Checkliste
Vorab-Erfassung Technische und organisatorische Maßnahmen
ISO 27001:2013

Diese Checkliste erfasst technische und organisatorischen Maßnahmen im Rahmen der Informationssicherheit, um möglichst schnell ein Überblick über die bereits im Unternehmen umgesetzten und etablierten Maßnahmen zu erhalten.

Die abgefragten Punkte ergeben sich aus der ISO 27001:2013, Anhang A:

A.8 Verwaltung der Werte
A.9 Zugangssteuerung
A.10 Kryptographie
A.11 Physische und umgebungsbezogene Sicherheit
A.12 Betriebssicherheit
A.13 Kommunikationssicherheit

Die Regelungen und Richtlinien sollten bereits als dokumentierte Information vorliegen. Dies gilt auch für die Nachweise von Prüfungen und Schulungen.

Zutrittskontrolle

Technische Maßnahmen

- ☐ Definierte Sicherheitszonen
- ☐ Zutrittskontrollsystem
- ☐ Alarmanlage
- ☐ Videoüberwachung
- ☐ Sicherheitstüren

Organsatorische Maßnahmen

- ☐ Pförtner / Überwachter Eingangsbereich
- ☐ Regelungen für Besucher/Lieferanten
- ☐ Regelungen für Mitarbeiterausweise
- ☐ Regelungen zur Videoüberwachung
- ☐ Sensibilisierung und Schulung von Mitarbeitern
- ☐ Regelung für die Vergabe und Kontrolle von Zutrittsberechtigungen
- ☐ Regelmäßige Prüfung von Zutrittsprotokollen und Notwendigkeit von Zutrittsberechtigungen

Zugriffskontrolle / Vertraulichkeit

Technische Maßnahmen

- ☐ Firewalls
- ☐ Verschlüsselung von Datenträgern und Systemen
- ☐ Virtual Private Networks

Organsatorische Maßnahmen

- ☐ Richtlinie zur Benutzerverwaltung und Rechtevergabe
- ☐ Passwortrichtlinie
- ☐ Regelungen zum Einsatz von Kryptographie
- ☐ Regelungen für die Nutzung des Internet am Arbeitsplatz
- ☐ Regelungen für das Sperren/ Herunterfahren des Arbeitsplatzrechners bei Nicht-Nutzung
- ☐ Regelungen für die Nutzung/ Außerbetriebnahme von externen Datenträgern, Notebooks, mobilen Geräten und Arbeitsplatzrechnern
- ☐ Regelmäßige Prüfung von Zugriffsprotokollen und Notwendigkeit von Benutzerrechten

---

Integrität

Technische Maßnahmen

- ☐ Einsatz von Virus und Malware-Schutzprogrammen
- ☐ Patch- und Schwachstellenmanagement

Organsatorische Maßnahmen

- ☐ Regelungen für die Installation von Betriebssystemen und Anwendersoftware

---

Verfügbarkeit

Technische Maßnahmen

- ☐ Feuer- und Rauchmeldeanlagen in Serverräumen/kritischen Gebäudeteilen
- ☐ Automatischen Löschanlagen in Serverräumen
- ☐ Feuerlöschgeräte
- ☐ Klimaanlagen in Serverräumen
- ☐ Unterbrechungsfreie Stromversorgung (USV)
- ☐ Steckdosen mit Schutzkontakt
- ☐ Angepasste Aufteilung der Stromkreise für Serverräume

Organsatorische Maßnahmen

- ☐ Regelungen für Datensicherung und Wiederherstellung
- ☐ Regelungen für "Off-Site"-Backup
- ☐ Notfallplan
- ☐ Regelmäßgie Schulungen und Übungen für die Ausführung des Notfallplans
- ☐ Regelmäßige Tests der Datenwiederherstellung
- ☐ Regelungen für den Brandfall/ Brandschutzübungen
- ☐ Regelmäßige Prüfung der technischen Anlagen