

Datenschutz- und Informationssicherheitskonzept

|  |  |  |
| --- | --- | --- |
| **Version** | **Autor** | **Notiz** |
| 1.0 | Berat Mengen | Erstversion |
|  |  |  |
|  |  |  |

**Änderungshistorie**

Inhalt

[1 Einführung 4](#_Toc129642600)

[2 Anwendungsbereich (Statement of Applicability) 4](#_Toc129642601)

[3 Normative Verweise 4](#_Toc129642602)

[4 Abkürzungs- und Begriffsverzeichnis 4](#_Toc129642603)

[5 Kontext der Organisation 4](#_Toc129642604)

[6 Führung 5](#_Toc129642605)

[7 Planung 5](#_Toc129642606)

[7.1 Organisatorische Maßnahmen 5](#_Toc129642607)

[7.2 Technische Maßnahmen 6](#_Toc129642608)

[8 Unterstützung 8](#_Toc129642609)

[9 Betrieb 8](#_Toc129642610)

[10 Bewertung der Leistungen 8](#_Toc129642611)

[11 Verbesserungen (KVP – Kontinuierlicher Verbesserungsprozess) 8](#_Toc129642612)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Datum | Autor/in | Änderung | Begründung | Betroffene Seiten |
| 1.0 | 13.03.2023 | Berat Mengen | Alles | Erstversion | Alle Seiten |
|  |  |  |  |  |  |

Inhalt

[1 Zweck und Anwendungsbereich 5](#_Toc129704501)

[2 Datenschutz und Informationssicherheitskonzept 5](#_Toc129704502)

[2.1 Organisatorische Maßnahmen 5](#_Toc129704503)

[2.2 Technische Maßnahmen 5](#_Toc129704504)

[3 Normative Verweise 6](#_Toc129704505)

[4 Abkürzungs- und Begriffsverzeichnis 6](#_Toc129704506)

[5 Kontext der Organisation 6](#_Toc129704507)

[6 Führung 7](#_Toc129704508)

[7 Planung 7](#_Toc129704509)

[7.1 Organisatorische Maßnahmen 7](#_Toc129704510)

[7.1.1 Spezielle Betrachtung von Home-Office und Telearbeiten 8](#_Toc129704511)

[7.2 Technische Maßnahmen 9](#_Toc129704512)

[8 Unterstützung 10](#_Toc129704513)

[9 Betrieb 10](#_Toc129704514)

[10 Bewertung der Leistungen 10](#_Toc129704515)

[11 Verbesserungen (KVP – Kontinuierlicher Verbesserungsprozess) 11](#_Toc129704516)

# Zweck und Anwendungsbereich

Dieses Dokument regelt die Vorgehensweise für die Implementierung und regelmäßige Überwachung eines Datenschutz- und Informationssicherheitssystems für die Wien-5-Tagesklinik Um das Sicherheitsniveau möglichst hochzuhalten, ist es von Notwendigkeit, dass das Dokument in der gesamten Unternehmensstruktur gilt und ohne Ausnahme befolgt und durchgeführt werden muss.

Das Dokument basiert auf die rechtlichen Gegebenheiten des österreichischen Gesetzesrahmen.

# Datenschutz und Informationssicherheitskonzept

## Organisatorische Maßnahmen

Für dieses Projekt wird ein Team zusammengestellt, dass sich aus 7 Personen zusammenstellt. Dieses Team sieht wie gefolgt aus, 1 CISO, 4 Fachkräfte der Firma „HEALTHSYS“ und 2 Mitarbeiter der „Wien-5-Tagesklinik“ Es ist von Notwendigkeit, dass sich das Team im Normalen betrieb jede dritte Woche trifft, um mögliche Gefährdungen oder Bedrohungen so früh wie möglich zu erkennen und die notwendigen Maßnahmen dazu planen und diese auch umsetzen. Die neuen schritte die Durchgeführt wurden, werden schriftlich protokolliert, damit die gesamte Organisation davon informiert werden kann. Dabei wird der Datenschutz der personenbezogenen Daten (DSVGO) und das NISG vollständig beachtet und durchgeführt, so dass mit diesen Daten sicher umgegangen werden kann. Damit die Infrastruktur einen hohen Standard besitzt, wird die CIA-Triade angewandt. Der CISO ist der Verantwortliche dieses gesamten Konzeptes und muss darauf achten, dass alles planmäßig abläuft.

