TITEL

|  |  |
| --- | --- |
| Dokumententyp | Orginasatorische Richtlinie / Technische Richtlinie |
| Klassifikation | TLB: ~~red /~~ amber ~~/ green / white~~ |
| Autor/in | 5BHBGM, Name |
| Letzte Änderung | Datum |
| Prüfer/in | Name Prüfer |
| Geprüft am | Datum geprüft |
| Freigeber/in | Name Freigeber |
| Freigegeben am | Datum freigegeben |
| Gültigkeitszeitraum | ab Freigabedatum: 12 Monate / ~~24 Monate~~ / ~~36 Monate~~ |
| Überprüfungsintervall | 3 Monate / ~~6 Monate~~ / ~~12 Monate~~ / ~~18 Monate~~ |
| Version | 1.0 |
| Vertraulichkeit | STATUS: ~~in Bearbeitung /~~ freigegeben ~~/ zurückgezogen~~ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Datum | Autor/in | Änderung | Begründung | Betroffene Seiten |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

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)

# Einführung

* Zweck des Dokumentes
* Richtlinien NIS/ DSGVO/ GTEl à Auf diese Gesetze verweisen

Dieses Dokument regelt die Vorgehensweise für die Implementierung und regelmäßige Überwachung eines Datenschutz- und Informationssicherheitssystems für die <SPENGER- KLINIK>. Um das Sicherheitsniveau möglichst hochzuhalten, ist es nötig, dass das Dokument in der gesamten Unternehmensstruktur gilt und ohne Ausnahme befolgt werden muss. Das Dokument basiert auf die rechtlichen Gegebenheiten des österreichischen Gesetzesrahmen.

# Anwendungsbereich (Statement of Applicability)

Diese Verfahrensanweisung betrifft nur die <Mitarbeiter der SPENGER-KLINIK>, die an dem Projekt beteiligt sind. Daraus erschließt sich, dass das Dokument laut <TLP gelb> ist, und somit die Weitergabe des Empfängers nur an die ausgewählten Mitarbeiter erfolgt.

# Normative Verweise

Da das Projekt im gesundheitlichen Sektor angesiedelt ist und es um den Schutz von Patientendaten geht, ist es wichtig, dass hierbei die DSGVO, GTelG, sowie das NISG in Kraft tritt. Es wird verlangt das Sicherheitskonzept für die Praxis 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

GDA Gesundheitsdiensteanbieter

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

Textbeilage erklären (Organisation der Klinik nennen -> Abteilungen, Mitarbeiter, …)

# Führung

Die kollegiale Führung ist die Leitung der Berufsgruppen. Bei einem Ausfall oder Angriff muss dieser sofort an die kollegiale Führung und dem NIS gemeldet werden. Außerdem muss das SOC in Kenntnis gesetzt werden, da dieses dafür verantwortlich ist den Normalzustand wieder herzustellen wie auch das System vor Angriffen zu schützen bzw. die Daten zu sichern.

# Planung

//Gefahrenbeschreibung

Hier werden die organisatorischen und technischen Maßnahmen zur VORBEUGUNG von Cyberangriffe genannt.

## 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:
  + Hoch
  + Mittel
  + Niedrig
* Maßnahmen zur Risikominimierung:
* Team bilden -> wöchentliche Meetings über Stand und Probleme
* Schulungen (Schulungen und Sensibilisierung von Mitarbeitern zu den technischen Maßnahmen und Verfahren | Bewusstsein für die Wichtigkeit von IT-Sicherheit und Datenschutz im Gesundheitswesen, um sicherzustellen, dass die Mitarbeiter diese Anforderungen verstehen und umsetzen können)
* Verwendung der CIA-Triade
* Regelung der Datensicherheit und des Datenschutzesà DSGVO
* Vorsorge-Ablaufplan zusammenstellen, sodass jeder in der Klinik weiß, woran er sich zu halten hatà Unsere Schule: Brandschutzplakat im Klassenzimmer
* Überwachung und Aktualisierung der definierten Maßnahmen
* 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

