**CHECKLISTENVORLAGE FÜR ISO 27001 CONTROLS **

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ABSCHNITT/ KATEGORIE** | **ANFORDERUNG/AUFGABE** | **ZUGEWIESEN ZU** | **KONFORM?** | **ZULETZT AKTUALISIERT AM** |
| ***5. Informationssicherheitsrichtlinien*** |
| 5.1 | Es gibt Sicherheitsrichtlinien. |   |   |   |
| 5.2 | Alle Richtlinien wurden vom Management genehmigt. |   |   |   |
| 5.3 | Nachweis für Compliance. |   |   |   |
| ***6. Organisation der Informationssicherheit*** |
| 6.1 | Rollen und Verantwortlichkeiten wurden definiert. |   |  |  |
| 6.2 | Trennung von Aufgaben definiert. |   |  |  |
| 6.3 | Verifizierungsstelle / Behörde zur Überprüfung der Compliance kontaktieren. |   |  |  |
| 6.4 | Kontakt zu speziellen Interessengruppen bezüglich Compliance herstellen |   |  |  |
| 6.5 | Nachweis der Informationssicherheit im Projektmanagement. |   |  |  |
| 6.6 | Richtlinie für Mobilgeräte definieren |   |  |  |
| 6.7 | Richtlinie für Remote-Arbeit festgelegen. |   |  |  |
| ***7. Sicherheit im Personalwesen*** |
| 7.1 | Richtlinie für die Überprüfung von Mitarbeitern vor der Anstellung definieren |   |  |  |
| 7.2 | Richtlinie für HR-Bedingungen und -Beschäftigungsverhältnisse definieren |   |  |  |
| 7.3 | Richtlinien für Verantwortlichkeiten des Managements definieren.  |   |  |  |
| 7.4 | Richtlinien für das Bewusstsein für Informationssicherheit, Bildung und Schulung. |   |  |  |
| 7.5 | Richtlinien für Disziplinarverfahren in Bezug auf die Informationssicherheit definieren. |   |  |  |
| 7.6 | Richtlinien für die Beendigung oder den Wechsel des Arbeitsverhältnisses in Bezug auf die Informationssicherheit definieren. |   |  |  |
| ***8. Asset-Management*** |
| 8.1 | Vollständige Bestandsliste der Assets. |   |  |  |
| 8.2 | Vollständige Eigentümerliste für Assets. |   |  |  |
| 8.3 | Richtlinie zur „zulässigen Nutzung“ von Assets definieren. |   |  |  |
| 8.4 | Richtlinie für die Rückgabe von Assets definieren. |   |  |  |
| 8.5 | Richtlinie zur Klassifizierung von Informationen definieren.  |   |  |  |
| 8.6 | Richtlinie für die Kennzeichnung von Informationen definieren. |   |  |  |
| 8.7 | Richtlinie für den Umgang mit Assets definieren. |   |  |  |
| 8.8 | Richtlinien für den Umgang mit Wechselmedien definieren. |   |  |  |
| 8.9 | Richtlinie für die Entsorgung von Medien definieren. |   |  |  |
| 8.10 | Richtlinie für die Übertragung physischer Datenträger definieren. |   |  |  |
| ***9. Zugriffskontrolle*** |
| 9.1 | Richtlinie für die An- und Abmeldung von Benutzer-Assets definieren. |   |  |  |
| 9.2 | Richtlinie für die Bereitstellung des Benutzerzugriffs definieren. |   |  |  |
| 9.3 | Richtlinie für die Verwaltung privilegierter Zugriffsrechte definieren. |   |  |  |
| 9.4 | Richtlinie für die Verwaltung von geheimen Authentifizierungsinformationen der Benutzer definieren. |   |  |  |
| 9.5 | Richtlinie zur Überprüfung der Benutzerzugriffsrechte definieren. |   |  |  |
| 9.6 | Richtlinie für die Entfernung oder Anpassung von Zugriffsrechten definieren. |   |  |  |
| 9.7 | Richtlinie zur Nutzung von geheimen Authentifizierungs-informationen definieren. |   |  |  |
