Technisch und organisatorische Massnahmen AGIBA IT Services AG (intern und Rechenzentren)

Zweck

Definition der technisch-organisatorischen Massnahmen für Auftragsverarbeitungsverträge und andere Zwecke.

Für die AGIBA IT Services AG

1 Zutrittskontrolle

- Manuelle Türsicherung durch Sicherheitsschlösser
- Schlüsselregelung mit Dokumentation der Schlüsselübergabe und -berechtigungen der Schlüssel
- Sicherer Serverraum (eigene Zone, Zugang geregelt)
- Besucherkontrolle
- Sorgfältige Auswahl von Reinigungspersonal

2 Zugangskontrolle

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername und Passwort und zusätzlich 2-Faktorauthentifizierung am Unternehmensnetzwerk und weiteren sensiblen Systemen
- Gebäudeverriegelung mit Sicherheitsschlössern
- Einsatz einer Firewall
- Einsatz von Anti-Viren Software
- Einsatz von Crypto Spike (Ransomware)

3 Zugriffskontrolle

- Anwendung eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministratoren und Applikationsadministratoren
- Anzahl der Administratoren auf das «Notwendigste» reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen und Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Verschlüsselung von Datenträgern
- Sichere Aufbewahrung von Datenträgern
- Ordnungsgemässe Vernichtung von Datenträgern
- Einsatz von Aktenvernichtern für Papierdokumente

4 Weitergabekontrolle

- gesichertes WLAN
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Protokollierung
- getunnelte bzw. verschlüsselte Datenverbindungen
- Sicherer Transport von Datenträgern

5 Eingabekontrolle

- limitierte Vergabe von Zugriffsrechten
- systemseitige Protokollierung insbesondere für die Eingabe, Änderung und Löschung von Daten
- Berechtigungsvergabe zum Zugriff auf Protokollierungen
- dokumentierte Zuweisung von Berechtigungen und Rollen
- Prozesse zur Aufrechterhaltung der Aktualität von Daten
- Festlegung des Sollverhaltens von Prozessen und regelmässiges Durchführen von Tests zur Feststellung und Dokumentation der Funktionalität, von Risiken, sowie Sicherheitslücken

6 Auftragskontrolle

- schriftlicher Vertrag zur Auftragsdatenverarbeitung mit Auftragnehmern
- Verpflichtung der Mitarbeiter zur unbedingten Einhaltung des Datengeheimnisses
- Überprüfung der Dienstleister

7 Verfügbarkeitskontrolle

- Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien (Back-up-Konzept)
- Schutz vor äusseren Einflüssen, u.a. durch Schadsoftware, Sabotage, höhere Gewalt
- unterbrechungsfreie Stromversorgung
- Redundanz von Hard- und Software, sowie Infrastruktur
- Vertretungsregeln für abwesende Mitarbeiter
- Notfallplan (BCM)
- Verschlüsselte Online-Backups
- Feuer- und Rauchmeldeanlage

8 Trennungskontrolle

- Getrennte Anwendungen und Datenbanken und getrennte Speicherung (je nach Schutzbedarf, Zweckbindung)
- Zugriffsberechtigungen für getrennte Datenbanken und Module der Datenbanken
- Trennung durch Zugriffsregelungen
- Protokollierung der Zugriffe
- Funktionstrennung (Trennung von Produktions-, Test- und Entwicklungsumgebungen)
- Anonymisierung von Daten zu Entwicklungszwecken

Die Rechenzentren

In allen unseren Rechenzentren gilt folgendes:

1 Zutrittskontrolle für Rechenzentren

- Absicherung von Gebäudeschächten
- Automatisches Zugangskontrollsystem
- Chipkarten-/Transponder-Schliesssystem
- Biometrische Zugangssperre
- Videoüberwachung der Zugänge
- Alarmanlage
- Lichtschranken/Bewegungsmelder
- Sicherheitsschlösser
- Schlüsselregelung
- Personenkontrolle beim Empfang
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal
- Tragepflicht von Berechtigungsausweisen

2 Zugangskontrolle für Rechenzentren

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername/Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Gehäuseverriegelungen
- Einsatz von VPN-Technologie
- Einsatz einer Hardware-Firewall
- Sicherheitsschlösser
- Einsatz von Intrusion-Detection-Systemen
- Verschlüsselung von mobilen Datenträgern
- Einsatz von Anti-Viren-Software
- Verschlüsselung von Datenträgern in Laptops/Notebooks
- Einsatz einer Software-Firewall

7 Verfügbarkeitskontrolle für Rechenzentren

- Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie, unterbrechungsfreie Stromversorgung, Virenschutz, Firewall, Meldewege und Notfallpläne.
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)
- Feuer- und Rauchmeldeanlagen