## Technische Maßnahmen

* Verschlüsselung der Daten -> kryptografische Verschlüsselungsmechanismen
  + Public Key Verfahren
  + Base64
  + BitLockerà zur Verschlüsselung des Filesystems
* Zutrittskontrolle -> Chipkarte für Ärzte
* Zugriffkontrolle (2 Authentifizierung) mit 1mal Tan (Computer sind passwortgeschützt)
* Deaktivierung nach 10-minütiger Inaktivität
* Home-Office? -> Terminal Server
* Datenintegrität -> MAC?
* Verwendung von HTTPS (Private key – Public key)
* Logging (Protokollierung)
* Time Keeping
* RBAC: Role Based Access Control: Rollenbasierte Zugriffskontrolle
  + Vllt Sicherheitsettiketen erwähnen:
* Digitale Signatur: Genehmigung von Lese-, Änderungs- und anderen Vorgängen
* Maßnahmen SQL- Injections:
  + Textüberprüfung der Input-Felderà Es dürfen keine Anführungszeichen drinnen stehen
  + Storage Procedures
* Backups ()
* Cloud-Lösungen (Daten werden nicht lokal gespeichert) -> müssen der DSGVO entsprechen
* Outsourcing
* Externes Rechenzentrum
* Notfallknöpfe in wichtigen Räumen
* Automatisierte Systemtests
* Hot cold warm standby (Ersatzgeräte)
* Notstromdiesel
* Raid Systeme (Redundanzen):
  + RAID-0;

Dieser Modus verteilt Daten auf mehrere Festplatten, um die Leistung zu erhöhen. Dabei werden die Daten in kleine Abschnitte aufgeteilt und auf jeder Festplatte gleichzeitig gespeichert. RAID 0 bietet hohe Leistung, da die Daten parallel auf mehrere Festplatten geschrieben und gelesen werden. Allerdings bietet RAID 0 keine Redundanz, d.h. wenn eine Festplatte ausfällt, gehen alle Daten auf allen Festplatten verloren.

**erhöht die Leistung, aber bietet keine Redundanz.**

* + RAID-1:

Dieser Modus spiegelt die Daten auf zwei oder mehr Festplatten, um die Redundanz zu erhöhen. Dabei werden die Daten auf zwei oder mehr Festplatten gleichzeitig geschrieben, so dass im Falle eines Festplattenausfalls die Daten auf den verbleibenden Festplatten gesichert sind. RAID 1 bietet eine hohe Redundanz, aber keine Leistungssteigerung.

**erhöht die Redundanz, aber bietet keine Leistungssteigerung.**

* + RAID-5:

Dieser Modus kombiniert Leistung und Redundanz. Dabei werden Daten und Paritätsinformationen auf mehreren Festplatten gespeichert, so dass im Falle eines Festplattenausfalls die verlorenen Daten aus den Paritätsinformationen wiederhergestellt werden können. RAID 5 bietet eine höhere Leistung als RAID 1, aber eine geringere Redundanz als RAID 1.

**kombiniert Leistung und Redundanz.**

* + RAID-10:

Dieser Modus kombiniert RAID 0 und RAID 1. Dabei werden die Daten auf mehreren Festplatten verteilt, um die Leistung zu erhöhen, und gleichzeitig werden die Daten gespiegelt, um die Redundanz zu erhöhen. RAID 10 bietet sowohl hohe Leistung als auch hohe Redundanz, aber es ist teurer als andere RAID-Modi, da es mindestens vier Festplatten benötigt.

**kombiniert RAID 0 und RAID 1 für hohe Leistung und Redundanz.**

* Server- Snapshots
* Redundanz bei den Versorgungsquellen (Strom, Wasser, Essen, etc.)

# 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

Mitarbeiterinnen und Mitarbeiter des SOC haben jeweils oder in festgelegten Teams ein Gebiet dieser Verteidigungslinie. Auf diesem Gebiet sind sie spezialisiert.

