Inhalt

[1 Zweck und Anwendungsbereich 1](#_Toc70943423)

[2 Geltungsbereich 1](#_Toc70943424)

[3 Grundlagen 2](#_Toc70943425)

[4 Qualitätsmanagement 2](#_Toc70943426)

[5 Vorgehensweise Informationssicherheitskonzept 2](#_Toc70943427)

[5.1 Organisatorische Maßnahmen 2](#_Toc70943428)

[5.2 Technische Maßnahmen 2](#_Toc70943429)

[6 Vorgehensweise Ausfallssicherheitskonzept 3](#_Toc70943430)

[6.1 Organisatorische Maßnahmen 3](#_Toc70943431)

[6.2 Technische Maßnahmen 3](#_Toc70943432)

# Zweck und Anwendungsbereich

Dieses Dokument regelt die Vorgehensweise für die Implementierung und regelmäßige Überwachung eines Datenschutz- und Informationssicherheitssystems für die Magaretner-Tagesklinik. 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.

# Geltungsbereich

Diese Verfahrensanweisung betrifft nur die Mitarbeiter der Firma ISMED, 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.

# Grundlagen

Da das Projekt im gesundheitlichen Sektor angesiedelt ist und es um den Schutz von Patientendaten geht, ist es wichtig, dass hierbei die DSGVO 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.

# Qualitätsmanagement

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).

# Vorgehensweise Informationssicherheitskonzept

## Organisatorische Maßnahmen

* Team bilden -> wöchentliche Meetings über Stand und Probleme
* Verwendung der CIA-Triade
* Prozesslandkarte einholen
* Prozesse priorisieren (Kritikalitätsanalyse)
* Gold bronze silber
* An Gesetze halten (DSGVO / NISG)

## Technische Maßnahmen

* Verschlüsselung der Daten -> kryptografische Verschlüsselungsmechanismen
* 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)

# Vorgehensweise Ausfallssicherheitskonzept

## Organisatorische Maßnahmen

* Prozesslandkarte einholen
* Prozesse priorisieren (gold silber bronze) -> Betrachtung der Ausfallzeiten (SLA)
* Implementierung eines Störfallprozesses (Störplan)
* Störfallmeldungsstelle errichten
* Störfallkatalog
* Notfallprozess -> dynamische Lage
* Notfallmanager
* Services stark einschränken
* CERT alamieren
* Disaster-Recovery-Plan
* Business-Continuity-Plan
* Qualitätsmanagement durchführen (PDCA)

## Technische Maßnahmen

* Backups ()
* Cloud-Lösungen (Daten werden nicht lokal gespeichert) -> müssen der DSGVO entsprechen
* Externes Rechenzentrum
* Notfallknöpfe in wichtigen Räumen
* Automatisierte Systemtests
* Hot cold warm standby (Ersatzgeräte)
* Notstromdiesel