

ANHANG 3: TECHNISCH-ORGANISATORISCHE MAßNAHMEN

ISO27001 Zertifizierung: <https://www.conova.com/iso-27001/>

Vertraulichkeit

- **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen mittels Videoüberwachungsanlagen, elektronischer Schließsysteme mit Zwei-Faktor-Authentifizierung (biometrischer Handvenenscanner und Schlüsselkarte), Alarmsysteme, rollenbasierter Zuordnung von Zutrittsberechtigungen, Protokollierung von Besuchern.
- **Zugangskontrolle:** Schutz vor unbefugter Systembenutzung mittels Kennwörter (einschließlich entsprechender Passwortrichtlinien), Zwei-Faktor-Authentifizierung (Smartcard und Passwort), automatischer Sperrmechanismen.
- **Zugriffskontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems mittels Standard-Berechtigungsprofile auf „need to do/know-Prinzip“, Firewall-Systeme mit rollenbasierten Berechtigungsprofilen auf „need to do/know-Prinzip“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodischer Überprüfung der vergebenen Berechtigungen.
- **Trennungskontrolle:** Trennung von Produktiv- und Testsystemen, physikalische Trennung von Systemen, Mandantenfähigkeit relevanter Systeme.
- **Klassifikationsschema für Informationen/Daten** (geheim/vertraulich/öffentlich).

Integrität

- **Weitergabekontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport mittels Verschlüsselung, Virtual Private Networks (VPN), elektronischer Signatur oder persönlicher Übergabe.

- **Eingabekontrolle:** Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, mittels Protokollierung.

Verfügbarkeitskontrolle, Belastbarkeit und Wiederherstellung der Verfügbarkeit

- Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust mittels online und offline Backup Systeme, Datensicherung in einem Ausweichrechenzentrum, Backup-Restore-Test auf System- und Datenebene, unterbrechungsfreier Stromversorgung (USV- und Notstromanlagen), Klimatisierungssysteme, Brandfrühesterkennungssysteme, Gaslöschsysteme, Redundanzkonzepte, Virenschutzsysteme, Firewallsysteme, DDoS-Angriffsschutz, Meldewege und Notfallpläne, Security Checks auf Infrastruktur- und Applikationsebene, Standardprozesse bei Eintritt, Wechsel und Ausscheiden von Mitarbeitern.
- **Löschfristen:** Sowohl für Daten selbst als auch Metadaten wie Logfiles.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutzmanagementsystem
- Informationssicherheitsmanagementsystem
- Incidentmanagementsystem
- Regelmäßige Mitarbeiter-Schulungen
- Verpflichtung auf Datengeheimnis
- Lieferantenbewertungssystem und Auftragskontrollsystem
- Prüfung und Dokumentation von Sicherheitsmaßnahmen
- Kontroll- und Auditrecht