| 9.8 | Richtlinie zur Beschränkung des Zugriffs auf Informationen definieren. |   |  |  |
| 9.9 | Richtlinie für sichere Anmeldeverfahren definieren. |   |  |  |
| 9.10 | Richtlinie für Kennwortmanage-mentsysteme definieren. |   |  |  |
| 9.11 | Richtlinie für die Verwendung von privilegierten Dienstprogrammen definieren. |   |  |  |
| 9.12 | Richtlinie für die Steuerung des Zugriffs auf Programmquellcode definieren. |   |  |  |
| ***10. Kryptografie*** |
| 10.1 | Richtlinie zur Verwendung kryptografischer Steuerungen definieren. |   |  |  |
| 10.2 | Richtlinien für das Schlüssel-management definieren. |   |  |  |
| ***11. Physische und Umgebungssicherheit*** |
| 11.1 | Richtlinien für physische Sicherheitsbereiche definieren. |   |  |  |
| 11.2 | Richtlinie für physische Zugangskontrollen definieren. |   |  |  |
| 11.3 | Richtlinien für die Absicherung von Büros, Räumen und Anlagen definieren. |   |  |  |
| 11.4 | Richtlinien zum Schutz gegen externe und Umweltbe-drohungen definieren. |   |  |  |
| 11.5 | Richtlinie für die Arbeit in sicheren Bereichen definieren. |   |  |  |
| 11.6 | Richtlinien für Liefer- und Ladebereiche definieren. |   |  |  |
| 11.7 | Richtlinien für die Standortwahl und Schutz der Ausrüstung definieren. |   |  |  |
| 11.8 | Richtlinie für Hilfsversorgungseinrichtungen definieren. |   |  |  |
| 11.9 | Richtlinie für die Verkabelungssicherheit definieren. |   |  |  |
| 11.10 | Richtlinie für die Gerätewartung definieren. |   |  |  |
| 11.11 | Richtlinie für das Entfernen von Assets definieren. |   |  |  |
| 11.12 | Richtlinie für die Sicherheit von Ausrüstung und Assets definieren, die nicht vor Ort sind. |   |  |  |
| 11.13 | Sichere Entsorgung oder Wiederverwendung von Ausrüstung. |   |  |  |
| 11.14 | Richtlinie für unbeaufsichtigte Benutzerausrüstung definieren. |   |  |  |
| 11.15 | Richtlinie für Clear Desk- und Clear-Screen-Richtlinien definieren. |   |  |  |
| ***12. Betriebssicherheit*** |
| 12.1 | Richtlinie für dokumentierte Betriebsabläufe definieren. |   |  |  |
| 12.2 | Richtlinien für das Changemanagement definieren. |   |  |  |
| 12.3 | Richtlinien für das Kapazitätsmanagement definieren. |   |  |  |
| 12.4 | Richtlinien für die Trennung von Entwicklungs-, Test- und Betriebsumgebungen definieren. |   |  |  |
| 12.5 | Richtlinien für Malware-Kontrolle definieren. |   |  |  |
| 12.6 | Richtlinie für die Sicherung von Systemen definieren. |   |  |  |
| 12.7 | Richtlinie für die Sicherung von Informationen definieren. |   |  |  |
| 12.8 | Richtlinie für die Ereignispro-tokollierung definieren. |   |  |  |
| 12.9 | Richtlinie zum Schutz von Protokollinformationen definieren. |   |  |  |
| 12.10 | Richtlinie für Administratoren- und Bedienerprotokoll definieren. |   |  |  |
| 12.11 | Richtlinie für die Uhrsynchronisierung definieren. |   |  |  |
| 12.12 | Richtlinie für die Installation von Software in betrieblichen Systemen definieren. |   |  |  |
| 12.13 | Richtlinie für die Verwaltung technischer Schwachstellen definieren. |   |  |  |
| 12.14 | Richtlinie für die Einschränkung von Softwareinstallationen definieren. |   |  |  |
