Rahmendienstvereinbarung

über den Einsatz von Informations- und Kommunikationstechnologien der Uniklinik Köln

Anlage 1 – Sicherheitsrichtlinie für Benutzer

§ 1

Bei Nutzung von IKT-Systemen sind geltende Gesetze und interne Regelungen einzuhalten. Interne Regelungen, Richtlinien und Sicherheitshinweise werden im Intranet veröffentlicht.
Alle Beschäftigten sind verpflichtet an angebotenen Schulungen zu Sicherheitsmaßnahmen vor der Nutzung von IKT-Systemen teilzunehmen.

§ 2

Die Nutzung der IT-Systeme und IT-Dienste ist grundsätzlich nur zu dienstlichen Zwecken zur Erledigung der zugewiesenen Aufgaben gestattet. Ausnahmen hierzu sind ggf. in den jeweiligen Nutzungsbedingungen geregelt.

§ 3

Bei den zentral durch die uk-it administrierten PCs wird die Software durch ein Softwareverteilsystem automatisch freigegeben und/oder installiert. Die Benutzung privater Hard- und Software zu dienstlichen Zwecken ist ohne Genehmigung durch die uk-it nicht zulässig.

§ 4

(1) An jedem PC ist der Bildschirmschoner so eingestellt und zu belassen, dass er beim Verlassen des Arbeitsplatzes manuell eingeschaltet werden kann oder nach einer Wartezeit von 15 Minuten automatisch aktiviert wird. Der Bildschirmschoner ist überdies mit einem Kennwortschutz zu versehen. In Bereichen mit Publikumsverkehr sind Monitore, Drucker und Faxgeräte so aufzustellen, dass das Risiko der Einsichtnahme Dritter möglichst ausgeschlossen wird.

(2) Beim Verlassen der Räume sind die Türen immer zu verschließen, soweit aus sicherheitstechnischen Gründen (z.B. Fluchtwege) hiervon nicht abgewichen werden muss. Das gilt auch bei vorübergehender Abwesenheit.

(3) Die Weitergabe der persönlichen Nutzerkennung sowie des dazugehörigen Kennwortes ist untersagt.

(4) Wenn der Verdacht besteht, dass die eigenen Zugangs- und Zugriffsberechtigungen unberechtigt durch Dritte genutzt werden oder genutzt worden sind, ist das Passwort umgehend zu ändern und die/der IT-Sicherheitsbeauftragte zu informieren.

§ 5

(1) Folgende Passwortregeln sind zu beachten:

1. Passwörter sind für Dritte unzugänglich aufzubewahren.
2. Passwörter dürfen nur dem Benutzer bekannt sein.
3. Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Das Passwort ist alphanumerisch (Buchstaben und Zahlen/Zeichen mit Sonderzeichen) zu gestalten.
4. Passwörter dürfen nicht leicht zu erraten sein. Vor- und Familiennamen oder Geburtstage sind beispielsweise nicht zur Bildung von Passwörtern geeignet. Es dürfen niemals Trivialpasswörter verwendet werden (z. B. 4711; 12345 oder andere nebeneinander liegende Tasten).
5. Die Passwörter sind spätestens alle 90 Tage zu wechseln.
6. Sofern Gruppenpasswörter zwingend erforderlich sind, gilt: Gruppenpasswörter sind umgehend zu ändern, wenn die Zusammensetzung der Gruppe sich verändert. Gleiches gilt, wenn Passwörter unautorisierten Personen bekannt geworden sind. Ausgenommen hiervon sind lediglich Gruppenaccounts, die ausschließlich Zugang zu einem Gerät ohne Zugriff auf kritische Daten ermöglichen. (z.B. Stations-PC im Mehrschichtbetrieb ohne Administratorrechte und zusätzlicher personenbezogener Authentifizierung zu den Applikationen (Klinisches Arbeitsplatzsystem (KAS), SAP, Email, etc.)). Gruppenpasswörter sind ebenfalls für Dritte unzugänglich aufzubewahren.
7. Einmal genutzte Passwörter sind nicht wieder zu verwenden.
8. Der Empfang des Initialpasswortes ist zu bestätigen. Das Initialpasswort ist jeweils sofort zu ändern.
9. Passwörter dürfen nicht als Teil eines automatischen, nicht passwortgeschützten Anmeldeprozesses verwendet werden.

(2) Für einzelne IT-Systeme können erweiterte Passwort-Regeln festgelegt werden.

§ 6

(1) Bei der Nutzung von Internet und E-Mail sind Virenschutzprogramme zu nutzen. Die zentral von der uk-it zur Verfügung gestellten Internet- und E-Mail-Dienste sowie PCs und Windows-Server sind mit einem Virenschutz ausgestattet.

(2) Vom Administrator voreingestellte Sicherheits-Konfigurationen dürfen nicht vom IT-Benutzer deaktiviert oder geändert werden.

(3) Beim Datenaustausch ist zu beachten:

1. Da zur Zeit kein Verschlüsselungsdienst zur Verfügung gestellt wird, ist der Versand von vertraulichen Informationen, wie z.B. Patientendaten, nicht zulässig.
2. Beim Faxversand von vertraulichen Informationen ist ein Sendezeitpunkt mit der Gegenseite abzustimmen. Hierbei ist möglichst Kurzwahl zu nutzen.
3. Ausdrucke mit vertraulichen Informationen sind umgehend aus dem Drucker zu entfernen.

§ 7

1. Die Datenverarbeitung von patientenbezogenen und patientenbeziehbaren Daten ist nur auf den dafür vorgesehen IT-Systemen zulässig.

2. Die Speicherung von patientenbezogenen und patientenbeziehbaren Daten auf lokalen Festplatten ist nicht erlaubt.

§ 9

1. Bei Sicherheitsvorfällen ist umgehend der IT-Servicedesk der uk-it unter Telefonnummer (-7555) zu benachrichtigen.

Sicherheitsvorfälle können z.B. sein:

- Versenden von SPAM-Mails
- ungewöhnliches Verhalten eines IT-Systems, das eine Virusinfektion vermuten lässt
- Unautorisierter Zugang zu einem IT-System bzw. dessen unautorisierte Nutzung
- Offenlegung oder Diebstahl von geschützten Informationen, Passwörten, etc.

Bei Sicherheitsvorfällen, bei denen personen- oder patientenbezogene Daten betroffen sind, ist der zuständige Datenschutzbeauftragte einzuschalten.