USZ Universitäts Spital Zürich		Direktion Betrieb	
Dokumentenart	Weisung	Version	28.01.2016
Erlassen durch	BTR	Gültig ab	15.02.2016
Geltungsbereich	USZ	Ersetzt	--
Erstellt durch	KUN	Kurztitel	WE_Datenbearbeitung betreffend elektronische Zutrittssysteme

Weisung
bezüglich Bearbeitung von Daten betreffend elektronische Zutrittssysteme

1. Zweck

Die vorliegende Weisung bezweckt die Sicherstellung einer datenschutzkonformen Bearbeitung von Daten betreffend elektronische Zutrittssysteme.

2. Geltungsbereich

Diese Weisung gilt für das USZ.

3. Definitionen

ABC	Atomar (radioaktiv), biologisch, chemisch
Kompetenzträger	Personen, die Anträge auf Zugang zu geschützten Räumen und Fächern bewilligen. Diese werden von den entsprechenden Organisationseinheiten (Direktionen, Medizinbereiche, Kliniken) ernannt.
KUN	Kundendienst
LCO	Legal Compliance Officer
Sichtausweis	Sichtausweis mit integriertem Chip, auf dem Zutrittsberechtigungen gespeichert werden können
SICUM	Sicherheit und Umwelt
SIDI	Sicherheitsdienst

4. Elektronische Zutrittssysteme im USZ

4.1. Zielsetzung

Der Zutritt zu vielen Räumen im USZ ist nur noch mit einem persönlichen und autorisierten Sichtausweis möglich aus den folgenden Gründen:

a. Zertifizierungsvorgaben lassen sich nur mittels elektronischer Zutrittskontrolle einhalten;

b. Sicherheit, beispielsweise überwachte Zutritte im Zusammenhang mit ABC-Stoffen, Strahlungen, etc.;

c. Die Entnahmen aus Betäubungsmittel- und Medikamentenschränken unterliegen strengen Vorschriften;

d. Patienten- und Personaldaten sind vertraulich und dürfen nur berechtigten Personen zugänglich sein;

e. Präventive Verhinderung von strafbaren Handlungen;

f. Organisatorische und strukturelle Veränderungen erfordern eine rasche und flexible Anpassung der Zutrittsberechtigungen. Elektronische Zutrittssysteme erfüllen diese Anforderungen deutlich besser als mechanische Schliessungen.

4.2. Antrag, Freigabe und Verwaltung der Zutrittsberechtigungen

Jeder Mitarbeitende, welcher eine Zutrittsberechtigung braucht, um seine Tätigkeit ordnungsgemäss ausüben zu können, muss diese mittels Formular „Ausweise und Schlüssel“ beim KUN beantragen.

Der KUN prüft die Anträge und gibt diese auf den Sichtausweisen der Mitarbeitenden frei oder lehnt sie unter Angabe einer Begründung ab.

Bei besonders schützenswerten Objekten (z.B. Labore, Direktionsbüros, etc.) ist das Formular durch den Kompetenzträger mit zu unterzeichnen. KUN führt eine Liste der Kompetenzträger und hält diese stets auf dem aktuellsten Stand.

KUN verfügt sodann über eine Liste, die alle sichtausweisgesicherten Objekte aufführt. Diese wird regelmässig aktualisiert und durch die Leitung SICUM/SIDI herausgegeben.

KUN obliegt die Verwaltung der Zutrittsberechtigungen In diesem Rahmen kann KUN begrenzte personenbezogene Auswertungen durchführen.

4.3. Erfassung, Aufbewahrung und Löschung von Zutrittsdaten

Die elektronischen Zutrittssysteme im USZ sind an eine Datenbank gekoppelt, welche Personendaten erfasst.

Folgende Daten werden erfasst:

a. Sichtausweis-Nummer, welche eine Identifikation des Mitarbeitenden ermöglicht;

b. Name und Vorname;

c. Personalnummer;

d. Datum und Uhrzeit des Ein- und/oder Austritts bzw. Öffnung und Schliessung einer Tür oder beispielsweise eines Faches in einem Giftschrank.

Diese Daten werden während neunzig (90) Tagen aufbewahrt und automatisch nach Ablauf dieser Zeitdauer auf dem Server gelöscht. Vorbehalten bleibt Ziffer 4.5., Absatz 4.

