LINDENHOFGRUPPE

Weisung für den sicheren Umgang mit Informations- und Kommunikations-mittel

1 Zweck und Geltungsbereich

Die vorliegende Weisung bezweckt die Förderung der Informatiksicherheit, die Gewährleistung des Datenschutzes und den verantwortungsbewussten Umgang mit Informatikmitteln.

Diese Weisung ist verbindlich für alle Personen, welche Informatikmittel der Lindenhofgruppe nutzen (nachfolgend «Benutzer»).

Informatikmittel im Sinne dieser Weisung sind Hardware (Computer, Tablets, Smartphones, Datenträger usw.), Software (Applikation, Anwendungsprogramme) Netzwerke und Dienste.

2 Persönliche Verantwortung

Alle Benutzer, die Zugang zu Informationen über Patienten, Mitarbeitende oder Geschäftsdaten haben, sind persönlich dafür verantwortlich, dass der Datenschutz beachtet und die Informationen sorgfältig bearbeitet werden (vgl. dazu die Merkblätter der Lindenhofgruppe zum Datenschutz).

3 Vorsichtsmassnahmen am Arbeitsplatz

Computer, Tablets, Smartphones und Datenträger sind vor unberechtigtem Zugriff zu schützen. Beim Verlassen des Arbeitsplatzes sind der Desktop und das Notebook mit Passwort zu sperren, Büroräume sind abzuschliessen. Patientendossiers, Mitarbeiterdossiers sowie vertrauliche/geheime Dokumente sind, wenn möglich, einzuschliessen. Vorbehalten bleiben anderslautende Anweisungen von Vorgesetzten.

Unterlagen mit Patienten- oder Mitarbeiterdaten sowie vertrauliche/geheime Dokumente sind umgehend aus Druckern oder Faxgeräten zu entfernen.

Die Mitarbeitenden achten darauf, dass sich keine unbefugten Personen in Räumen aufhalten, die nicht allgemein zugänglich sind. Wenn solche Personen angetroffen werden, werden diese aufgefordert den Raum unverzüglich zu verlassen. Sofern erforderlich, wird der technische Dienst informiert.

4 Umgang mit Software

Änderungen an den Systemeinstellungen (Installation, Deinstallation, Änderung der Konfiguration usw.) dürfen nur von den dazu berechtigten Administratoren vorgenommen werden. Es ist verboten,

Sicherheitssoftware (Virenschutz, Firewall usw.) auszuschalten, zu blockieren oder sicherheitsrelevante Einstellungen an diesen zu verändern.

Es ist nicht erlaubt, eigenmächtig Software- und Hardware-Erweiterungen auf Informatikmitteln der Lindenhofgruppe zu installieren.

5 Daten sicher bearbeiten

Die Mitarbeitenden dürfen nur ihre eigenen, persönlichen Benutzerkonten oder die ihnen zugeteilten funktionellen IT-Konten verwenden. Sie sind für die mit ihrer Benutzer-ID erfolgten Zugriffe verantwortlich.

Geschäftsbezogene Daten müssen auf den dafür bestimmten Serverlaufwerken gespeichert werden. Die Speicherung solcher Daten auf den persönlichen Laufwerken ist verboten. Es ist aus Sicherheitsgründen verboten, Patientendaten, Mitarbeiterdaten und vertrauliche/geheime Geschäftsdaten in Cloud-Diensten (DropBox, WhatsApp etc.) zu speichern oder verschicken.

Geschäftliche Daten dürfen von den Vorgesetzten und anderen berechtigten Mitarbeitenden eingesehen werden. Dies ist auch bei Abwesenheit sicherzustellen. Bei Aus- oder Übertritt sind die Dokumente der vorgesetzten Stelle zu übergeben.

6 Passwörter und PIN

Passwörter/PIN sind persönlich und vertraulich. Sie dürfen nicht aufgeschrieben, unverschlüsselt auf Geräten abgespeichert oder anderen Personen (auch nicht den Vorgesetzen, Stellvertretern usw.) bekannt gegeben werden.

Passwörter müssen eine Kombination von Buchstaben, Ziffern und Sonderzeichen enthalten. Leicht erratbare Passwörter und solche, die einen Bezug zur eigenen Person aufweisen (z.B. Name, Name von Angehörigen, Geburtsdatum usw.), sind nicht erlaubt.

Die Verwendung von gleichen oder ähnlichen Passwörtern/PIN für den geschäftlichen und den privaten Gebrauch ist zu vermeiden.

Initialisierungspasswörter müssen sofort, andere Passwörter regelmässig (z.B. alle 90 Tage) gewechselt werden. Besteht der Verdacht, dass ein Passwort einem Dritten zur Kenntnis gelangt sein könnte, so ist dieses unverzüglich durch ein neues zu ersetzen.

7 Private Nutzung der Informatikmittel

Die Benützung der Informatikmittel für private Zwecke ist erlaubt, solange die Arbeitsleistung nicht beeinträchtigt wird und die beanspruchten Ressourcen (wie Netz-, System- und Speicherkapazität) gering sind. Persönliche Daten müssen auf dem persönlichen Netzwerklaufwerk „U:\“ abgespeichert werden.

