



TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

VERTRAULICHKEIT

ZUTRITTSKONTROLLE

- Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch Zutrittskontrollsysteme und Videoüberwachung der Zugänge zu sensiblen Bereichen.
- Papierakten werden zusätzlich in versperrten Schränken aufbewahrt.
- Zugang zu sensiblen Bereichen für externe Personen erfolgt nur unter Aufsicht eines internen Mitarbeiters.

ZUGANGSKONTROLLE

- Rollen- oder personenbezogene Zugangsrechte, die auf personalisierten Accounts vergeben werden. Die Accounts sind durch Passwörter geschützt, deren Komplexität über Richtlinien gesteuert wird. Regelmäßige Änderung der Passwörter (spätestens nach 3 Monaten)
- Sperrmechanismen um Missbrauch oder Umgehung der Richtlinien vorzubeugen
- Verhaltensregeln zum sicheren Umgang mit Login-Daten
- Verhaltensregeln zum Umgang mit Mobile-Devices (z.B. automatische Displaysperre bei Inaktivität, verpflichtende Authentifizierung bei der Reaktivierung)

ZUGRIFFSKONTROLLE

- Rollen- oder personenbezogene Zugriffsrechte, die auf personalisierte Accounts vergeben werden.
- Rechte sollen auf Bedarfsbasis die Möglichkeiten zum Sichten, Anlegen, Lesen, Verändern, Kopieren und Entfernen regulieren.
- Periodische Prüfung der Zugriffsrechte

PROZESSTEST

- Sicherstellen, dass bei Produkt- und Softwaretests nur anonymisierte bzw. pseudonymisierte Daten verwendet werden, soweit diese Daten für Tests notwendig sind und dass die Daten nach Beendigung der Tests wieder entfernt werden.





NETZWERKSICHERHEIT

Schutz vor unbefugtem Zugriff auf netzwerketechnische Maßnahmen z.B. Firewall

INTEGRITÄT

KONTROLLE DER DATENÜBERMITTLUNG

- Datenübertragung nur über freigegebene Systeme, Medien und Applikationen
- Externer Zugriff nur über gesicherte VPN-Verbindungen

PROTOKOLLIERUNG VON DATENEINGABE UND VERÄNDERUNG

- Über Logfiles oder sonstige Protokollierungen

KONTROLLE BEI FERNZUGRIFF

- Fernzugriff nur nach Bestätigung des für die Hardware Verantwortlichen
- Zugriff nur über geprüfte und freigegebene Mittel

VERFÜGBARKEIT

BACKUP-SYSTEME

- Systeme zum sicheren Erstellen von Backups
- Sichere Aufbewahrung der Backup-Dateien
- Schutz vor unbefugtem Zugriff, Veränderung, Löschung der Backupdateien

SCHUTZ GEGEN SYSTEMAUSFALL

Schutz der Systeme gegen infrastrukturelle Ausfälle (z.B. Energieversorgung, Datenleitung...)

BAULICHE ABSICHERUNG

Bauliche Absicherung der primären Datenverarbeitungssysteme (z.B. Server) gegen äußere Einwirkungen (z.B. Naturkatastrophen, Infrastrukturschäden)

PROZESS ZUR WIEDERHERSTELLUNG

Definierter Wiederherstellungsprozess, um eine schnelle und akkurate Datenwiederherstellung zu gewährleisten

PSEUDONYMISIERUNG

Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt und gesondert aufbewahrt

VERSCHLÜSSELUNG

INTEGRIERTE DATENTRÄGER

Verschlüsselung interner Datenträgern von Systemen, die außerhalb der gesicherten Arbeitsumgebung (z.B. Büro) verwendet werden.





SONSTIGE DATENTRÄGER

Schutz von Dateien, die personenbezogene Daten enthalten, durch Passwortauthentifizierung bzw. Verschlüsselung.

REGELUNG DER ARBEITSWEISE

INTERNE RICHTLINIEN

- Richtlinien zum allgemeinen Umgang mit personenbezogenen Daten
- Explizite Richtlinien zum Umgang mit Daten bei Vorgängen, die ein hohes Risiko für Betroffene darstellen können.

REGELMÄSSIGE SCHULUNGEN ZUM DATENSCHUTZ

Regelmäßige Schulungen aller Mitarbeiter, die mit der Verarbeitung von personenbezogenen Daten zu tun haben.

UMGANG MIT MÖGLICHEN DATENLECKS

NOTFALLPLAN DATENLECK

Notfallplan, um im Anlassfall eine schnellere Reaktion zuzulassen um:

- Datenlecks zu schließen
- Auswirkungen für Betroffene zu vermeiden/zu minimieren
- Zu bestimmen, ob Betroffene und/oder die Datenaufsichtsbehörde informiert werden müssen und diese Meldungen durchzuführen.
- Maßnahmen zu setzen, um erneute Datenlecks zu vermeiden.

EVALUIERUNGSMASSNAHMEN

INTERNE AUDITS

Regelmäßige Durchführung interner Audits, um die Angemessenheit und Aktualität der einzelnen Schutzmaßnahmen zu gewährleisten.

AKTIVES FEEDBACK

Mitarbeiter und Partner werden ermutigt, Meldungen über vermutete Systeme und Situationen, die zu Datenschutzverletzungen führen könnten, sowie Verbesserungsvorschläge zum allgemeinen Datenschutz jederzeit, auf Wunsch auch anonym, einzubringen.

