

IT-Sicherheitskonzept gemäß ISO 27001

Inhaltsverzeichnis

Prüfung und Freigabe	2
Änderungshistorie	3
Dokumentensteuerung und Verteilerkreis	4
1 Relevante Normen und Standards	7
2 Abkürzungen	7
3 Begriffe	7
4 Das Informationssicherheitsmanagementsystem	8
4.1 Management und Steuerung des ISMS	10
5 Kontext der Organisation	12
5.1 Verstehen der Organisation und Ihres Kontextes	12
5.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien	13
5.2.1 Rechtliche und vertragliche Anforderungen (IT-Compliance)	14
5.3 Festlegung des Anwendungsbereichs des Informationssicherheitsmanagementsystems	15
5.3.1 Anwendungsbereich des Informationssicherheitsmanagementsystems	15
6 Führung	17
6.1 Führung und Verpflichtung	17
6.2 Strategie für das Management und die Steuerung des ISMS	18
6.2.1 Festlegung der Strategie für die Informationssicherheit	19
6.2.2 Bekanntmachung der Strategien für die Informationssicherheit	19
6.2.3 Leitlinie zur Informationssicherheit	19
6.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	20
7 Planung und Steuerung des ISMS	22
7.1 Umgang mit Risiken	23
7.2 Festlegung von Zielen für die Umsetzung, Aufrechterhaltung und Verbesserung der Informationssicherheit	24
7.3 Planung von Änderungen am ISMS	25
8 Unterstützung des Betriebs des ISMS	27
8.1 Ressourcen	28
8.2 Kompetenzen	29
8.2.1 Kompetenzen der beteiligten Personen für den Betrieb des ISMS	29
8.2.2 Kompetenzen der Organisation für den Betrieb des ISMS	30
8.3 Awareness, Schulung und Unterweisung	32
8.4 Interne und externe Kommunikation	32
8.5 Dokumentierte Information	33
8.5.1 Erstellen und Aktualisieren	35
8.5.2 Lenkung dokumentierter Informationen	35
9 Betrieb des ISMS	36
9.1 Planung und Steuerung der Informationssicherheit	37

9.2 Schutzbedarfsfeststellung.....	38
9.2.1 Informationssicherheitsrisikobeurteilung.....	40
9.2.2 Informationssicherheitsrisikobehandlung.....	43
9.2.2.1 Umsetzung der Maßnahmen aus der Informationssicherheitsrisikobehandlung.....	45
10 Bewertung der Leistung des ISMS.....	48
10.1 Überwachung und Messung.....	48
10.2 Analyse und Bewertung.....	50
10.3 Internes Audit.....	50
10.3.1 Auditprogramme.....	52
10.4 Managementbewertung.....	53
10.4.1 Eingaben für die Managementbewertung.....	54
10.4.2 Ergebnisse der Managementbewertung.....	56
11 Verbesserung des ISMS.....	58
11.1 Fortlaufende Verbesserung.....	59
11.2 Nichtkonformität und Korrekturmaßnahmen.....	60
12 Liste der Verfahren und mitgeltenden Dokumentationen für die Umsetzung, die Aufrechterhaltung und die fortlaufende Verbesserung der Informationssicherheit.....	62