Systemkomponenten und Peripheriegeräte dürfen nicht für private Zwecke vom Arbeitsplatz entfernt werden. Geschäftsdaten dürfen nicht privat genutzt oder in privaten Datenablagen oder auf den persönlichen Laufwerken gespeichert werden.

Die private Nutzung der Informatikmittel zu kommerziellen Zwecken ist nicht erlaubt.

8 Einsatz mobiler Geräte

Die Benutzer von mobilen Geräten sind selbst für die Datensicherung und die datenschutzgerechte Aufbewahrung auf diesen verantwortlich.

Für mobile Geräte gilt:

a. Die Geräte sind mit einem Passwort / PIN / Fingerprint oder ähnliche Sicherheitsmechanismen zu schützen.
b. Die Geräte dürfen in öffentlich zugänglichen Räumen nicht unbeaufsichtigt gelassen werden und müssen vor fremden Zugriffen geschützt werden.
c. Die Geräte dürfen nicht anderen Personen zur Nutzung überlassen werden.
d. Es dürfen keine zusätzlichen Applikationen installiert werden (Produktekatalog der Informatik für Hard- und Software). Besteht ein begründeter Bedarf, muss dieser beim Leiter Informatik beantragt werden dieser entscheidet über die Installation.

9 Einsatz privater Geräte

Es dürfen keine privaten Informatikmittel für geschäftliche Aufgaben eingesetzt oder mit dem produktiven Netzwerk der Lindenhofgruppe verbunden werden, die nicht den geltenden Standards der Lindenhofgruppe entsprechen und von der Informatik freigegeben wurden.

10 Fernzugriff

Der Fernzugriff auf das Netzwerk der Lindenhofgruppe wird von der Informatik den Berechtigten Mitarbeitenden freigegeben, sofern die Voraussetzungen erfüllt und die Sicherheitsvorschriften eingehalten werden. Erfolgt der Fernzugriff aus privaten oder öffentlichen Räumen, sind folgedne Vorkehrungen zu treffen, um die Offenlegung von Patienten- oder Mitarbeiterdaten oder vertraulichen/geheimen Dokumenten gegenüber Dritten (Familienangehörige, Besucher etc.) zu vermeiden:

a. Beim Verlassen des Arbeitsplatzes oder bei einem Unterbruch der Arbeit ist die Verbindung zum Server durch korrektes Abmelden zu beenden.
b. Das Gerät ist so zu platzieren, dass keine ungewollte Einsichtnahme möglich ist.
c. Das Gerät muss mit Benutzername und Passwort geschützt und die automatische Computersperre aktiviert werden.

11 Sicherer Umgang mit E-Mails

11.1 Geschäftliche E-Mails

E-Mails mit vertraulichem Inhalt, insbesondere mit Patienten- oder Mitarbeiterdaten oder vertrauliche/geheime Dokumente müssen verschlüsselt versandt werden[1]. Ist eine Verschlüsselung nicht möglich, muss eine andere Versandart gewählt werden (nicht jedoch FAX).

Nicht erlaubt ist das automatische Weiterleiten von E-Mails und das Freigeben der persönlichen Mailbox an eine Drittperson ohne schriftliche Erlaubnis des oder der vorgesetzten Stelle. Bei mehrtägigen Abwesenheiten ist die Funktion des Abwesenheitsassistenten zu nutzen.

[1] Versand von E-Mails über HIN, d.h. von Vorname.Name@lindenhofgruppe.ch an Vorname.Name@lindenhofgruppe.ch oder an beispiel@hin.ch oder andere für HIN-Verschlüsselung registrierte Firmen-Adresse. Eine Überprüfung kann auf www.hin.ch vorgenommen werden.

Das Versenden von E-Mails mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt, Massen-Mails oder das Versenden von E-Mails mit der Aufforderung zum Weiterversand im Schneeballsystem sind verboten.

Es ist verboten, fremde E-Mailsysteme (beispiel@bluewin; @gmail; @yahoo etc.) für Patienten- und Mitarbeiterdaten zu verwenden.

Bei Aus- oder Übertritt sind dienstliche Mailarchive der vorgesetzten Stelle zu übergeben.

11.2 Private Nutzung der Lindenhofgruppe E-Mail-Adresse

Private E-Mails müssen entweder gelöscht oder im persönlichen Ordner (mit «Privat» gekennzeichnet) abgelegt werden. In den nicht persönlichen Ordnern wird nicht unterschieden zwischen geschäftlichen und persönlichen Mails.

Alle von einer von der Lindenhofgruppe zur Verfügung gestellten E-Mail-Adresse ein- und ausgehenden E-Mails werden archiviert und können nicht individuell gelöscht werden. Dies gilt auch für private E-Mails.

