INFORMATIONSSICHERHEITSRICHTLINIE FÜR EXTERNE

RICHTLINIE

INHALT

1. Einleitung

Im Marienhospital Stuttgart nehmen Informationssicherheit und Datenschutz einen hohen Stellenwert ein. Die Sicherheit der verarbeiteten Daten – insbesondere die Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Compliance und aufgrund der Tätigkeit in der Gesundheitsbranche die Sicherstellung der Patientensicherheit und der Behandlungseffektivität – ist von höchster Priorität. Aus diesem Grund haben auch Externe, welche Zugriff auf Daten oder Systeme im Marienhospital Stuttgart erhalten, entsprechende Vorgaben in Bezug auf Informationssicherheit und Datenschutz umzusetzen.

Diese Richtlinie gilt für alle Externen, die im Auftrag des Marienhospital Stuttgart tätig sind bzw. Arbeiten für das Marienhospital Stuttgart verrichten (z. B. Auftragnehmer, Dienstleister, Partner etc.). Der Externe hat seine Mitarbeiter über diese Richtlinie und die einzuhaltenden Vorgaben zu informieren. Die vorliegende Richtlinie kann durch das Marienhospital Stuttgart jederzeit erweitert oder angepasst werden. Der Externe wird über Änderungen informiert.

2. Datenschutz und Wahrung des Datengeheimnisses

Das Gesetz über den kirchlichen Datenschutz (KDG) - Entsprechung in § 53 BDSG-neu - in der geltenden Fassung gilt uneingeschränkt. Alle Mitarbeiter des Externen sind durch dieses zur Wahrung des Datengeheimnisses gemäß § 5 KDG zu verpflichten. Insbesondere sind personenbezogene Daten sowie interne Daten im Marienhospital Stuttgart geheim zu halten. Das Datengeheimnis gilt auch über das Ende des Vertrags- und Dienstverhältnisses hinaus.

Die im Zuge der Tätigkeit erlangten Daten dürfen nicht für eigene Zwecke verwendet werden und müssen nach Beendigung an das Marienhospital Stuttgart zurückgegeben oder nachweislich vernichtet werden.

3. Sicherheits- und Datenschutzvorfälle

Alle sicherheits- oder datenschutzrelevanten Ereignisse sowie erkannte Schwachstellen, die Auswirkungen auf das Marienhospital Stuttgart haben oder haben könnten, sind sofort dem Informationssicherheitsbeauftragten oder dem Informationssicherheitskoordinator des Marienhospital Stuttgart zu melden (siehe Kapitel 0 Kontaktdaten). Für die Aufklärung der Ereignisse sind alle notwendigen Informationen bereitzustellen.

Beispiele für sicherheits- oder datenschutzrelevante Ereignisse sind

- Verdacht auf Missbrauch von Benutzerkennungen
- Ungewünschte Veröffentlichung von internen Daten des Marienhospital Stuttgart im Internet
- Verlust / Diebstahl von IT-Systemen oder Datenträgern mit internen Daten des Marienhospital Stuttgart
- Versehentliches Versenden einer E-Mail mit internen Daten des Marienhospital Stuttgart an den falschen Empfänger
- Infektion mit Schadsoftware
- etc.

4. Fernwartungszugriff

Wird dem Externen im Zuge seiner Tätigkeit für das Marienhospital Stuttgart ein Fernwartungszugriff auf Systeme im Marienhospital Stuttgart zur Verfügung gestellt, sind die folgenden Vorgaben einzuhalten:

- Der Fernwartungszugang darf ausschließlich von denjenigen Personen verwendet werden, für die der Zugang zur Verfügung gestellt wurde.
- Der Fernwartungszugang darf nur für dienstliche Zwecke und ausschließlich zur Durchführung der vereinbarten Tätigkeiten verwendet werden. Jede andere Verwendung ist ausdrücklich untersagt.
- Eine geöffnete Fernwartungssitzung darf nicht unbeaufsichtigt gelassen werden.
- Sobald die durchzuführenden Tätigkeiten erledigt sind und die Fernwartungssitzung nicht mehr benötigt wird, ist diese umgehend zu schließen.
- Der Externe hat Aufzeichnungen über die durchgeführten Tätigkeiten zu führen und diese auf Anfrage an das Marienhospital Stuttgart zu übermitteln. Die Aufzeichnungen umfassen mindestens folgende Angaben:
    - Mitarbeiter, der eine Tätigkeit durchgeführt hat
    - System, auf dem die Tätigkeit durchgeführt wurde
    - Beschreibung der durchgeführten Tätigkeit
    - Startzeitpunkt der durchgeführten Tätigkeit (Datum und Uhrzeit)
    - Endzeitpunkt der durchgeführten Tätigkeit (Datum und Uhrzeit)
- Alle Fernwartungszugriffe sowie auf den Systemen im Marienhospital Stuttgart durchgeführten Tätigkeiten werden protokolliert und ggf. ausgewertet.
- Der Externe hat dem aktuellen Stand der Technik entsprechende technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen, dass die Fernwartungsverbindung nicht missbräuchlich verwendet wird und kein unbefugter Zugriff auf Daten und Systeme im Marienhospital Stuttgart besteht.
- Bei Verdacht auf Missbrauch des Fernwartungszugangs ist dies unverzüglich dem Informationssicherheitsbeauftragten oder dem Informationssicherheitskoordinator des Marienhospital Stuttgart zu melden.

