Dokumente nach DIN/ISO 27001

Diese Liste bietet eine gute Übersicht über die zu erstellenden Dokumente, erhebt aber keinen Anspruch auf Vollständigkeit und wird ständig überarbeitet.
Die Dokumente müssen nicht einzeln gehalten werden, sondern können durchaus zusammengefasst sein. Es sollte beachtet werden, dass die Dokumente gelenkte Dokumente.

Erforderliche Dokumente:

- ☐ Anwendungsbereich von ISMS (Normkapitel 4.3)
- ☐ Informationssicherheitspolitik und Ziele (Normkapitel 5.2 und 6.2)
- ☐ Risikobewertungs- und Risikobehandlungsmethodik (Normkapitel 6.1.2)
- ☐ Anwendbarkeitserklärung (Normkapitel 6.1.3 d)
- ☐ Risikobehandlungsplan (Normkapitele 6.1.3 e und 6.2)
- ☐ Risikobewertungsbericht (Normkapitel 8.2)
- ☐ Definition der Sicherheits-Rollen und Verantwortlichkeiten (Normkapitel A.7.1.2, A.13.2.4)
- ☐ Verzeichnis der Assets (Normkapitel A.8.1.1)
- ☐ Akzeptable Nutzung von Assets (Normkapitel A.8.1.3)
- ☐ Richtlinie für Zugriffskontrolle (Normkapitel A.9.1.1)
- ☐ Betriebsverfahren für das IT-Management (Normkapitel A.12.1.1)
- ☐ Prinzipien des sicheren System Engineering (Normkapitel A.14.2.5)
- ☐ Sicherheitspolitik für Lieferanten (Normkapitel A.15.1.1)
- ☐ Incident Management-Verfahren (Normkapitel A.16.1.5)
- ☐ Verfahren für betriebliche Kontinuität (Normkapitel A.17.1.2)
- ☐ Gesetzliche, behördliche und vertragliche Anforderungen (Normkapitel A.18.1.1)

Erforderliche Aufzeichnungen:

- ☐ Aufzeichnungen über Schulungen, Fähigkeiten, Erfahrung & Qualifikationen (Normkapitel 7.2)
- ☐ Überwachungs- und Messergebnisse (Normkapitel 9.1)
- ☐ Internes Audit-Programm (Normkapitel 9.2)
- ☐ Ergebnisse interner Audits (Normkapitel 9.2)
- ☐ Ergebnisse aus Managementbewertungen (Normkapitel 9.3)
- ☐ Ergebnisse von Korrekturmaßnahmen (Normkapitel 10.1)
- ☐ Protokolle über Anwenderaktivitäten, Ausnahmen und Sicherheitsereignisse (Normkapitel A.12.4.1 und A.12.4.3)

Zusätzliche Dokumente:

- ☐ Verfahren zur Lenkung von Dokumenten (Normkapitel 7.5)
- ☐ Verwaltung von Aufzeichnungen (Normkapitel 7.5)
- ☐ Verfahren für interne Audits (Normkapitel 9.2)
- ☐ Verfahren für Korrekturmaßnahmen (Normkapitel 10.1)
- ☐ Bring Your Own Device (BYOD)-Richtlinie (Normkapitel A.6.2.1)
- ☐ Richtlinie für Mobilgeräte und Telearbeit (Normkapitel A.6.2.1)

- ☐ Richtlinie zur Informationsklassifizierung (Normkapitel A.8.2.1, A.8.2.2, A.8.2.3)
- ☐ Passwort-Richtlinie (Normkapitele A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3)
- ☐ Richtlinie für Entsorgung und Vernichtung (Normkapitel A.8.3.2, A.11.2.7)
- ☐ Verfahren für Arbeiten in Sicherheitsbereichen (Normkapitel A.11.1.5)
- ☐ Clear Desk und Clear Screen-Richtlinie (Normkapitel A.11.2.9)
- ☐ Change Management-Richtlinie (Normkapitel A.12.1.2 und A.14.2.4)
- ☐ Backup-Richtlinie (Normkapitel A.12.3.1)
- ☐ Richtlinie für Informationstransfer (Normkapitel A.13.2.1, A.13.2.2, A.13.2.3)
- ☐ Geschäftsauswirkungsanalyse (Normkapitel A.17.1.1)
- ☐ Übungs- und Testplan (Normkapitel A.17.1.3)
- ☐ Wartungs- und Überprüfungsplan (Normkapitel A.17.1.3)
- ☐ Strategie für betriebliche Kontinuität (Normkapitel A.17.2.1)