IT-Security-Dokumente nach Reifegradstufen

# Reifegradstufe 1: Basis

|  |  |  |
| --- | --- | --- |
| **Dokument** | **Zweck** | **Bemerkung** |
| Informationssicherheitsleitlinie | Bekennung der Geschäftsführung zur Umsetzung von IT-Sicherheit und Festlegung grundlegender Ziele, des Anwendungsbereichs, von Rollen und Aufgaben. | Dokumentvorlage in Anlage **Informationssicherheitsleitlinie**  Hilfestellung in Maßnahme 3.2 des Maßnahmenkatalogs |
| Dokumentation über IT-Sicherheitsvorfälle | Strukturierte Befassung mit und Erfassung von Sicherheitsvorfällen und ihre geeignete Dokumentation. | Dokumentvorlage in Anlage **Doku-Sicherheitsvorfälle**  Hilfestellung in Maßnahme 3.6 des Maßnahmenkatalogs |
| Risikoeinschätzung: Prozesseinschätzung | Definition der wichtigsten Prozesse im Krankenhaus. Jeder Prozess wird gemäß seiner Relevanz eingestuft; es werden grundlegende Überlegungen zum Ersatz oder Kompensation bei Ausfall definiert. | Dokumentvorlage in Anlage **Prozesseinschätzung**  Hilfestellung in Maßnahme 3.5 des Maßnahmenkatalogs |
| Grundlegende Notfallplanung und Betriebswiederherstellung | Für die wichtigsten Prozesse wird eine tiefergreifende Notfallplanung mit Maßnahmen zur Aufrechterhaltung des Betriebs erstellt. Außerdem grundlegende Überlegungen zur Wiederherstellung des Normalbetriebs des jeweiligen Prozesses. | Dokumentvorlage in Anlage **Richtlinie Sicherheitsvorfälle**  Hilfestellung in Maßnahme 3.7 des Maßnahmenkatalogs |
| Plan zur Mitarbeiterschulung | Awareness für IT-Sicherheit bei Mitarbeitern ist aufgrund der hohen Bedeutung möglichst früh herzustellen. In Phase 1 wird daher bereits ein Plan dafür angelegt, welcher über 1-2 Jahre laufen soll. | Dokumentvorlage in Anlage **Plan-Mitarbeiterschulung**  Hilfestellung in Maßnahmen 4.1-4.4 des Maßnahmenkatalogs |

# Reifegradstufe 2: Ausbau

|  |  |  |
| --- | --- | --- |
| **Dokument** | **Zweck** | **Bemerkung** |
| Sicherheitsrichtlinie Passwort | Festlegung krankenhausweit geeigneter Kriterien für sichere Passwörter anhand der Länge und Komplexität. Unterscheidung nach Bereich und Privilegien möglich. | *Dokumentvorlage in Anlage* ***Sicherheitsrichtlinie***  Hilfestellung in Maßnahme 3.4 des Maßnahmenkatalogs |
| Sicherheitsrichtlinie Backup | Festlegung von Kriterien geeigneter Backups, insb. Prozess, Häufigkeit, Art des Backups, Häufigkeit Wiedereinspielungs-Tests. | Dokumentvorlage in Anlage ***Sicherheitsrichtlinie***  Hilfestellung in Maßnahme 6.4 des Maßnahmenkatalogs |
| Sicherheitsrichtlinie Clean-Desk | Bestimmung zur sicheren Verwahrung und einem datenschutz-konformen Gebrauch von Dokumenten und Systemen. Insbesondere Anweisung zum Verschluss sensibler Dokumente nach Gebrauch. | Dokumentvorlage in Anlage ***Sicherheitsrichtlinie***  Hilfestellung in Maßnahme 3.4 des Maßnahmenkatalogs |
| Sicherheitsrichtlinie Informationsaustausch | Festlegung von Kriterien zum sicheren Austausch von Daten im Krankenhaus und darüber hinaus. Z.B. mit sicheren Kommunikationswegen, Kryptographie-Verfahren und Software-Werkzeugen | Dokumentvorlage in Anlage ***Sicherheitsrichtlinie***  Hilfestellung in Maßnahme 9.4 des Maßnahmenkatalogs |
| Sicherheitsrichtlinie Verhalten in Arbeitszonen | Festlegung von Verhalten der Mitarbeiter in physisch definierten Schutzzonen (z. B. öffentlicher Bereich, kontrollierter Bereich, usw.). | Dokumentvorlage in Anlage ***Sicherheitsrichtlinie***  Hilfestellung in Maßnahme 8.1 des Maßnahmenkatalogs |
| Sicherheitsrichtlinie Lieferanten und Dienstleister | Festlegung des Umgangs mit Dienstleistern unter Aspekten der IT-Sicherheit. Dazu zählen notwendige Vertragsklauseln, Schulungen, Richtlinien zum Informationsaustausch und die Überprüfung von Lieferanten. | Dokumentvorlage in Anlage ***Sicherheitsrichtlinie***  Hilfestellung in Maßnahme 9.5 des Maßnahmenkatalogs |
| Sicherheitsrichtlinie Telearbeit | Festlegung von Verfahren zum sicheren Umgang mit Systemen und Informationen bei Telearbeit (z. B. Home-Office). | Dokumentvorlage in Anlage ***Sicherheitsrichtlinie***  Hilfestellung in Maßnahme 9.2 des Maßnahmenkatalogs |
| Sicherheitsrichtlinie für Notfallplan | Festlegung von Inhalten und einem Prozess bei der Notfallplanungerstellung; bei bis dato bestehenden Notfallplänen werden hier oft Revisionen notwendig. | Dokumentvorlage in Anlage **Sicherheitsrichtlinie Notfallmanagement**  Hilfestellung in Maßnahme 3.7 des Maßnahmenkatalogs |
| Risikoeinschätzung: Asseteinschätzung | Festlegung wichtiger Assets, insbesondere in Bezug auf zuvor definierte kritische Prozesse im Krankenhausbetrieb. Zuweisung von Abhängigkeiten von Prozessen zu Assets sowie Einschätzung der Kritikalität der einzelnen Assets für darauf aufbauende Prozesse. | Dokumentvorlage in Anlage **Asseteinschätzung**  Hilfestellung in Maßnahme 3.5 des Maßnahmenkatalogs |

# Reifegradstufe 3: Überwachung und weitere Verbesserung

|  |  |  |
| --- | --- | --- |
| **Dokument** | **Zweck** | **Bemerkung** |
| Risikoeinschätzung: Bedrohungseinschätzung | Anlegen einer Sammlung potenzieller Bedrohungen, die die Zuverlässigkeit von Assets und Prozesse negativ beeinflussen. Sammeln möglicher Maßnahmen zur Absicherung gegen Bedrohungen (insb. präventiv und reagierend). | Dokumentvorlage in Anlage **Bedrohungseinschätzung**  Hilfestellung in Maßnahme 3.5 des Maßnahmenkatalogs |
| Sicherheitsrichtlinie für interne Audits | Festlegung eines einheitlichen Prozesses zur internen Auditierung. Dazu zählt die Planung von Audits, die Bestimmung neutraler Auditoren und die Durchführung von Audits. | Dokumentvorlage in Anlage ***Sicherheitsrichtlinie*** |