bethesda
SPITAL

THE SWISS LEADING HOSPITALS
Best in class.

Bethesda Spital AG
Gellertstrasse 144
Postfach 2372
4002 Basel
Tel. +41 61 315 21 21
Fax +41 61 312 13 42
www.bethesda-spital.ch

ICT
Joachim Suter
Tel. +41 61 315 21 46
joachim.suter@bethesda-spital.ch

Reglement der ICT-Nutzung

Dokument Nr.:		Erstelldatum:	30.03.2015
Ersteller:	J. Suter	Funktion:	Leiter ICT
Datum Freigabe:	01.05.2015	Funktion Freigabe:	ICTK

Inhaltsverzeichnis

1. Allgemeines ... 4
1.1 Ziele ... 4
1.2 Geltungsbereich ... 4
1.3 Verantwortungsbereich ... 4

2. Die 9 goldenen Informatik-Sicherheitsregeln ... 4

3. Zugangskonto ... 4
3.1 Passwörter ... 5
3.2 Bildschirmsperre ... 6
3.3 Austritt ... 6

4. Hardware ... 6
4.1 Standard Informatikmittel ... 6
4.2 Smartphones und Tablets ... 6
4.3 Entsorgung alter Hardware ... 6

5. Software ... 6
5.1 Beschaffungen, Installationen und Veränderungen ... 6

6. Bethesda Netzwerk ... 7
6.1 Allgemeine Verbindungen ... 7
6.2 Mobile Verbindungen ... 7

7. Internet ... 7
7.1 Fluch und Segen ... 7
7.2 Nutzung ... 7
7.3 Sicherheitseinstellungen ... 8
7.4 Gesperrte Websites ... 8
7.5 Verhalten ... 8

8. E-Mail ... 8
8.1 Nutzung ... 8
8.2 Geschäftliche E-Mail-Adresse ... 8
8.3 Aufräumen Ihres Postfachs ... 8
8.4 Archivierung ... 9
8.5 Verdächtige E-Mails ... 9
8.6 Vertrauliche und geheime E-Mails ... 9
8.7 E-Mail- und Postfachgrösse ... 9
8.8 Zugriff auf Outlookpostfach ... 9

9. Dateiablage ... 9

9.1 Speicherung von geschäftlichen Daten 9
9.2 Ablagestruktur 10
9.2.1 Home (H:) 10
9.2.2 Public Spital (P:) 10
9.2.3 Transfer (T:) 10
9.3 Austritt Mitarbeitende 10

10. Cloud-Dienste 10

11. ICT-Servicedesk 11
11.1 Pikett 11
11.2 Private Anfragen 11

12. Wartungsfenster 11

13. Inkrafttreten 12

1. Allgemeines

Diese Weisung regelt die Benutzung der ICT-Ressourcen am Bethesda Spital durch berechtigte Benutzerinnen und Benutzer. Diese Weisung ist Teil des Frameworks „Informationssicherheit im Bethesda Spital".

1.1 Ziele

Die vorliegende Weisung dient der Gewährleistung der Informatiksicherheit, des Datenschutzes und der Förderung des verantwortungsbewussten Umganges mit Informatikeinrichtungen (Vertraulichkeit, Verfügbarkeit, Datenintegrität).

1.2 Geltungsbereich

Diese Weisung gilt für alle Mitarbeiterinnen und Mitarbeiter des Bethesda Spitals, einschliesslich Aushilfs- und Temporärpersonal. Sie umfasst alle für Spitalzwecke eingesetzten Informatikmittel. Die Linie kann für einzelne Bereiche ergänzende Regelungen treffen.

1.3 Verantwortungsbereich

Für die Einhaltung dieser Weisung sind die Departemente resp. Abteilungen zuständig.

2. Die 9 goldenen Informatik-Sicherheitsregeln

1. Ich schütze meine Arbeitsstation vor unberechtigtem Zugriff auf Daten.
2. Ich sperre beim Verlassen des Arbeitsplatzes die Arbeitsstation (Ctrl+Alt+Del).
3. Ich gebe meine Passwörter nicht weiter, sie sind persönlich.
4. Ich gehe vorsichtig mit dem Versenden und Empfangen von E-Mails um.
5. Ich beschaffe, installiere oder verändere niemals Hard- / Software ohne Genehmigung.
6. Ich lade und installiere keine Software aus dem Internet auf die Arbeitsstation.
7. Ich konsumiere und speichere keine Daten mit widerrechtlichem, beleidigendem oder herabwürdigendem Inhalt.
8. Ich melde Störungen und Sicherheitsrisiken unverzüglich den ICT-Servicdesk.
9. Ich lasse nicht mehr benötigte Datenträger (CD, USB-Stick, etc.) physisch zerstören.

