugriff auf alle Geschäftsdokumente hat. Der Zugriff auf Geschäftsverzeichnisse mit vertraulichen Dokumenten kann über die ICT nach Bedarf weiter eingeschränkt werden. Persönliche Dokumente (Lebenslauf, Zeugnisse etc.) dürfen auf dem persönlichen Laufwerk gespeichert werden. Private Dokumente dürfen nicht bzw. nur eingeschränkt auf dem persönlichen Laufwerk abgelegt werden (vgl. 8. Private Nutzung).
- Benutzende erhalten für den Zugriff auf Systeme und Anwendungen persönliche Benutzerkontos mit persönlichem Passwort. Sie sind für die mit ihrem Konto erfolgten Zugriffe verantwortlich.
- Auf gemeinsam benutzten Systemen ("Stations-PC") haben sich Benutzende nach Abschluss der Tätigkeiten abzumelden ("Logout").
- Wird ein Arbeitsplatz verlassen, muss das genutzte Gerät gesperrt werden (Ctrl + Alt + Del bzw. Win + L).
- Die Benutzenden melden alle sicherheitsrelevanten Ereignisse sowie Schäden und Verlust von Hardware und Software unmittelbar der Hotline der Direktion ICT.

3. Datenschutz und Informationssicherheit

- Die Benutzenden haben darauf zu achten, dass Unbefugte keinen Zutritt zu den nicht öffentlichen Arbeitsräumlichkeiten haben. Halten sich externe Personen in nicht öffentlichen Arbeitsräumen auf, müssen diese begleitet werden. Dabei ist darauf zu achten, dass diese keinen Zugang zu nicht öffentlichen Informationen erhalten.
- Der Arbeitsplatz ist bei Abwesenheit so zu hinterlassen, dass keine vertraulichen oder höher klassifizierten Unterlagen und Datenträger offen zugänglich sind.

- Werden vertrauliche oder höher klassifizierte Dokumente gedruckt, muss dies über «Follow-me Printing» geschehen.
- Interne und höher klassifizierte Daten (ab Datenschutzklasse 2) müssen innerhalb des USZ-Netzwerks oder auf durch das USZ zur Verfügung gestellten bzw. zugelassenen Online-Informatikdienstleistungen gespeichert werden.
- Für öffentliche und interne Daten (Datenschutzklasse 1-2) gilt eine Online-Informatikdienstleistung als durch das USZ zugelassen, wenn mindestens die allgemeinen Geschäftsbedingungen sowie die Datenschutzbestimmungen des Anbieters den Vorgaben des USZ entsprechen, die Verrechnung für die Nutzung über das USZ abgewickelt wird und der Zugriff über USZ Nutzerprofile erfolgt (z.B. Terminumfrage über Doodle, Projekte über Trello, Umfragen über SurveyMonkey).
- Für vertraulich und höher klassifizierte Daten (Datenschutzklasse 3-5) gilt eine Online-Informatikdienstleistung als durch das USZ zugelassen, wenn diese durch den Rechtsdienst und den Chief Information Security Officer abgenommen wurde.
- Die Nutzung von privaten Messenger Services (z.B. WhatsApp) ist für die Meldung von Verspätungen, Abwesenheiten etc. zulässig. Geschäftliche Daten, insbesondere vertrauliche Daten oder Patientendaten dürfen nicht über private Messenger Services ausgetauscht werden.
- Die betriebliche Nutzung von Informatikmitteln, welche nicht durch das USZ zugelassen sind, ist untersagt (hiervon ausgenommen ist die temporäre Nutzung von lokalen Speichermedien).
- Die dauerhafte Speicherung von Daten auf lokalen Speichermedien wie USB-Sticks ist nicht zulässig. Werden vertraulich oder höher klassifizierte Daten temporär auf einem lokalen Speichermedium abgelegt, müssen diese verschlüsselt werden. Handelt es sich dabei nur um einzelne Daten z.B. wenige Angaben zu einer einzelnen Person, kann der Datenträger alternativ z.B. durch konsequentes wegschliessen und den Transfer über einen sicheren Kanal geschützt werden. Das USZ bietet hierzu sowohl verschlüsselte wie auch unverschlüsselte Speichermedien an.
- Nicht mehr verwendete lokale Speichermedien müssen physisch vernichtet und/oder so formatiert werden, dass die Wiederherstellung der Daten nicht möglich ist.
- Vertrauliche Unterlagen und Dokumente müssen über die dafür zur Verfügung stehenden Behälter für die Entsorgung von Diskret-Makulatur entsorgt werden.
- Als Alternative für den Datentransfer über lokale Speichermedien steht im USZ für den sicheren Datenaustausch grosser Dateien der Transfer Service (https://transfer.usz.ch) zur Verfügung.
- Datenzugriffe dürfen nur nach dem Need-to-Know Prinzip erfolgen und werden zentral protokolliert. Unberechtigte Zugriffe werden auf Antrag nachverfolgt und haben personalrechtliche Konsequenzen.
- 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.
- Passwörter sind vertraulich zu behandeln. Passwörter dürfen nicht aufgeschrieben, unverschlüsselt auf Systemen gespeichert oder Dritten bekannt geben werden. Zudem dürfen am USZ verwendete Passwörter nur am USZ verwendet werden und nicht auch für weitere, nicht USZ-zugehörige Dienste. Das Passwort muss bei entsprechender Aufforderung geändert werden. Passwörter müssen mindestens 08, besser 12 Zeichen lang sein und neben Buchstaben auch Zahlen und Sonderzeichen (z.B. '%@', etc.) enthalten.