5. Fotografieren und Filmen

Das Fotografieren und Filmen in den Räumlichkeiten des Marienhospital Stuttgart ist gemäß Hausordnung grundsätzlich untersagt.
In der freigegebenen Dienstanweisung für "Foto- und Filmaufnahmen am Arbeitsplatz" wird für Patienten und Mitarbeiter die Hausordnung weiter spezifiziert, sowie der Umgang mit zulässigen Bildaufnahmen (z. B. aus medizinischen Gründen, zur Aus- und Weiterbildung oder für Publikationen) auf Grundlage gesetzlicher Bestimmungen oder Einwilligungen der Betroffenen geregelt.

6. Technische und organisatorische Maßnahmen (TOMs)

Der Externe hat in seinem Verantwortungsbereich dem aktuellen Stand der Technik entsprechende technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen, dass die Daten des Marienhospital Stuttgart angemessen vor unbefugtem Zugriff, Veröffentlichung, Zerstörung und Manipulation geschützt sind. Es sind die in den folgenden Abschnitten beschriebenen Maßnahmen oder als gleichwertig anzusehende Alternativen umzusetzen.

6.1 Verschlüsselung von externen Speichermedien

Werden Daten des Marienhospital Stuttgart auf externen Speichermedien (z. B. USB-Sticks) gespeichert, so sind diese gemäß dem aktuellen Stand der Technik zu verschlüsseln. Als Passwort ist ein sicheres Passwort gemäß den Vorgaben in Kapitel 6.7 zu wählen.

6.2 Absicherung der E-Mail-Kommunikation

Um eine Sicherung von E-Mails auf dem Transportweg zu gewährleisten, ist die Verschlüsselung des Transportwegs (zumindest Server zu Server) auf den Mailservern des Externen zu aktivieren. Vertrauliche Inhalte dürfen nicht per E-Mail übertragen werden, der Übertragungsweg ist dann im Einzelfall abzustimmen.

6.3 Übertragung von personenbezogenen Daten

Personenbezogene Daten (z. B. in Datenbank-Dumps, Backups, Screenshots mit derartigen Daten usw.) dürfen **nicht unverschlüsselt per E-Mail übertragen** werden! Es ist ein sicherer Übertragungsweg zu verwenden, der im Einzelfall mit dem Marienhospital Stuttgart abgestimmt werden muss.

6.4 Verschlüsselung von mobilen IT-Systemen

Alle mobilen IT-Systeme (z. B. Notebooks, Smartphones etc.), mit denen Zugriff auf Daten oder Systeme im Marienhospital Stuttgart möglich ist, müssen über eine Festplattenverschlüsselung bzw. Datenspeicherverschlüsselung verfügen.

6.5 Malwareschutz

Alle Systeme, mit denen Zugriff auf Daten oder Systeme im Marienhospital Stuttgart möglich ist bzw. auf denen Daten im Marienhospital Stuttgart verarbeitet werden, sind mit einer Malwareschutzlösung vor Schadsoftware zu schützen. Die Malwarepatches sind regelmäßig (mehrmals täglich) zu aktualisieren.

6.6 Patch Management

Auf allen Systemen, mit denen Zugriff auf Daten oder Systeme im Marienhospital Stuttgart möglich ist bzw. auf denen Daten des Marienhospital Stuttgart verarbeitet werden, sind sicherheitsrelevante Patches zeitnah zu installieren. Dies betrifft nicht nur Patches des Betriebssystems, sondern auch zusätzlich installierter Applikationen. Zum Einsatz dürfen nur Betriebssysteme kommen, welche vom jeweiligen Hersteller noch mit sicherheitsrelevanten Patches versorgt werden.