3. Zugangskonto

Das ICT Zugangskonto (Account) wird durch die ICT-Abteilung anhand von „Funktions-Rollen" passend zur Anstellung erstellt und beim Eintritt dem Mitarbeitenden durch das HR übergeben.

Funktionsrollen definieren eine Funktion einer Anstellung und leiten sich aus der Funktion im führenden Personalsystem ab. Die Definition der einzelnen Rolle erfolgt in Abstimmung mit den Abteilungsleitern.

Individuelle und zusätzliche Zugriffe sind durch den Vorgesetzten schriftlich an den ICT-Servicedesk zu melden.

Das Zugangskonto ist persönlich und nicht übertragbar. Die auf das Zugangskonto eingetragene Person ist für dessen Geheimhaltung unter Beachtung aller zumutbaren Vorsichtsmassnahmen verantwortlich. Besteht die Vermutung, dass ein Zugangskonto von Unbefugten benutzt wird, muss dies umgehend dem Servicedesk des Bethesda Spitals gemeldet werden.

3.1 Passwörter

Ein Passwort muss mindestens 8-stellig sein und drei der folgenden Kriterien erfüllen:

- ein Kleinbuchstabe
- ein Grossbuchstabe
- eine Zahl
- ein Sonderzeichen wie zum Beispiel +*&_?!

Ein gutes Passwort ist zum Beispiel: ZnDsu$67

- Das Hauptpasswort zum Netzwerk muss quartalsweise geändert werden.
- Das Passwort muss je nach Applikation periodisch geändert werden.

Gehen Sie sorgfältig mit Login und Passwörter um. Das Unsachgemässe aufbewahren von Passwörtern wie beispielsweise das Ankleben am Bildschirm oder ein Zettel unter der Tastatur sind unsachgemäss und nicht erlaubt.

Passwörter, sind persönlich und vertraulich, sie dürfen niemandem ausgehändigt oder bekannt gemacht werden. Bei Verlust der Berechtigungsmittel ist unverzüglich der ICT-Servicedesk zu benachrichtigen.

Falls der Verdacht besteht, dass das Passwort Dritten bekannt ist (zum Beispiel, wenn eine Person die Passworteingabe beobachtet hat), muss das Passwort unverzüglich geändert werden. Bei Applikationen ist der Zugang durch die applikationsverantwortliche Person unverzüglich zu deaktivieren.

Wird ein Passwort innerhalb 15 Minuten 5-mal falsch eingegeben wird das Zugangskonto für 15 Minuten gesperrt. Das Zugangskonto schaltet sich nach dieser Zeit wieder frei.

3.2 Bildschirmsperre

Alle Computer und Daten sind vor unberechtigtem Zugriff zu schützen. Beim Verlassen des Arbeitsplatzes sind der Desktop oder das Notebook zu sperren. Das System sperrt notfalls nach 15 Minuten Inaktivität den Bildschirm automatisch.

3.3 Austritt

Nach Austritt eines Mitarbeiters werden die Zugänge umgehend gesperrt. Das Mail wird deaktiviert und generiert eine entsprechende Meldung. Nach 3 Monaten wird das gesamte Zugangskonto aufgelöst (Account, Laufwerk H:, Mailbox).

4. Hardware

4.1 Standard Informatikmittel

Die Beschaffung darf nur in Absprache mit der ICT erfolgen. Die ICT stellt einen Standard Produktekatalog von kompatiblen und getesteten Informatikmitteln die bestellt und eingesetzt werden dürfen bereit.

Änderungen an der Hardware sind nicht gestattet. Dies gilt für alle Aus- und Umbauten der Geräte sowie für den Anschluss zusätzlicher Geräte. Bei einem Arbeitsplatzwechsel dürfen Geräte nur in Absprache mit der Linie und der ICT verschoben werden.

