

Datenschutz- und Informationssicherheitskonzept

|  |  |  |
| --- | --- | --- |
| **Version** | **Autor** | **Notiz** |
| 1.0 | David Stöger | Erstversion |
|  |  |  |
|  |  |  |

**Änderungshistorie**

Inhalt

[1 Zweck und Anwendungsbereich 1](#_Toc100178381)

[2 Geltungsbereich 1](#_Toc100178382)

[3 Grundlagen 2](#_Toc100178383)

[4 Qualitätsmanagement 2](#_Toc100178384)

[5 Vorgangsweise für das DISMS “Klinik-Wien-6-Tage” 3](#_Toc100178385)

[5.1 Prozessbeschreibung und Ablauf für Datenschutzrichtlinie 3](#_Toc100178386)

[5.2 Vorschlag der Datenschutzrichtlinie 4](#_Toc100178387)

[5.2.1 Rollenmodell 4](#_Toc100178388)

[5.2.2 Organisatorische und technische Vorgaben für Authentifizierung anhand der verschiedenen Rollen 5](#_Toc100178389)

[5.2.3 Spezielle Betrachtung von Home-Office und Telearbeiten 5](#_Toc100178390)

[6 Glossar 5](#_Toc100178391)

# Zweck und Anwendungsbereich

Dieses Dokument regelt die Vorgehensweise für den Prozess, der die Datenschutzrichtlinie (DS-Policy) erstellt, umsetzt, überprüft und verbessert. Um den Datenschutz 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. Hier vorallem die Dokumentenleitung wichtig. Was wollt ihr machen? Hoheiser gibt uns da Spielraum

# Geltungsbereich

Diese Richtlinie betrifft nur die Mitarbeiter der Firma Klinik-Wien-6-Tage. Da das Dokument internen Zwecken dient erschließt sich, dass es laut TLP gelb ist, und somit nur in der Firma nach dem „Need-to-know“-Prinzip verteilt werden darf. Dies gilt natürlich nur für das Konzept zur Erstellung und Umsetzung und nicht für öffentlichen Datenschutzrichtlinien des Dokuments.

# Grundlagen

Da die Firma hochsensible Patientendaten bearbeitet und speichert, müssen diese geschützt werden. Dabei ist es wichtig, dass hierbei die DSGVO sowie das NISG in Kraft tritt. Diese sollen bestmöglich geachtet und geschützt werden, um die Sicherheit der Patientendaten zu gewährleisten.

Ebenso sollen nicht alle Mitarbeiter Zugriff auf alle Daten und Systeme erhalten. Externer Zugriff auf Systeme soll hierbei gesondert betrachtet und gesichert werden. Abschließend gilt es noch den Hauptverantwortlichen des Dokuments zu ernennen, in diesem Fall: **Der CISO**

# 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 es wird 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) und neue Dokumentenversionen zu erstellen. Ebenso ist regelmäßig zu überprüfen, ob die Datenschutzrichtlinien eingehalten und beachtet werden.

Darüber hinaus soll das Dokument durch den zuständigen Juristen einmal jährlich überprüft und auf den neuersten Gesetzesstand gebracht werden. Weiters ist der Datenschutzbeauftragte dazu verpflichtet regelmäßig Protokolle über die Überprüfung und Aktualisierung der Richtlinie zu führen.

Folgende Abstände sind also zu beachten:

|  |  |  |
| --- | --- | --- |
| **Tätigkeit** | **Zeitrahmen** | **Verantwortliche Personen** |
| Risikoanalyse | Alle 3 Monate | CISO |
| Besprechungen zu neuen Bedrohungen und Miteinbeziehung selbiger | Alle 3 Monate | CISO, Datenschutzbeauftragter und ausgewählte Personen |
| Stichprobenartige Umsetzungs- und Einhaltungskontrolle | Alle 6 Monate | CISO, Datenschutzbeauftragter und Chefität |
| Aktualitätskontrolle Gesetz | Jedes Jahr | Jurist |

# Vorgangsweise für das DISMS “Klinik-Wien-6-Tage”

## Prozessbeschreibung und Ablauf für Datenschutzrichtlinie

* Teams bilden
* Basis-Checkliste des Österreichischen IT-Sicherheitshandbuches durchgehen (<https://www.sicherheitshandbuch.gv.at/downloads/Basis-Checkliste.pdf>)
* Daten analysieren und Kritikalität der einzelnen Bestandteile bei Verlust priorisieren
* Technische Gegebenheiten analysieren
* Sicherungskonzept überlegen
* DS-Policy erstellen
* Regelmäßige Bedrohungsanalysen
* Regelmäßig Gesetzesänderungen prüfen
* Verwendung der CIA-Triade
* An Gesetze halten (DSGVO / NISG)
* Qualitätsmanagement beachten

## Vorschlag der Datenschutzrichtlinie

### Rollenmodell

* Firmenstruktur überlegen:
  + Ärztinnen und Ärzte
  + Verwaltungspersonal
  + Technisches Personal
* **Anwendungsprogramme**:

Auf die Anwendungsprogramme sollten alle Mitarbeiter, welche diese Programme für ihre Arbeit brauchen oder sie warten, Zugriff erhalten. Dabei sollte ein Logging implementiert werden, um bei Datenverlust oder ähnlichem die Quelle finden zu können.

* **Systemprogramme**:

Auf die Systemprogramme sollen nur Mitarbeiter des technischen Personals Zugriff erhalten. Sie sollen wie in folgendem Punkt gesichert werden und es ist hier ebenso sinnvoll ein Logging zu implementieren.

|  |  |  |  |
| --- | --- | --- | --- |
| **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 |

### Organisatorische und technische Vorgaben für Authentifizierung anhand der verschiedenen Rollen

* 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 10-minütiger Inaktivität
* Geschütze Bildschirme (bei seitlicher Betrachtung kann ein Beobachter nichts sehen)

### 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

# Glossar

TLP…Traffic Light Protocol  
CISO…Chief Information and Security Manager  
DISMS…Datenschutz- und Informationssicherheitsmanagementsystem  
CIA-Triade…Confidentiality, Integrity and Availability