**CHECKLISTE FÜR GESCHÄFTSKONTINUITÄT NACH ISO 27001 **

|  |  |  |  |
| --- | --- | --- | --- |
| **ANFORDERUNGSABSCHNITT/****KATEGORIE** | **BEWERTUNG** | **KONFORM?** | **BEMERKUNGEN** |
| ***5. Informationssicherheitsrichtlinien*** |  |  |
| 5.1 | Gibt es Sicherheitsrichtlinien? |   |  |
| 5.2 | Alle Richtlinien wurden vom Management genehmigt? |   |  |
| 5.3 | Nachweis für Compliance? |   |  |
| ***6. Organisation der Informationssicherheit*** |   |  |
| 6.1 | Rollen und Verantwortlichkeiten definiert? |   |  |
| 6.2 | Trennung von Aufgaben definiert? |   |  |
| 6.3 | Verifizierungsstelle / Behörde zur Überprüfung der Compliance kontaktiert? |   |  |
| 6.4 | Haben Sie Kontakt zu speziellen Interessengruppen bezüglich Compliance hergestellt? |   |  |
| 6.5 | Nachweis der Informationssicherheit im Projektmanagement? |   |  |
| 6.6 | Richtlinie für Remote-Arbeit festgelegt? |   |  |
| ***7. Sicherheit im Personalwesen*** |   |  |
| 7.1 | Richtlinie für die Überprüfung von Mitarbeitern vor der Anstellung definiert? |   |  |
| 7.2 | Richtlinie für HR-Bedingungen und -Beschäftigungsverhältnisse definiert? |   |  |
| 7.3 | Richtlinien für Verantwortlichkeiten des Managements definiert? |   |  |
| 7.4 | Richtlinien für das Bewusstsein für Informationssicherheit, Bildung und Schulung definiert? |   |  |
| 7.5 | Richtlinien für Disziplinarverfahren in Bezug auf die Informationssicherheit definiert? |   |  |
| 7.6 | Richtlinien für die Beendigung oder den Wechsel des Arbeitsverhältnisses in Bezug auf die Informationssicherheit definiert? |   |  |
| ***8. Asset-Management*** |   |  |
| 8.1 | Vollständige Bestandsliste der Assets? |   |  |
| 8.2 | Vollständige Eigentümerliste für Assets? |   |  |
| 8.3 | Richtlinie zur „zulässigen Nutzung“ von Assets definiert? |   |  |
| 8.4 | Richtlinie für die Rückgabe von Assets definiert? |   |  |
| 8.5 | Richtlinie zur Klassifizierung von Informationen definiert? |   |  |
| 8.6 | Richtlinie für die Kennzeichnung von Informationen definiert? |   |  |
| 8.7 | Richtlinie für den Umgang mit Assets definiert? |   |  |
| 8.8 | Richtlinien für den Umgang mit Wechselmedien definiert? |   |  |
| 8.9 | Richtlinie für die Entsorgung von Medien definiert? |   |  |
| 8.10 | Richtlinie für die Übertragung physischer Datenträger definiert? |   |  |
| ***9. Zugriffskontrolle*** |   |   |  |
| 9.1 | Richtlinie für die Zugriffskontrollen-Richtlinie definiert? |   |  |
| 9.2 | Richtlinie für den Zugriff auf Netzwerke und Netzwerkdienste definiert? |   |  |
| 9.3 | Richtlinie für die An- und Abmeldung von Benutzer-Assets definiert? |   |  |
| 9.4 | Richtlinie für die Bereitstellung des Benutzerzugriffs definiert? |   |  |
| 9.5 | Richtlinie für die Verwaltung privilegierter Zugriffsrechte definiert? |   |  |
| 9.6 | Richtlinien für den Umgang mit geheimen Authentifizierungsdaten von Benutzern definiert? |   |  |
| 9.7 | Richtlinie zur Überprüfung der Benutzerzugriffsrechte definiert? |   |  |
| 9.8 | Richtlinie für die Entfernung oder Anpassung von Zugriffsrechten definiert? |   |  |
| 9.9 | Richtlinie zur Nutzung von geheimen Authentifizierungsinformationen definiert? |   |  |
| 9.10 | Richtlinie zur Beschränkung des Zugriffs auf Informationen definiert? |   |  |
| 9.11 | Richtlinie für sichere Anmeldeverfahren definiert? |   |  |
| 9.12 | Richtlinie für Kennwortmanagementsysteme definiert? |   |  |
| 9.13 | Richtlinie für die Verwendung von privilegierten Dienstprogrammen definiert? |   |  |
| 9.14 | Richtlinie für die Kontrolle von Zugriffen auf Programm-Quellcodes definiert? |   |  |
| ***10. Kryptografie*** |   |  |
| 10.1 | Richtlinie zur Verwendung kryptografischer Steuerungen definiert? |   |  |
| 10.2 | Richtlinien für das Schlüsselmanagement definiert? |   |  |
| ***11. Physische und Umgebungssicherheit*** |   |  |
| 11.1 | Richtlinien für physische Sicherheitsbereiche definiert? |   |  |
| 11.2 | Richtlinie für physische Zugangskontrollen definiert? |   |  |
| 11.3 | Richtlinien für die Absicherung von Büros, Räumen und Anlagen definiert? |   |  |
| 11.4 | Richtlinien zum Schutz gegen externe und Umweltbedrohungen definiert? |   |  |
| 11.5 | Richtlinie für die Arbeit in sicheren Bereichen definiert? |   |  |