4.2 Smartphones und Tablets

Für Smartphones und Tablets bestehen gesonderte Regelungen. Geräte die als „Agenda“ verwendet werden (Mail, Kalender, Kontakte) werden durch die Mitarbeitenden gestellt und unter Einhaltung der Bethesda Sicherheitsrichtlinien eingebunden („BYOD“).

Geräte die durch das Bethesda Spital für spezielle Anwendungsfälle gestellt werden und nicht „BYOD“ unterliegen gilt ebenfalls Kapitel Standard Informatikmittel.

4.3 Entsorgung alter Hardware

Nicht mehr benötigte Hardware und vor allem Datenträger sind der ICT zur fachgerechten Zerstörung und Entsorgung zu retournieren.

5. Software

5.1 Beschaffungen, Installationen und Veränderungen

Die Beschaffung darf nur in Absprache mit der Linie und der Leitung ICT erfolgen.

Die Installation und Konfiguration von Software (Eigentum des Bethesda Spital) darf nur von der ICT vorgenommen werden.

Die Aktualisierung des Betriebssystems und der Antivirussoftware wird ausschliesslich durch die ICT vorgenommen. Alle Sicherheitseinstellungen werden ausschliesslich von der ICT verwaltet

Die Installation von privater Software ist verboten.

6. Bethesda Netzwerk

6.1 Allgemeine Verbindungen

Es ist aus Sicherheitsgründen nicht erlaubt betriebsfremde Geräte an das Bethesda Netzwerk anzustecken (z.B. per Netzwerkkabel). Für Fremdgeräte steht im ganzen Bethesda ein Public WLAN zur Verfügung, dass genutzt werden darf.

Der gleichzeitige Anschluss an das interne Netzwerk des Bethesda und an ein externes Netz (zum Beispiel Public-WLAN) ist aus Sicherheitsgründen (unkontrollierbarer und ungesicherter Netzwerkübergang) untersagt.

6.2 Mobile Verbindungen

Unterbrechen Sie unterwegs jeweils die WLAN-Verbindung, wenn sie nicht benötigt wird. So sind Sie nicht nur sicherer vor Datenmissbrauch, sondern reduzieren auch die Verbindungskosten und erhöhen die Akkulaufzeit ihres mobilen Gerätes.

Es wird empfohlen die unsicheren Bluetooth und Infrarotverbindungen grundsätzlich zu deaktivieren.

7. Internet

7.1 Fluch und Segen

Das Internet eröffnet uns den Zugang zu einer unerschöpflichen Vielfalt an Informationen und Dienstleistungen, die wir am Arbeitsplatz nutzen können. Das Surfen im Internet birgt aber auch Gefahren wie das Verteilen von Malware (Viren, Trojaner usw.), Hackerangriffe, Ablesen von E-Mails oder Spionage. Nutzen Sie das Internet deshalb mit Vorsicht und Verantwortungsbewusstsein.

7.2 Nutzung

Das Internet ist für dienstliche Zwecke in Erfüllung der übertragenen Aufgaben zu verwenden. Es gelten die Bestimmungen des Personalreglements und des Betriebsreglement über Informationssicherheit und Datenschutz in der Informatik.

7.3 Sicherheitseinstellungen

Die Sicherheitseinstellungen des Internetbrowsers (Internet Explorer) sind standardisiert und können von den Benutzern nicht verändert werden.

7.4 Gesperrte Websites

Aus Gründen der Sicherheit und der Verfügbarkeit ist der Zugriff auf unsichere Websites verboten und gesperrt. Sollten Sie dennoch eine gesperrte Website für den dienstlichen Gebrauch benötigen, beantragen Sie den Zugriff beim ICT-Servicedesk.

7.5 Verhalten

Achten Sie auf Sicherheits-Meldungen und verlassen Sie bei Unsicherheiten umgehend die Website.

Aus Sicherheitsgründen ist das Herunterladen (Download) von Dateien, welche die Sicherheit Ihres Gerätes gefährden, gesperrt. Denn oftmals wird mit einem scheinbar seriösen Angebot auch eine Schadsoftware (Malware) mitgeliefert und auf Ihrem Gerät installiert. Im schlimmsten Fall können Informationen an Unberechtigte gelangen. Falls Schadsoftware (Malware) auf Ihren Desktop-PC oder Ihr Notebook gelangt, ist der ICT-Servicedesk zwingend zu informieren.