## Technische Maßnahmen

Jegliche Daten, die in der Datenbank der „Wien-5-Tagesklinik“ gespeichert werden, werden verschlüsselt abgespeichert, mittels Bitlocker. Führungspersonal und Mitarbeiter\*Innen bekommen Chipkarten, die Ihnen in gewisse Räume eintritt, verschafft. Wodurch Patienten ohne Personal nicht in unerlaubte Räume gelangen können. Die Computer im Behandlungs- und Untersuchungsbereich sind Passwort geschützt, die jedes Mal beim Verlassen des Platzes wieder versperrt werden müssen. PCs im Wartebereich der Anmeldung, kriegen nach ca 25 Minuten Inaktivität einen Bildschirmschoner, wodurch sie wieder Ihr Kennwort eingeben müssen. Mitarbeiter die aus gesundheitlichen Gründen nicht vor Ort sein können haben auch die Möglichkeit von einem anderen Netzwerk sich per VPN mit dem Server zu verbinden. Daten können so nicht heruntergeladen werden, wodurch die Daten nicht entwendet werden können.

# Normative Verweise

Da das Projekt im gesundheitlichen Sektor angesiedelt ist und der Schutz der Patientendaten ein sehr wichtiger Punkt ist, ist es wichtig, dass hierbei die DSGVO, GTelG, sowie das NISG eingehalten wird. Es wird verlangt das Sicherheitskonzept der „Wien-5-Tagesklinik“ nach aktuellen Standards und unter Einhaltung von entsprechenden Normen zu implementieren, um das Sicherheitsniveau im IKT-Bereich möglichst hochzuhalten.

# Abkürzungs- und Begriffsverzeichnis

CIA Confidentiality, Integrity, Availability (=Vertraulichkeit, Integrität, Verfügbarkeit)

CISO Chief Information Security Officer

DSGVO Datenschutzgrundverordnung

GTelG Gesundheitstelematikgesetz

KOFÜ Kollegiale Führung

KVP Kontinuierlicher Verbesserungsprozess

NISG Netz- und Informationssicherheitsgesetz

PDCA Plan, Do, Check, Act (=Planen, Durchführen, Kontrollieren, Agieren)

SOC Security Operations Center

# Kontext der Organisation

* Wien-5-Tagesklinik:
  + Ärztinnen und Ärzte
  + Verwaltungspersonal
  + Technisches Personal
  + CISO
* HEALTHSYS:
  + Mitarbeiter

|  |  |  |  |
| --- | --- | --- | --- |
| **Intern/Extern** | **Rolle** | **Zugriffsberechtigung** | **Homeoffice** |
| Intern | Ärztinnen und Ärzte | Anwendungsprogramme | Nicht vorgesehen, in speziellen Fällen kann Homeoffice beantragt werden |
| Extern | Ärztinnen und Ärzte | Keine speziellen Zugriffsberechtigungen, Anwendungsprogramme können bei Bedarf freigeschaltet werden (Genehmigung durch CISO) | Nicht vorgesehen |
| Intern | Verwaltungspersonal | Anwendungsprogramme | Nicht vorgesehen, in speziellen Fällen kann Homeoffice beantragt werden |
| Extern | Verwaltungspersonal | Keine speziellen Zugriffsberechtigungen vorgesehen -> Anwendungsprogramme können gemeinsam mit internen Personal verwendet werden | Nicht vorgesehen |
| Intern | Technisches Personal | Anwendungs- & Systemprogramme | Homeoffice kann beantragt werden |
| Extern | Technisches Personal | Zugriff auf Anwendungs- & Systemprogramme muss durch CISO oder Chefität genehmigt werden | Nicht vorgesehen, in speziellen Fällen kann Homeoffice beantragt werden |

# Führung

Der CISO übernimmt die Verantwortung für die kollegiale Führung. Im Falle eines Ausfalls oder Angriffs ist er verpflichtet, umgehend die kollegiale Führung und das NIS zu informieren. Zusätzlich dazu muss das SOC benachrichtigt werden, da es dafür zuständig ist, den Normalbetrieb wiederherzustellen, das System vor Angriffen zu schützen und die Daten zu sichern.