| 12.15 | Richtlinie für die Kontrolle von Informationssystem-Audits definieren. |   |  |  |
| ***13. Kommunikationssicherheit*** |
| 13.1 | Richtlinie für Netzwerksteuerung definieren. |   |  |  |
| 13.2 | Richtlinie für die Sicherheit von Netzwerkdiensten definieren. |   |  |  |
| 13.3 | Richtlinie für die Trennung von Netzwerken definieren. |   |  |  |
| 13.4 | Richtlinie für Richtlinien und Vorgehensweisen bei Informationsübertragungen definieren. |   |  |  |
| 13.5 | Richtlinien für Vereinbarungen zur Informationsübertragung definieren. |   |  |  |
| 13.6 | Richtlinie für elektronische Nachrichtenübermittlung definieren. |   |  |  |
| 13.7 | Richtlinie für Vertraulichkeits- oder Geheimhaltungs-vereinbarungen definieren. |   |  |  |
| 13.8 | Richtlinie für Systemakquise, -entwicklung und -wartung definieren. |   |  |  |
| ***14. Systemakquise, -entwicklung und -wartung*** |
| 14.1 | Richtlinie für die Analyse und Spezifikation von Informations-sicherheitsanforderungen definieren. |   |  |  |
| 14.2 | Richtlinie zur Absicherung von Anwendungsdiensten in öffentlichen Netzwerken definieren. |   |  |  |
| 14.3 | Richtlinie zum Schutz von Transaktionen in Anwendungs-diensten definieren. |   |  |  |
| ***15. Lieferantenbeziehungen*** |
| 15.1 | Richtlinie für Lieferantenbe-ziehungen definieren. |   |  |  |
| ***16. Management von Informationssicherheitsvorfällen*** |
| 16.1 | Richtlinien für das Informationssicherheitsmanagement definieren. |   |  |  |
| ***17. Informationssicherheitsaspekte des Geschäftskontinuitätsmanagements*** |
| 17.1 | Richtlinie für Redundanzen definieren. |   |  |  |
| ***18. Compliance*** |
| 18.1 | Richtlinie für die Ermittlung geltender Rechtsvorschriften und vertraglicher Anforderungen definieren. |   |  |  |
| 18.2 | Richtlinien für Rechte an geistigem Eigentum definieren. |   |  |  |
| 18.3 | Richtlinie zum Schutz von Datensätzen definieren. |   |  |  |
| 18.4 | Richtlinie für den Datenschutz und Schutz personenbezogener Daten definieren. |   |  |  |
| 18.5 | Richtlinie zur Regulierung krypto-grafischer Steuerung definieren. |   |  |  |
| 18.6 | Richtlinie zur Einhaltung von Sicherheitsrichtlinien und -standards definieren. |   |  |  |
| 18.7 | Richtlinie für die Prüfung technischer Compliance definieren. |   |  |  |

**HAFTUNGSAUSSCHLUSS**

Alle von Smartsheet auf der Website aufgeführten Artikel, Vorlagen oder Informationen dienen lediglich als Referenz. Wir versuchen, die Informationen stets zu aktualisieren und zu korrigieren. Wir geben jedoch, weder ausdrücklich noch stillschweigend, keine Zusicherungen oder Garantien jeglicher Art über die Vollständigkeit, Genauigkeit, Zuverlässigkeit, Eignung oder Verfügbarkeit in Bezug auf die Website oder die auf der Website enthaltenen Informationen, Artikel, Vorlagen oder zugehörigen Grafiken. Jegliches Vertrauen, das Sie in solche Informationen setzen, ist aus eigener Verantwortung.

Diese Vorlage wird nur als Beispiel bereitgestellt. Diese Vorlage ist in keiner Form als rechtliche oder Compliance-Beratung gedacht. Benutzer dieser Vorlage müssen feststellen, welche Informationen notwendig und erforderlich sind, um ihre Ziele zu erreichen.