Durch das Herunterladen von grösseren Datenmengen wie Internet-TV und -Radio sowie Videos beeinträchtigen Sie die Verfügbarkeit des Bethesda Datennetzwerkes. Es können längere Wartezeiten bei Applikationen, E-Mail- und Drucker-Diensten entstehen. Vermeiden Sie Datenverkehr der nicht zwingend für die Erfüllung Ihrer Aufgabe notwendig ist.

8. E-Mail

8.1 Nutzung

Das E-Mail ist für dienstliche Zwecke in Erfüllung der übertragenen Aufgaben zu verwenden. Es gelten die Bestimmungen des Personalreglements und des Betriebsreglement über Informationssicherheit und Datenschutz in der Informatik.

8.2 Geschäftliche E-Mail-Adresse

Geben Sie Ihre E-Mail-Adresse nur gezielt weiter. Die geschäftliche E-Mail-Adresse darf nicht für private Zwecke (Wettbewerbe, Bestellungen, private Newsletter, soziale Netzwerke usw.) benutzt werden.

8.3 Aufräumen Ihres Postfachs

Räumen Sie Ihr Postfach regelmässig auf. Löschen Sie nicht mehr benötigte E-Mails.
Löschen Sie im Outlook-Ordner "Gelöschte Objekte" die E-Mails endgültig.

8.4 Archivierung

Geschäftsrelevante E-Mails müssen archiviert werden.

8.5 Verdächtige E-Mails

Öffnen Sie keine E-Mails von unbekannten Absendern, da diese Malware enthalten können. Verdächtige Anhänge und/oder unbekannte Links dürfen niemals geöffnet werden. Diese E-Mails sind umgehend und endgültig (auch zwingend im Outlook-Ordner "Gelöschte Objekte") zu löschen.

8.6 Vertrauliche und geheime E-Mails

Falls ein Geschäftsprozess die Verschlüsselung von E-Mails verlangt, muss dazu das Verfahren "HIN" angewendet werden. Vertrauliche und/oder geheime Informationen (insbesondere Patientendaten) dürfen niemals unverschlüsselt übermittelt werden.

8.7 E-Mail- und Postfachgrösse

Die maximale E-Mail Grösse von und an externe Empfänger beträgt 20 MB. Grössere Dateien müssen über den Dienst Docsafe abgewickelt werden. Die ICT hilft hier weiter.

Die Postfachgrösse ist auf 200 MB beschränkt. Sie werden über ein volles Postfach informiert. Ist das Postfach voll, können keine weiteren Mails versendet werden. Der Empfang bleibt sichergestellt.

Grössere Postfächer sind durch den Abteilungsleiter am ICT-Servicedesk begründet zu beantragen.

8.8 Zugriff auf Outlookpostfach

Nur das entsprechende Zugangskonto hat Zugriff auf das persönliche Postfach.

Der Domänen-Administrator kann auf das Postfach zugreifen. Dieser macht dies aber immer nur mit Einwilligung und Auftrag des jeweiligen Mitarbeitenden. Zugriffe können nicht durch direkte Vorgesetzte angeordnet werden (z.B. aufgrund von Krankheit). In begründeten, ausserordentlichen Notfällen kann der Direktor den Zugriff anordnen.

9. Dateiablage

9.1 Speicherung von geschäftlichen Daten

Um die Verfügbarkeit geschäftlicher Daten sicherzustellen, dürfen diese nie auf einem lokalen oder externen Laufwerk, sondern müssen auf den entsprechenden Netzlaufwerken (Home (H:), Public Spital (P:), Transfer (T:)) sowie in den Fachapplikationen gespeichert werden.

Diese Daten werden in regelmässigen Abständen mittels „Backup“ gesichert und können im Bedarfsfall durch die ICT wieder hergestellt werden. Die Aufbewahrungsfrist variiert je nach Datenklasse.

Es ist nicht gestattet Kopien von geschäftlichen Daten auf externen Speichermedien anzulegen. Sämtliche Bethesda Geschäftes-Daten verbleiben zu jederzeit im Rechenzentrum.

9.2 Ablagestruktur

9.2.1 Home (H:)

Das Laufwerk Home ist ein persönliches Laufwerk des Mitarbeitenden. Nur der Benutzer des dazugehörigen Zugangskontos hat Zugriff auf diese Daten.
Verwenden Sie dieses Laufwerk für Ihre persönlichen, geschäftsrelevanten Daten (z.B. Kopie ihres MAG). Weiter werden auf H: ihre persönlichen Einstellungen wie der Desktop oder ihre Favoriten gespeichert.

