1. VERTRAULICHKEIT

1.1. Zutrittskontrolle

Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen

- ✓ Alarmanlage
- ✓ Sicherheitspersonal
- ✓ Schlüsselregelung
- ✓ Videoüberwachung der Zugänge
- ✓ Sicherheitsschlösser
- ✓ Personenkontrolle
- ✓ Berechtigungsausweise
- ✓ Protokollierung Besucher & Besucherbegleitung

1.2. Zugangskontrolle

Schutz vor unbefugter Systembenutzung

- ✓ rollenbasierte Zuordnung von Benutzerrechten
- ✓ Security Incident Management Security Operation Center
- ✓ sichere Kennwörter inkl. Passwortrichtlinie
- ✓ automatische Sperrmechanismen/ Bildschirmsperre
- ✓ Zwei-Faktor Authentifizierung

1.3. Zugriffskontrolle

Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

- ✓ Berechtigungskonzept „need to know“- Basis
- ✓ sichere Aufbewahrung von Datenträgern
- ✓ Protokollierung von Zugriffen
- ✓ Firewall
- ✓ Verschlüsselung von Datenträgern
- ✓ datenschutzkonforme Entsorgung der Datenträger und Protokollierung
- ✓ Verwaltung der Rechte durch Systemadministratoren
- ✓ Clear Screen, Clear Desk Policy
- ✓ Klassifikationsschema für Daten
- ✓ Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
- ✓ VPN-Technologie

2. INTEGRITÄT

2.1. Weitergabekontrolle

Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen bei Übermittlung

- ✓ verschlüsselte Datenübertragung
- ✓ sichere Transportbehältnisse
- ✓ Anti-Viren-Software
- ✓ Datenträgerverschlüsselung
- ✓ Intrusion-Detection-System
- ✓ Elektronische Signatur

2.2. Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

- ✓ Protokollierung
- ✓ Dokumentenmanagement

3. VERFÜGBARKEIT UND BELASTBARKEIT

3.1. Verfügbarkeitskontrolle

Schutz vor Zerstörung und Verlust von Daten

- ✓ Backup & Restore-Test
- ✓ Feuer- und Rauchmeldeanlagen
- ✓ unterbrechungsfreie Stromversorgung
- ✓ Recovery-Konzept/Wiederanlaufplan
- ✓ Löschungsfristen
- ✓ Klimaanlage
- ✓ Notfallvorsorgeplan/ Redundanzkonzepte
- ✓ Meldewege und Notfallpläne

4. VERFAHREN ZUR ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- ✓ Datenschutz-Management
- ✓ regelmäßige Mitarbeiterschulungen
- ✓ Sicherheitsmanagement
- ✓ Security Checks auf Infrastruktur- und Applikationsebene

5. SONSTIGE

- ✓ eindeutige Vertragsgestaltung
- ✓ formalisiertes Auftragsmanagement
- ✓ sorgfältige Auswahl von Dienstleistern
- ✓ Prüfung und Dokumentation von Sicherheitsmaßnahmen
- ✓ Verpflichtung auf Datengeheimnis (z.B. Mitarbeiter)
- ✓ Trennung von Produktiv- und Testsystem