Durch die Einrichtung von Filtern, durch Archivierung, das zeitlich begrenzte Zurückhalten oder Verändern von Nachrichten oder durch sonstige Eingriffe kann auch auf private E-Mails Eingriff genommen werden.

11.3 Verdächtige E-Mails

E-Mails mit unbekanntem Absender, verdächtigem Betreff oder unüblichem Inhalt sind im Hinblick darauf, dass sie von der Virenschutzsoftware nicht erkannte Viren enthalten können, ungeöffnet zu löschen; angehängte Dateien, insbesondere solche, die ausführbare Programme enthalten, dürfen keinesfalls geöffnet werden.

12 Sichere Nutzung des Internets

Patienten- oder Mitarbeiterdaten sowie vertrauliche/geheime Geschäftsdaten dürfen via Internet nur verschlüsselt oder über eine geschützte Verbindung (bspw. HIN-Netz) übermittelt werden. Es ist verboten, externe Internetdienste (bspw. GoogleCalendar, Acrobat.com, Dropbox) für Patienten- und Personaldaten zu verwenden.

Geschäftsrelevante Daten der Lindenhofgruppe dürfen nur von den dazu durch die Geschäftsleitung ausdrücklich berechtigten Personen im Internet publiziert werden.

Der Zugriff auf Internet-Seiten mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt und die zu privaten Zwecken erfolgende Nutzung von Chatrooms, sowie Tauschbörsen ist verboten. Die Informatik kann im Auftrag der Geschäftsleitung den Zugriff auf bestimmte Online-Dienste sperren.

13 Umgang mit Sozialen Medien

Geben Sie niemals Informationen über Patientinnen und Patienten, Arbeitskolleginnen und -kollegen sowie geheime, vertrauliche oder nicht öffentliche Informationen der Lindenhofgruppe auf sozialen Netzwerken preis. Verwenden Sie zur Registrierung nicht ihre Lindenhofgruppe E-Mail-Adresse.

Melden sich bei Ihnen medienschaffende oder Social-Media-User wegen einer Auskunft, die Ihren Arbeitgeber betrifft, antworten Sie nicht selbst sondern verweisen an die Kommunikationsstelle der Lindenhofgruppe.

Die private Nutzung sozialer Netzwerke (bspw. Facebook, XING) soll ausserhalb der Arbeitszeit erfolgen. Während der Arbeitszeit ist sie auf ein Minimum zu beschränken.

14 Datenlöschung, Reparatur und Entsorgung von Datenträgern

Daten die nicht mehr gebraucht und auch nicht archiviert werden müssen, sind sicher zu vernichten bzw. zu löschen.

Elektronische Datenträgern (z.B. USB-Sticks, Speicherkarten, CDs, Geräte mit fest eingebauten Speichermedien) auf denen Patienten- oder Mitarbeiterdaten sowie vertrauliche/geheime Geschäftsdaten abgespeichert oder auf denen früher einmal solche Daten gespeichert worden sind, sind der Informatik zur Löschung oder Entsorgung zu übergeben. Diese entscheidet gemäss ihren Richtlinien über die weitere Verwendbarkeit oder die Entsorgung solcher Komponenten.

Nur die Informatik darf Informatikmittel in die Reparatur oder zur Entsorgung geben. Sie sorgt dafür, dass die Vertraulichkeit von Patientendaten, vertraulichen Mitarbeiter- oder Geschäftsdaten der Lindenhofgruppe gewährleistet bleibt.

Papierunterlagen mit Patientendaten, mit vertrauliche Mitarbeiter- oder Geschäftsdaten der Lindenhofgruppe sind entweder in den dafür bereitgestellten Containern oder in einem Aktenvernichter zu entsorgen.

15 Gefahren und Verluste melden

Der Verlust oder Diebstahl von Informatikmitteln der Lindenhofgruppe oder von geschäftlich benützten privaten Geräten ist unverzüglich dem ServiceDesk und der vorgesetzten Stelle zu melden.

Besteht der Verdacht, dass Zugangs- oder Zugriffsberechtigungen unberechtigt durch Dritte genutzt werden oder dass ein Informatikmittel mit schadenverursachender Software (Viren, Trojaner usw.) infiziert sein könnte, ist dies umgehend dem ServiceDesk zu melden.

Umgehend zu melden ist auch der Verlust:

a. von Schlüsseln dem Technischen Dienst;
b. von Badges dem Human Resources.

16 Schlussbestimmungen

Die Einhaltung der vorliegenden Weisung wird u.a. anhand von automatisch erstellten Aufzeichnungen überprüft (Protokollierung der Benutzeraktivitäten). Für Kontrollen werden die Empfehlungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) sinn- und sachgemäss angewandt.

Verstösse gegen diese Weisung können disziplinarische und/oder personalrechtliche Massnahmen zur Folge haben.

17 Inkrafttreten

Diese Weisung tritt am 1. Juni 2018 in Kraft und ersetzt alle früheren Regelungen und Bestimmungen der Lindenhof AG respektive deren Spitäler, welche zu dieser Weisung im Widerspruch stehen.