# Planung

## Organisatorische Maßnahmen

PDCA: Plan Do Check Act

* Risikoanalyse
* Identifizierung der bestehende/ möglichen Bedrohungen und Risiken
* Bewertung der Risiken und Schwachstellen unter Berücksichtigung der DSGVO, NIS, GTel- Gesetze
* Kategorisierung der Risiken in den Kategorien:
  + HIGH RISK
  + MID RISK
  + LOW RISK
* Maßnahmen zur Risikominimierung:
* Team bilden -> alle 3 Wochen Meetings über Stand und Probleme
* Kritische Räume (Büros mit PCs, Serverraum) mittels Chipkarten absichern und Zugangskontrollen einbauen -> Überlegungen wer Zutritt erhält
* Verschlüsselung der Daten -> kryptografische Verschlüsselungsmechanismen
* Zutrittskontrolle -> Rollenverteilung mit verschiedenen Zugriffsrechten
* Zugriffkontrolle (2 Faktor Authentifizierung) mit 1mal Tan (Computer sind passwortgeschützt) oder (noch besser) Biometrischen Daten
* Deaktivierung nach 25-minütiger Inaktivität
* Geschütze Bildschirme (bei seitlicher Betrachtung kann ein Beobachter nichts sehen)
* Verwendung der CIA-Triade
* Regelung der Datensicherheit und des Datenschutzesà DSGVO
* Sicherheitsmanagement
  + Regelungen zur Meldung von Sicherheitsvorfällen
  + Verfahren zur Behebung von Sicherheitsvorfällen
  + Dokumentation von Sicherheitsvorfällen
* Verantwortlichkeiten und Zuständigkeiten
  + Festlegung von Verantwortlichkeiten und Zuständigkeiten
  + Zuweisung von Aufgaben und Verantwortlichkeiten
* Brandschutzplan
* Notfallplan erstellen:
  + Meldungsstelle errichten
  + Notfallmanager
* Belastung/Strapazierfähigkeit der Services einschränken
* CERT (Team, welches sich mit Bedrohungen/ Angriffe befasst) alamieren
* Disaster-Recovery-Plan
* Business-Continuity-Plan: beschreibt Strategien, welche
* Qualitätsmanagement durchführen (PDCA)
* Brandschutzplan:
  + Argongas;
  + Alarmsystem zur Erkennung des Brandfalls
  + Alarmsystem vor dem Freisetzen des Argongases, sodass die Personen in einem Raum raus gehen können
  + Notfallknopf, sodass eine Person, die in einem Raum ist, die Freisetzung des Gases verzögern kann

### Spezielle Betrachtung von Home-Office und Telearbeiten

* Online-Firmenportal mit notwendigen Daten etc. schaffen, sodass nichts am PC direkt gespeichert wird
* Anonymisierung der Daten in manchen Fällen möglich? -> Dann anonymisieren
* Zugang nur über firmeninternes Netz oder VPN ermöglichen
* Firmenlaptops ohne Installationsberechtigung o.ä. vergeben (evtl. verschlüsseln)
* Logging implementieren
* Regelmäßiges evaluieren ob Home-Office notwendig
* Ohne Interaktion -> Firmenportal nach 10 Minuten ausloggen

