solira

Benötigte Dokumente und Nachweise (Records) basierend auf **ISO/IEC 27001:2017-5**

Mindest Dokumentationsanforderungen	ISO 27001:2017-5 Kapitel	Bemerkung
Anwendungsbereich des Informationssicherheits-managementsystems	4.3	Der Anwendungsbereich des ISMS muss als dokumentierte Information verfügbar sein.
IS Politik und IS Ziele	5.2, 6.2	Die Informationssicherheitspolitik sowie die Informationssicherheitsziele müssen als dokumentierte Information verfügbar sein.
Informationssicherheits-risikobeurteilung	6.1.2	Die Organisation muss dokumentierte Information über den Informationssicherheitsrisiko Beurteilungsprozess aufbewahren.
Erklärung zur Anwendbarkeit	6.1.3 d)	Eine Erklärung zur Anwendbarkeit muss erstellt werden.
Informationssicherheits-risikobehandlung	6.1.3 e), 6.2	Die Organisation muss dokumentierte Information über den Informationssicherheitsrisiko Behandlungsprozess aufbewahren.
Kompetenz	7.2	Nachweis der geforderten Sicherheitskompetenz der Mitarbeiter muss dokumentiert werden.
Dokumentierte Information	7.5	Das Informationssicherheits-Managementsystem der Organisation muss sowohl die von dieser Internationalen Norm geforderte dokumentierte Information beinhalten wie auch Information, welche die Organisation als notwendig für die Wirksamkeit des Managementsystems bestimmt hat.
Lenkung dokumentierter Information	7.5.3	Dokumentierte Information, welche notwendig für Planung und Betrieb des Informationssicherheits-Managementsystems ist, muss angemessen gekennzeichnet und gelenkt werden.

Betriebliche Planung und Steuerung	8.1	Die Organisation muss dokumentierte Information im notwendigen Umfang aufbewahren, so dass die Prozesse wie geplant umgesetzt werden können.
Informationssicherheits-risikobeurteilung	8.2	Die Organisation muss dokumentierte Information über die Ergebnisse der Informationssicherheits Risikobeurteilungen aufbewahren.
Informationssicherheits-risikobehandlung	8.3	Die Organisation muss dokumentierte Information über die Ergebnisse der Informationssicherheits Risikobehandlung aufbewahren.
Bewertung der Leistung	9.1	Die Organisation muss geeignete dokumentierte Information als Nachweis der Ergebnisse der Managementbewertung aufbewahren.
Internes Audit	9.2	Die Organisation muss Information als Nachweis des Auditprogramms und der Ergebnisse der Audits aufbewahren.
Managementbewertung	9.3	Die Organisation muss dokumentierte Information als Nachweis der Ergebnisse der Managementbewertung aufbewahren.
Verbesserung	10.1	Die Organisation muss dokumentierte Information als Nachweis der Nichtkonformität und der entsprechenden Korrekturmassnahmen sowie der Ergebnisse jeder Korrekturmassnahme aufbewahren.
Beschäftigungs- und Vertragsbedingungen	A.7.1.2, A.13.2.4	In den vertraglichen Vereinbarungen mit Beschäftigten und Auftragnehmern sind deren Verantwortlichkeiten und diejenigen der Organisation festgelegt.
Verwaltung der Werte	A.8.1.1	Information und andere Werte, die mit Information und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, sind erfasst und ein Inventar dieser Werte ist erstellt und wird gepflegt.
Verwaltung der Werte	A.8.1.3	Regeln für den zulässigen Gebrauch von Information und Werten, die mit Information und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, sind aufgestellt, dokumentiert und angewendet.

Geschäftsanforderungen an die Zugangssteuerung	A.9.1.1	Eine Zugangssteuerungsrichtlinie ist auf Grundlage der geschäftlichen und sicherheitsrelevanten Anforderungen erstellt, dokumentiert und überprüft.
Betriebsabläufe und -verantwortlichkeiten	A.12.1.1	Die Bedienabläufe sind dokumentiert und allen Benutzern, die sie benötigen, zugänglich.
Protokollierung und Überwachung	A.12.4.1, A.12.4.3	Ereignisprotokolle, die Benutzertätigkeiten, Ausnahmen, Störungen und Informationssicherheitsvorfälle aufzeichnen, werden erzeugt, aufbewahrt und regelmässig überprüft.
Informationsübertragung	A.13.2.4	Anforderungen an Vertraulichkeits- oder Geheimhaltungsvereinbarungen, werden identifiziert, regelmässig überprüft und sind dokumentiert.
Sicherheit in Entwicklungs- und Unterstützungsprozessen	A.14.2.5	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme sind festgelegt, dokumentiert, werden aktuell gehalten.
Informationssicherheit in Lieferantenbeziehungen	A.15.1.1	Die Informationssicherheitsanforderungen im Zusammenhang mit dem Zugriff von Lieferanten auf Werte der Organisation werden mit dem Zulieferer vereinbart und sind dokumentiert.
Handhabung von Informationssicherheits-vorfällen und Verbesserungen	A.16.1.5	Auf Informationssicherheitsvorfälle wird entsprechend den dokumentierten Verfahren reagiert.
Aufrechterhalten der Informationssicherheit	A.17.1.2	Die Organisation dokumentiert Prozesse, Verfahren und Massnahmen um das erforderliche Niveau an Informationssicherheit in einer widrigen Situation aufrechterhalten zu können.
Einhaltung gesetzlicher und vertraglicher Anforderungen	A.18.1.1	Alle relevanten gesetzlichen, regulatorischen, selbstauferlegten oder vertraglichen Anforderungen sowie das Vorgehen der Organisation zur Einhaltung dieser Anforderungen sind dokumentiert.

Üblicherweise verwendete **nicht obligatorische Dokumentation**

Dokumente	Referenz Norm
Verfahren für die Dokumentenlenkung	7.5
Vorgaben für die Verwaltung von Datensätzen	7.5
Vorgabe für die Durchführung von internen Audits	9.2
Verfahren für die Umsetzung von Korrekturmassnahmen	10.1
Weisungen für Mobilgeräte und Telearbeit	A.6.2.1
Weisung für die Klassifizierung und den Umgang mit klassifizierten Werten (Transport, Speicherung, Vernichtung etc.)	A.8.2.1, A.8.2.2, A.8.2.3
Passwort policy	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
Weisung für das Arbeiten in Sicherheitsbereichen	A.11.1.5
Clear desk and clear screen policy	A.11.2.9
Change management policy	A.12.1.2, A.14.2.4
Backup policy	A.12.3.1
Sicherheitsvorgaben bei Business Continuity Plänen	A.17.1.3