| 11.6 | Richtlinien für Liefer- und Ladebereiche definiert? |   |  |
| 11.7 | Richtlinien für die Standortwahl und Schutz der Ausrüstung definiert? |   |  |
| 11.8 | Richtlinie für Hilfsversorgungseinrichtungen definiert? |   |  |
| 11.9 | Richtlinie für die Verkabelungssicherheit definiert? |   |  |
| 11.10 | Richtlinie für die Gerätewartung definiert? |   |  |
| 11.11 | Richtlinie für das Entfernen von Assets definiert? |   |  |
| 11.12 | Richtlinie für die Sicherheit von Ausrüstung und Assets definiert, die nicht vor Ort sind? |   |  |
| 11.13 | Sichere Entsorgung oder Wiederverwendung von Ausrüstung? |   |  |
| 11.14 | Richtlinie für unbeaufsichtigte Benutzerausrüstung definiert? |   |  |
| 11.15 | Richtlinie für Clear Desk- und Clear-Screen-Richtlinien definiert? |   |  |
| ***12. Betriebssicherheit*** |   |  |
| 12.1 | Richtlinie für dokumentierte Betriebsabläufe definiert? |   |  |
| 12.2 | Richtlinien für das Changemanagement definiert? |   |  |
| 12.3 | Richtlinien für das Kapazitätsmanagement definiert? |   |  |
| 12.4 | Richtlinien für die Trennung von Entwicklungs-, Test- und Betriebsumgebungen definiert? |   |  |
| 12.5 | Richtlinien für Malware-Kontrolle definiert? |   |  |
| 12.6 | Richtlinie für die Sicherung von Systemen definiert? |   |  |
| 12.7 | Richtlinie für die Sicherung von Informationen definiert? |   |  |
| 12.8 | Richtlinie für die Ereignisprotokollierung definiert? |   |  |
| 12.9 | Richtlinie zum Schutz von Protokollinformationen definiert? |   |  |
| 12.10 | Richtlinie für Administratoren- und Bedienerprotokoll definiert? |   |  |
| 12.11 | Richtlinie für die Uhrsynchronisierung definiert? |   |  |
| 12.12 | Richtlinie für die Installation von Software in betrieblichen Systemen definiert? |   |  |
| 12.13 | Richtlinie für die Verwaltung technischer Schwachstellen definiert? |   |  |
| 12.14 | Richtlinie für die Einschränkung von Softwareinstallationen definiert? |   |  |
| 12.15 | Richtlinie für die Kontrolle von Informationssystem-Audits definiert? |   |  |
| ***13. Kommunikationssicherheit*** |   |  |
| 13.1 | Richtlinie für Netzwerksteuerung definiert? |   |  |
| 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 definiert? |   |  |
| 13.5 | Richtlinien für Vereinbarungen zur Informationsübertragung definiert? |   |  |
| 13.6 | Richtlinie für elektronische Nachrichtenübermittlung definiert? |   |  |
| 13.7 | Richtlinie für Vertraulichkeits- oder Geheimhaltungsvereinbarungen definiert? |   |  |
| 13.8 | Richtlinie für Systemakquise, -entwicklung und -wartung definiert? |   |  |
| ***14. Systemakquise, -entwicklung und -wartung*** |   |  |
| 14.1 | Richtlinie für die Analyse und Spezifikation von Informationssicherheitsanforderungen definiert? |   |  |
| 14.2 | Richtlinie zur Absicherung von Anwendungsdiensten in öffentlichen Netzwerken definiert? |   |  |
| 14.3 | Richtlinie zum Schutz von Transaktionen in Anwendungsdiensten definiert? |   |  |
| 14.4 | Richtlinie für die interne Entwicklung definiert? |   |  |
| ***15. Lieferantenbeziehungen*** |   |  |
| 15.1 | Richtlinie für Lieferantenbeziehungen definiert? |   |  |
| ***16. Management von Informationssicherheitsvorfällen*** |   |  |
| 16.1 | Richtlinien für das Informationssicherheitsmanagement definiert? |   |  |
| ***17. Informationssicherheitsaspekte des Geschäftskontinuitätsmanagements*** |  |
| 17.1 | Richtlinien für die Informationssicherheitskontinuität definiert? |   |  |
| 17.2 | Richtlinie für Redundanzen definiert? |   |  |
| ***18. Compliance*** |   |   |  |
| 18.1 | Richtlinie für die Ermittlung geltender Rechtsvorschriften und vertraglicher Anforderungen definiert? |   |  |
| 18.2 | Richtlinien für Rechte an geistigem Eigentum definiert? |   |  |
| 18.3 | Richtlinie zum Schutz von Datensätzen definiert? |   |  |
| 18.4 | Richtlinie für den Datenschutz und Schutz personenbezogener Daten definiert? |   |  |
| 18.5 | Richtlinie zur Regulierung kryptografischer Steuerung definiert? |   |  |
| 18.6 | Richtlinie zur Einhaltung von Sicherheitsrichtlinien und -standards definiert? |   |  |
| 18.7 | Richtlinie für die Prüfung technischer Compliance definiert? |   |  |

**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.