Je nach Aufgabenbereich sind manche für die Verschlüsselung der Daten verantwortlich, das Speichern dieser Daten auf einen Backup-Server, um die Verfügbarkeit zu garantieren oder Daten allgemein zu schützen.

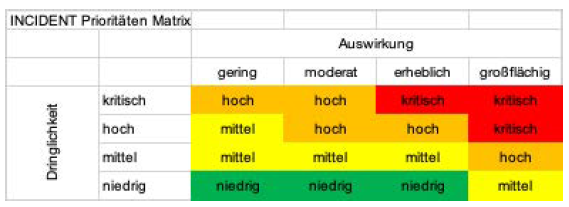
Mittels gezielten Tests und Angriffen seitens der IT-Abteilung werden Sicherheitslücken aufgedeckt, die wiederum von anderen Beschäftigen des SOCs gelöst werden. Regelmäßig, nach jedem Update oder Wartungen eines Systems muss das System wieder getestet werden.

Weiters soll das SOC das System vor Angriffen schützen und diese abwehren.

Die Richtlinien und Dokumente, die vom SOC ausgehen müssen laufend aktualisiert werden, sofern sich Dinge, wie Geräte oder ähnliches ändern.

# Bewertung der Leistungen

* Riskobewertung:
  + Risikoplan einholen
  + Betroffene Risiken priorisieren (Hoch Mittel Niedrig)



# 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).

# Konzept

**ALLES NACH DEM HINAUSLÖSCHEN (Folgende Punkte nur als Info, nicht in Abgabe mit reingeben)**

**Wichtig: Erstellung eines Konzepts. Das Konzept ist das LETZTE Kapitel im Dokument 🡪Kapitel12**

**Vorgehensweise beim Konzept:**

1. Vorgehensweise bei der Arbeit:

* Angabe lesen
* Konzept erstellen: Das Konzept beinhaltet deine Gedanken zu den Aufgabenpunkte. Das Konzept ist sehr vorteilhaft, da die Prüfperson sich dieses durchlesen kann, um deine Denkweise bei den einzelnen Aufgaben zu verstehen. Dies heißt, wenn die Prüfperson nicht deine Vorgehensweise bei einer Aufgabe nachvollziehen kann, schaut diese in das Konzept. Das könnte Punkte bedeuten.
* Das Konzept wird in der Word-Datei als letztes Kapitel dazugegeben.

1. Erstellen eines Konzeptes für die Prüfaufgabe 4b (siehe für Angabe in Moodle) Das Konzept wurde anhand einer Angabe erstellt als BEISPIEL