4. Hard- und Software

- Es darf nur Hard- und Software verwendet werden, die das USZ beschafft und/oder 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 Speicherung von nicht öffentlichen Daten auf privaten Geräten ist nicht gestattet (vgl. Weisung über die Nutzung von mobilen Geräten).
- Der Betrieb und der Unterhalt der Hard- und Software darf ausschliesslich durch die Direktion ICT oder durch die Bereiche Medizinische Informatik, Administrative Applikationen oder Informatik Forschung & Entwicklung wahrgenommen werden.
- Die Verbindung von Informatikmitteln mit einem Netz oder System ausserhalb des USZ-Netzwerkes, muss über die ICT erfolgen.
- Die Entsorgung oder Reparatur von Informatikmitteln darf ausschliesslich durch die Direktion ICT oder durch die Abteilung Medizintechnik erfolgen.
- Festinstallierte Systemkomponenten und Peripheriegeräte dürfen nur auf Anweisung und in Abstimmung mit der Direktion ICT vom Arbeitsplatz entfernt und gezügelt werden.

5. Mobile Geräte

- Unter mobilen Geräten versteht das USZ Handy, Tablet, Laptops und weitere tragbare Geräte, egal ob diese dem USZ gehören oder ob es private Geräte sind, die für USZ-Zwecke verwendet werden (z.B. für das Lesen von E-Mails).
- Die Synchronisation von USZ E-Mail-, Kalender- und Kontaktdaten mit privaten Mobilgeräten ist im Rahmen der Weisung über die Nutzung von mobilen Geräten erlaubt.
- Sofern auf einem mobilen Gerät besondere Personendaten (Datenschutzklasse 4) bearbeitet werden, muss dieses in das «Mobile Device Management» des USZ eingebunden sein.
- Weitere zu beachtende Details sind in der Weisung über die Nutzung von mobilen Geräten geregelt.

6. Virenschutz

- Sämtliche innerhalb des USZ-Netzwerk betriebene Systeme müssen über einen aktuellen Virenschutz verfügen. Nutzer dürfen die Virenschutzsoftware und deren laufende Aktualisierung nicht ausschalten, blockieren oder deren Konfiguration verändern.
- Für nicht zentral verwaltete Clients (Laptops, PC etc.) verantwortliche Personen müssen sicherstellen, dass die Systeme über einen aktuellen Virenschutz verfügen.
- Mobile Datenträger wie USB-Sticks dürfen nur mit USZ-Geräten verbunden werden, wenn sie aus einer bekannten und vertrauenswürdigen Quelle stammen.

7. Empfangen und Versenden von E-Mails

- Obwohl das USZ über umfangreiche technische Mittel verfügt, um E-Mails mit Schadsoftware und/oder Phishing Emails abzufangen, erreichen einzelne dieser E-Mails die Nutzer. E-Mails müssen daher immer kritisch geprüft werden. Verdächtig erscheinende E-Mails müssen der ICT-Hotline gemeldet werden. Anhänge oder Links in verdächtig erscheinenden E-Mails dürfen nicht geöffnet werden.
- Vertrauliche Daten, insbesondere Patientendaten, dürfen nur verschlüsselt an externe Empfänger verschickt werden. Hierfür steht am USZ der HIN Secure E-Mail Service zur Verfügung.