Der Domänen-Administrator kann auf das Laufwerk zugreifen. Dieser macht dies aber immer nur mit Einwilligung und Auftrag des jeweiligen Mitarbeitenden. Zugriffe können nicht durch direkte Vorgesetzte angeordnet werden (z.B. aufgrund von Krankheit). In begründeten, ausserordentlichen Notfällen kann der Direktor den Zugriff anordnen.

9.2.2 Public Spital (P:)

Das Laufwerk Public Spital ist für sämtliche geschäftlichen Daten die im Spital verwendet werden. Die Ordnerstruktur ist Abteilungsbezogen, kann aber für Kommissionen oder Projekte auch interdisziplinär sein. Die entsprechenden Zugriffe werden mit sogenannten „Gruppen“ gesteuert. Der Abteilungsleiter, Kommissionsvorsitzende oder Projektleiter definiert die notwendigen Zugriffe.

9.2.3 Transfer (T:)

Das Laufwerk Transfer ist für die Zusammenarbeit mit der Stiftung geschaffen worden. Ferner liegen hier auch temporäre Daten für den Austausch oder öffentlich zugängliches Material, dass innerhalb der Bethesda Gruppe benötigt wird.

9.3 Austritt Mitarbeitende

Vor dem Austritt speichert der Mitarbeitende alle geschäftlichen Daten, die ggf. noch auf dem „Home“ liegen, in den von der vorgesetzten Stelle bestimmten Speicherort. Das Laufwerk Home wird drei Monate nach einem Austritt gelöscht.

10. Cloud-Dienste

Es ist aus Sicherheitsgründen verboten, interne, vertrauliche oder geheime Daten in Cloud-Diensten (z.B. Dropbox, Google Drive usw.) zu speichern. In Cloud-Diensten gespeicherte

Daten können jederzeit und überall, ohne Kenntnis oder Erlaubnis des Dateninhabers gelesen, verändert oder gelöscht werden.

11. ICT-Servicedesk

Das Bethesda Spital verfügt über einen ICT-Servicedesk der Ihnen bei Fragen rund um die ICT zur Verfügung steht.

- Störungen
- Anfragen
- Bestellungen

Der ICT-Servicedesk steht wie folgt zur Verfügung:
Montag bis Freitag 07:30 Uhr bis 17:00 Uhr

Für die Kommunikation mit dem ICT-Servicedesk verwenden Sie wenn immer Möglich IBI-helpMe („Rettungsring“) oder die Emailadresse servicdesk@bethesda-spital.ch.

Für ganz dringende Anliegen wenden Sie sich an Telefon intern 2345.

11.1 Pikett

Ausserhalb dieser Betriebszeiten steht für Notfälle ein Pikettdienst bereit. Notfälle sind Störungen die den Betrieb wesentlich einschränken. Der Pikettdienst wird durch den Empfang aufgeboten.

11.2 Private Anfragen

Der ICT Servicedesk steht für private Anfragen oder Dienstleistungen nicht zur Verfügung.

12. Wartungsfenster

Die Infrastruktur und Verfügbarkeit ist auf 7 x 24 Stunden ausgelegt. Jedoch unterliegen verschiedene Systeme regelmässigen Updates, Erweiterungen oder einem kontrollierten Neustart. Die ICT ist bemüht dies möglichst ausserhalb der Betriebszeiten durchzuführen.

Folgende Unterbrüche sind heute berücksichtigt:

Neustart Citrix-Server	Sie werden aufgefordert sich neu an Citrix anzumelden.	Täglich 01:00 – 03:00 Uhr
Neustart App-Server	Neustart definierter Applikations-Server:	Jeweils Sonntag 01:00 -03:00 Uhr
Wartungsabend ICT	Offizieller Wartungsabend. Es kann zu Unterbrüchen kommen. Kritische Unterbrüche werden vorab angekündigt	Jeweils letzter Mittwoch im Monat ab 18:00 Uhr.

13. Inkrafttreten

Dieses Betriebsreglement über ICT-Nutzung tritt per 1. Mai 2015 in Kraft.

Vom Direktor genehmigt am 01.05.2015