* Es gibt 2 Firmen:
  + Health Care Austria
  + Primary- Health- Center
* Wozu gehöre ich?: Angabe genau durchlesen
  + Ich bin Mitarbeiter der Health Care Austria und berate die Firma Primary Health Center
* Wichtige Infos auf der 1. Seite:
  + Technische & organisatorische Maßnahmen
  + Verweis auf NISG
    - ACHTUNG: NIS = ungültig
    - Das Gesetz heißt NIS**G**
    - Die Verordnung heißt NIS**V**
    - Dasselbe gilt für GTel, etc🡪 also GTel**G**
  + Mit dem Gesetz muss auch die Verordnung erwähnt werden
* PUNKT 2\_: Was wissen wir zu PHC (=Primary Health Center)?
  + 8 Standorte
    - 6 mit je einer Ordination für Allgemeinmedizin
    - 2 Orte mit: […] siehe Angabe
  + Ganz wichtig: ÖFFNUNGSZEITEN:
    - Es herrscht keine 24h & 365Tage Betriebszeit
  + Vom vorherigen Punkt abgeleitet kann man daher sagen:
    - 1. Wir sind ja zuständig für die IT und Sicherheit. Dafür beraten wir ja PHC
    - Anhand der Öffnungszeiten: Die IT Arbeit muss vorher schon beginnen. Wir legen fest 1h davor und danach🡪 also von den Öffnungszeiten
    - Wartungen finden also dementsprechend auch außerhalb der Öffnungszeiten statt
* PUNKT 3\_:
  + Fiber To The Desk:
    - Fiber = Glas🡪 Glasfaserkabel
  + Andere Kabelarten: bsw. Kupfer
  + Hintergrundwissen zu Kupfer vs. Fiber:
    - Nachteil von Kupfer:
      * Weniger belastbar
      * Brandbreitenproblem
      * Nicht so Ausfallssicher wie Fiber
      * Verkabelung muss abgeschirmt werden
      * Leichter abhörbar
    - Fiber:
      * Multimode: 1.7km
      * Singlemode: bis zu 7km
* Ableitung: Wir brauchen keine Überlegungen für die Stockwerke, da sich von der Länge her ausgehen wird. Bei Kupfer bräuchten wir „Nachrichtenkisten“ (~k.A. wie Hoheißer es genau genannt hat) mit denen wir die Geräte erreichen
  + - FIBER bietet viele Vorteile
  + Wichtige Info: Rechenzentrum ist für 4h konzipiert
* PUNKT 4\_:
  + NISV: regelt welche Sektoren, welche Ausfallssicherheit benötigen
  + Gesundheitssektor: Ausfallssicherheit von 3h
* Also nach 3h muss die Behörde informiert werden
  + Wir erinnern uns an die Öffnungszeiten. Geht sich eine Ausfallssicherheit von 3h bei diesen Öffnungszeiten aus? Antwort: Nein
* Diesen Punkt kann man bei den organisatorischen Maßnahmen in PUNKT 3 beschreiben

1. Einführung:
   * Dieser Abschnitt enthält den Zweck des Dokuments sowie Verweise auf relevante Gesetze wie NIS, DSGVO und GTel.
2. Anwendungsbereich (Statement of Applicability):
   * Dieser Abschnitt gibt an, wer von dieser Verfahrensanweisung betroffen ist und wer Zugang zu den Informationen hat.
3. Normative Verweise:
   * In diesem Abschnitt werden Gesetze und Normen genannt, die bei der Implementierung eines Datenschutz- und Informationssicherheitssystems im Gesundheitssektor zu berücksichtigen sind.
4. Abkürzungs- und Begriffsverzeichnis:
   * Hier werden Abkürzungen und Begriffe erläutert, die in diesem Dokument verwendet werden.
5. Kontext der Organisation:
   * Dieser Abschnitt gibt einen Überblick über die Organisation der Klinik, einschließlich Abteilungen und Mitarbeiter.
6. Führung:
   * In diesem Abschnitt wird beschrieben, wer im Falle eines Ausfalls oder Angriffs zu informieren ist und welche Verantwortlichkeiten und Zuständigkeiten im Zusammenhang mit der Sicherheit und dem Datenschutz in der Klinik bestehen.
7. Planung:
   * Dieser Abschnitt enthält organisatorische und technische Maßnahmen zur VORBEUGUNG von Cyberangriffen, einschließlich einer Risikoanalyse und Maßnahmen zur Risikominimierung.
8. Unterstützung:
   * Hier werden Schulungen und die Einhaltung gesetzlicher Vorschriften und Richtlinien erwähnt.
9. Betrieb:
   * Dieser Abschnitt beschreibt die Rolle des Security Operations Center (SOC) und die Verantwortlichkeiten von Mitarbeitern in Bezug auf den Schutz von Daten.
10. Bewertung der Leistungen:
    * Dieser Abschnitt enthält Informationen zur Bewertung der Leistung des Sicherheits- und Datenschutzsystems der Klinik.
11. Verbesserungen (KVP - Kontinuierlicher Verbesserungsprozess):
    * In diesem Abschnitt wird der PDCA-Zyklus beschrieben, der verwendet wird, um die Wirksamkeit von Maßnahmen zu überprüfen und kontinuierliche Verbesserungen zu erreichen.