- Sofern das USZ durch eine Drittperson (z.B. Patient) per E-Mail angeschrieben wird und die Echtheit des Absenders feststeht, kann die Beantwortung der Frage unverschlüsselt erfolgen. Nach Bedarf und Möglichkeit muss der Absender auf die fehlende Vertraulichkeit eines unverschlüsselten E-Mails aufmerksam gemacht werden.
- Das automatische Umleiten (Forwarding) von E-Mails an Adressen ausserhalb des USZ ist nicht erlaubt.
- Ebenfalls nicht erlaubt ist die automatische Weiterleitung von E-Mails an interne Stellvertreter. Um bei Anwesenheit die Stellvertretung zu gewährleisten, kann die Stellvertreterfunktion in Outlook genutzt und/oder in der Abwesenheitsmeldung auf die Stellvertretung verwiesen werden.
- Bei unvorhersehbarer Abwesenheit und bei Unerreichbarkeit des Mitarbeitenden ist das USZ ermächtigt, den Abwesenheitsassistenten zu aktivieren.
- Die interne automatische Weiterleitung aus einer internen Gruppen-Mailbox an einzelne interne empfangsberechtigte Personen ist zulässig.
- 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 (OWA) 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. Private Geräte, welche nicht über einen aktuellen Virenschutz verfügen und nicht regelmässig aktualisiert werden, dürfen nicht über OWA mit dem USZ-Netzwerk verbunden werden.

8. Private Nutzung von Informatikmittel des USZ (Internet, Outlook, persönliches Laufwerk)

- 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 angegeben werden.

9. Beendigung des Anstellungsverhältnisses

- Auf den letzten Arbeitstag hin deaktiviert das USZ alle Benutzerkonten der austretenden Mitarbeitenden. Diese haben alle USZ-Informatikmittel dem USZ zurück zu geben. Mails, die nach der Deaktivierung an E-Mail-Adressen gesendet werden, werden ohne Weiterleitung abgewiesen (Zustellfehlerbericht).
- Das USZ ist berechtigt, nach Beendigung des Anstellungsverhältnisses sämtliche Daten auf den persönlichen Laufwerken sowie E-Mail-Konten zu löschen. Besteht die Vermutung, dass sich Geschäftsdokumente darauf befinden, wird der oder die ehemalige (oder abwesende) Mitarbeitende aufgefordert, die Geschäftsdokumente auf Geschäftsverzeichnisse zu überführen. Ist dies

technisch nicht möglich oder verweigert er oder sie die Mitwirkung oder ist er oder sie unerreichbar, ist die ICT berechtigt nach Rücksprache mit dem Rechtsdienst, auf die persönlichen Verzeichnisse und E-Mail-Konten zuzugreifen, um die Geschäftsdokumente zu übertragen.

10. Kontrolle der Internet- und E-Mail-Dienste und Vorgehen bei Missbrauch

- 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.
- Wird im Rahmen dieser anonymen Kontrollen eine Verletzung der vorliegenden Nutzungsregelung festgestellt, informiert die Direktion ICT den Chief Information Security Officer. Sollten weitere Abklärungen nötig sein, bezieht dieser den Corporate Compliance Officer ein.
- 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, können nach vorgängiger Abmahnung durch die Spitaldirektion die Internet-Zugriffe oder der E-Mail-Verkehr fortan personenbezogen protokolliert und ausgewertet werden. Der Überwachungszeitraum darf drei Monate nicht übersteigen. Eine permanente Überwachung ist unzulässig.

11. Schlussbestimmung

Anträge für Ausnahmeregelungen von dieser Weisung müssen durch den Chief Information Security Officer bewilligt werden.

Wird eine Verletzung dieser Nutzungsregelung bzw. eine missbräuchliche oder gesetzeswidrige Nutzung der Informatikmittel festgestellt, können Sanktionen bis hin zu personalrechtlichen Konsequenzen angeordnet werden.

Diese Weisung tritt mit Genehmigung durch die Spitaldirektion in Kraft.