## Technische Maßnahmen

* Kryptografische Verschlüsselungsmechanismen, wie z.B. das Public Key Verfahren, Base64 und BitLocker, werden für die Verschlüsselung der Daten genutzt.
* Zutrittskontrolle erfolgt über eine Chipkarte für Ärzte und für den Zugriff ist eine zweifache Authentifizierung mittels einem einmaligen TAN erforderlich. Computer sind passwortgeschützt und deaktivieren sich nach 15-minütiger Inaktivität.
* Für die Arbeit im Home-Office wird ein Terminal Server verwendet.
* Die Datenintegrität wird durch Mechanismen wie MAC sichergestellt.
* Die Verwendung von HTTPS mit privatem und öffentlichem Schlüssel gewährleistet eine sichere Übertragung der Daten.
* Zur Protokollierung wird Logging eingesetzt und Time Keeping wird gewährleistet.
* Die Rollenbasierte Zugriffskontrolle (RBAC) und Sicherheitsetiketten sind Teil der Zugriffskontrolle.
* Digitale Signaturen werden für die Genehmigung von Lese-, Änderungs- und anderen Vorgängen genutzt.
* Maßnahmen gegen SQL-Injections, wie z.B. Textüberprüfung der Input-Felder und Stored Procedures, werden umgesetzt.
* Regelmäßige Backups und Cloud-Lösungen, die der DSGVO entsprechen, werden eingesetzt.
* Outsourcing der Datenverarbeitung an ein externes Rechenzentrum ist eine weitere Maßnahme.
* In wichtigen Räumen sind Notfallknöpfe installiert und es werden automatisierte Systemtests durchgeführt.
* Für den Notfall gibt es Hot-, Cold-, Warm-Standby-Systeme und Notstromaggregate. Die Redundanz wird durch RAID-Systeme gewährleistet.
* Server- Snapshots
* Redundanz bei den Versorgungsquellen

# Unterstützung

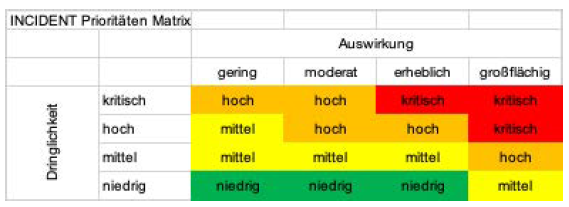
* Schulungen:
  + Phishing Mails:
  + Passwörter:
  + Smishing:
  + Schutz vor Drittpersonen (Folie auf Laptopbildschirm)
  + Nichts Privates auf Firmengeräte speichern
  + Social Engineering
* Compliance
  + Einhaltung von gesetzlichen Vorschriften und Richtlinien, insbesondere der DSGVO, NIS und des Gesundheitstelematikgesetzes
  + Regelmäßige Überprüfung und Aktualisierung der Richtlinie, um sicherzustellen, dass sie den aktuellen Anforderungen und Standards entspricht

# Betrieb

Die Mitarbeiterinnen und Mitarbeiter des SOC haben jeweils oder in speziell zugewiesenen Teams bestimmte Bereiche der Verteidigungslinie, auf die sie sich spezialisiert haben. Je nach Zuständigkeitsbereich sind einige Mitarbeiterinnen und Mitarbeiter für die Verschlüsselung von Daten verantwortlich, während andere dafür zuständig sind, diese Daten auf einem Backup-Server zu speichern, um deren Verfügbarkeit sicherzustellen oder Daten im Allgemeinen zu schützen. Das SOC deckt Sicherheitslücken durch gezielte Tests und Angriffe auf, die von anderen Mitarbeiterinnen und Mitarbeitern des SOCs behoben werden. Nach jedem Update oder Wartungsvorgang eines Systems muss das System erneut getestet werden. Das SOC soll das System vor Angriffen schützen und diese abwehren. Die Richtlinien und Dokumente, die vom SOC erstellt werden, müssen ständig aktualisiert werden, um Änderungen in Geräten oder anderen Faktoren zu berücksichtigen..

# Bewertung der Leistungen

* Riskobewertung:
  + Risikoplan verschaffen
  + Betroffene Risiken priorisieren (HIGH RISK MID RISK LOW RISK)



# Verbesserungen (KVP – Kontinuierlicher Verbesserungsprozess)

PDCA-Zyklus: Für die Überprüfung der Maßnahmen, ob sie tatsächlich wirken, muss es einen regelmäßigen Kontrollprozess geben (Qualitätsmanagement). In der Planungsphase werden die TOMs definiert und geplant. Im Do werden diese umgesetzt und implementiert. Im Check werden diese überwacht und die Planung mit den Ergebnisse verglichen. Im Act werden Fehler behoben und versucht den Prozess zu verbessern. Es ist wichtig für jedes Risiko die Maßnahmen regelmäßig zu überprüfen und auch immer wieder neue Bedrohungen in den Prozess miteinzubeziehen (z.B. Lessons Learned nach einem Notfall).

Ein Bild, das Text, Brief enthält.

Automatisch generierte Beschreibung