4.4. Rechte betroffener Personen

Betroffenen Personen steht gemäss § 20 IDG ein Auskunftsrecht zu. Auf schriftliches Auskunftsbegehren an das Generalsekretariat SDI, Legal Compliance Office, prüft der LCO das Gesuch, welches aus Praktikabilitätsgründen Ort und Zeit des Zutritts zu enthalten hat, und entscheidet über die Freigabe von Informationen im Zusammenhang mit Zutrittsdaten.

4.5. Auswertung von Zutrittsdaten

Wenn ein zivil- oder strafrechtlich relevantes Ereignis festgestellt wurde kann die Leitung SICUM/SIDI Zutrittsdaten personenbezogen auswerten.

Liegt ein konkreter Verdacht einer strafbaren Handlung vor, entscheiden die Leitung SICUM/SIDI und der LCO über das weitere Vorgehen.

Die Auswertung hat zeitnah nach Feststellen des Ereignisses durch ein Mitglied der Leitung SICUM/SIDI nach Möglichkeit zusammen mit einer Zweitperson im Sinne des Vieraugenprinzips zu erfolgen.

Über jeden Zugriff auf Zutrittsdaten erstattet die Leitung SICUM innert drei (3) Arbeitstagen nach der Einsicht Bericht zuhanden des LCO‘s. Der schriftliche Bericht enthält die Namen der Personen, welche Einsicht nehmen, den konkreten Anlass für die Einsichtnahme, die Angabe des Zutrittskontrollobjektes, den Zeitraum des ausgewerteten Datenmaterials, die Sachverhaltsfeststellung sowie eingeleitete oder empfohlene Massnahmen.

Der LCO legt zusammen mit dem Leiter SICUM fest, ob und wie lange die Zutrittsdaten über die Frist gemäss Ziffer 4.3. gespeichert bleiben. Die Dauer hat so kurz wie möglich zu sein.

Anonyme Auswertungen der Zutrittsdaten, z.B. im Rahmen von Planungen von Neu- und Umbauten zur Berechnung von Nutzungsfrequenzen, sind ohne vorgängige Information jederzeit möglich.

4.6. Bekanntgabe von Zutrittsdaten

Auf schriftlich begründetes Gesuch oder auf Verfügung von zuständigen Behörden werden Zutrittsdaten bekannt gegeben, soweit diese für straf-, verwaltungs- oder zivilrechtliche Verfahren erforderlich sind. Die Leitung SICUM prüft die Anfrage und entscheidet über die Bekanntgabe von Zutrittsdaten. Sie kann jederzeit den Rechtsdienst oder den LCO in den Entscheidungsfindungsprozess involvieren. Das Amtsgeheimnis ist in jedem Fall zu wahren.

Die Leitung SICUM kann bei Feststellung oder Meldung eines zivil- oder strafrechtlich relevanten Ereignisses aus Eigeninitiative Zutrittsdaten an Strafverfolgungsbehörden und Gerichte bekanntgeben, soweit die Umstände es erfordern. Das Amtsgeheimnis ist in jedem Fall zu wahren.

Die Leitung SICUM erstattet dem LCO mindestens einmal jährlich zusammenfassend Bericht über die Bekanntgabe von Zutrittsdaten.

4.7. Datensicherheit

Die Übermittlung der Zutrittsdaten an den Server erfolgt verschlüsselt.

Der Server befindet sich in einem geschlossenen Raum, zu welchem nur berechtigte Personen mit elektronischem Sichtausweis Zutritt haben. Zum Kreis der berechtigten Personen gehören ausschliesslich Mitarbeitende der ICT gemäss USZ-Schliesskonzept. Die Daten auf dem Server sind nur mittels Autorisation (Benutzername/Passwort) verfügbar.

Die Berichte gemäss Ziffer 4.5., Absatz 3, sind sechs (6) Monate beim SICUM aufzubewahren. Der Zugriff auf Berichte bleibt dem LCO und dem Leiter oder stellvertretenden Leiter SICUM vorbehalten.

5. Schlussbestimmungen

Diese Weisung tritt per 15. Februar 2016 in Kraft.