6.7 Passwörter

Alle Zugänge, mit denen Zugriff auf Daten oder Systeme im Marienhospital Stuttgart möglich ist, sind mit einem personalisierten Passwort vor unbefugtem Zugriff zu schützen. Bei der Wahl des Passworts sind folgende Vorgaben einzuhalten:

- Länge: mind. 12 Zeichen
- Komplexität (Verwendung von Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen)
- Vermeidung von Personennamen (z. B. eigener Name, Name des Partners, Namen der Kinder, Name des Haustiers)
- Vermeidung von Systemnamen (z. B. Kennung des eigenen Arbeitsgeräts)
- Vermeidung von allen Wörtern, die in einem Wörterbuch vorkommen (auch fremdsprachige Wörterbücher)
- Vermeidung einfacher Buchstaben- und Zahlenkombinationen (z. B. abcdef, 1234 usw.)
- Trennung der Kennwörter für Firmen- und Privatgebrauch
- Sonderzeichen und Zahlen sollten nicht am Schluss an das Passwort angehängt werden

Jeder Mitarbeiter des Externen ist für die sichere Auswahl des Passworts und dessen Geheimhaltung verantwortlich. Die Weitergabe des persönlichen Benutzereinstiegs ist nicht zulässig.

Passwörter können auf freiwilliger Basis jederzeit geändert werden. Bei Verdacht auf Kompromittierung sind Passwörter zwingend zu ändern. Initialpasswörter sind bei der ersten Anmeldung auf persönliche Passwörter zu ändern.

6.8 Personalisierte Zugänge

Alle Zugänge, mit denen Zugriff auf Daten oder Systeme des Marienhospital Stuttgart möglich ist, müssen personalisiert sein. Der Zugriff auf Daten mittels Gruppenuser ist zu unterbinden. Es muss zu jedem Zeitpunkt nachvollziehbar sein, welcher Benutzer auf welche Daten oder Systeme des Marienhospital Stuttgart zugegriffen hat.

6.9 Clear Desk/Clear Screen

Alle Daten im Marienhospital Stuttgart (digital oder ausgedruckt) sind vor unbefugtem Zugriff zu schützen.

Ausgedruckte Dokumente dürfen nicht offen liegen gelassen werden. Ausgedruckte Dokumente dürfen nicht im Drucker verbleiben, sondern sind schnellstmöglich abzuholen. Das gilt insbesondere für Räumlichkeiten, zu denen auch Externe Zugang haben. Nicht mehr benötigte vertrauliche Dokumente sind sicher zu vernichten (z. B. mittels geeigneter Aktenvernichter). Zudem ist darauf zu achten, dass das Führen von vertraulichen Telefonaten/Gesprächen, die das Marienhospital Stuttgart betreffen, nur in einer leicht zu überblickenden Umgebung stattfinden soll.

Alle Clients, mit denen ein Zugriff auf Daten oder Systeme des Marienhospital Stuttgart möglich ist, sind bei Abwesenheit zu sperren.

6.10 Vernichtung von Daten

Ausgeschiedene Datenträger sowie nicht mehr benötigte Dokumente, auf denen Daten des Marienhospital Stuttgart enthalten sind, sind sicher zu vernichten.

7. Auditrecht

Das Marienhospital Stuttgart hat das Recht, die Einhaltung der Sicherheitsmaßnahmen bei Externen zu überprüfen oder durch einen beauftragten Dritten überprüfen zu lassen.

8. Informations- und Rückgabepflicht bei Personaländerungen

Tritt ein Mitarbeiter des Externen aus dem Unternehmen aus bzw. ändert sich sein Aufgabengebiet, sodass er keine Tätigkeiten mehr für das Marienhospital Stuttgart durchführt, hat der Externe das Marienhospital Stuttgart unverzüglich darüber zu informieren. An den Mitarbeiter ausgegebene Geräte oder Zutrittskarten des Marienhospital Stuttgart sind an das Marienhospital Stuttgart zurückzugeben.

9. Konsequenzen bei Verstößen

Zuwiderhandlungen gegen diese Richtlinie oder jedes andere Verhalten, das einen Verstoß gegen diese Richtlinie darstellt, können vertragliche Sanktionen bis hin zu straf- oder zivilrechtlichen Konsequenzen zu Folge haben.

10. Kontaktdaten

	Rolle	Name	Telefon
	Informationssicherheitsbeauftragter	Axel Schneider (x-tention)	+43 7242 2155 6226 axel.schneider@x-tention.at
	Informationssicherheitskoordinator	Zur Zeit nicht besetzt	-
	Datenschutzkoordinatorin	Claudia Carl-Willing	+ 49 711 6489-3004 Claudia.Carl-Willing@vinzenz.de