**CHECKLISTENVORLAGE FÜR 
ISO 27002 INFORMATIONSSICHERHEITSRICHTLINIEN**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ISO 27001 CONTROL-NUMMER** | **RANG** | **PRIORITÄT** | **INHABER** | **ZUWEISUNGS-DATUM** | **FÄLLIGKEITS-DATUM** | **KONFORM?** | **STATUS** | **ANMERKUNGEN** |
| **5. Sicherheitsrichtlinienmanagement** |
| 5.1 – Das Management hat die Compliance-Richtung vorgegeben und Unterstützung geboten?   |  |   |  |   |   |   |  |   |
| **6. Sicherheitsmanagement des Unternehmens** |
| 6.1 - Wurde eine Interne Task Force für Informations-sicherheit eingerichtet?  |   |   |   |   |   |   |  |   |
| 6.2 - Maßnahmen zum Schutz der mobilen Geräte und des Netzwerks des Unternehmens?   |   |   |   |   |   |   |  |   |
| **7. Sicherheitsmanagement des Personals** |
| 7.1 - Richtlinie zur Überprüfung der Sicherheit vor der Beschäftigung festgelegt? |   |   |   |   |   |   |  |   |
| 7.2 - Richtlinie zur Überprüfung der Sicherheit während der Beschäftigung festgelegt?  |   |   |   |   |   |   |  |   |
| 7.3 - Richtlinie zur Sicherheit bei der Kündigung festgelegt?  |   |   |   |   |   |   |  |   |
| **8. Organisatorisches Asset-Management** |
| 8.1 - Richtlinie für Unternehmensassets festgelegt?  |   |   |   |   |   |   |  |   |
| 8.2 - Richtlinie für die Methode der Informationsklassifizierung festgelegt?  |   |   |   |   |   |   |  |   |
| 8.3 - Richtlinie zur Kontrolle physischer Medien festgelegt?  |   |   |   |   |   |   |  |   |
| **9. Informationszugriffsmanagement** |
| 9.1 – Richtlinie für das Informationszugriffsmanagement für Geschäftsanforderungen festgelegt?  |   |   |   |   |   |   |  |   |
| 9.2 - Richtlinie für die Verwaltung der Zugriffsrechte aller Benutzer festgelegt?  |   |   |   |   |   |   |  |   |
| 9.3 – Richtlinie für die Benutzerauthentifizierung festgelegt?  |   |   |   |   |   |   |  |   |
| 9.4 - Richtlinie zur Kontrolle des Zugriffs auf Systeme festgelegt?  |   |   |   |   |   |   |  |   |
| **10. Richtlinienmanagement für Kryptografie** |
| 10.1 - Richtlinie zur Kontrolle der Verwendung von kryptografischen Steuerungen und Schlüsseln festgelegt?  |   |   |   |   |   |   |  |   |
| **11. Physisches Sicherheitsmanagement** |
| 11.1 – Richtlinie für das physische Sicherheitsmanagement festgelegt?   |   |   |   |   |   |   |  |   |
| 11.2 - Richtlinie zum Schutz der Ausrüstung der Organisation festgelegt?  |   |   |   |   |   |   |  |   |
| **12. Betriebliches Sicherheitsmanagement** |
| 12.1 - Richtlinien für betriebliche Sicherheitsmanagementverfahren und -verantwortlichkeiten festgelegt?  |   |   |   |   |   |   |  |   |
| 12.2 - Richtlinie zum Schutz der Ausrüstung der Organisation vor Malware festgelegt?   |   |   |   |   |   |   |  |   |
| 12.3 - Richtlinie zur regelmäßigen Erstellung von Sicherungskopien festgelegt?  |   |   |   |   |   |   |  |   |
| 12.4 - Richtlinie für die Verwendung von Protokollen zur Aufzeichnung von Sicherheitsereignissen festgelegt?  |   |   |   |   |   |   |  |   |
| 12.5 - Richtlinie zur Kontrolle der betrieblichen Software der Organisation festgelegt?  |   |   |   |   |   |   |  |   |
| 12.6 – Richtlinie zur Behebung der technischen Schwachstellen der Organisation festgelegt?  |   |   |   |   |   |   |  |   |
| 12.7 - Richtlinie zur Minimierung der Auswirkungen von Auditaktivitäten festgelegt?  |   |   |   |   |   |   |  |   |
| **13. Netzwerksicherheitsmanagement** |
| 13.1 - Richtlinie zum Schutz von Netzwerken und Einrichtungen festgelegt?  |   |   |   |   |   |   |  |   |
| 13.2 - Richtlinie zum Schutz der Informationsübermittlung festgelegt?  |   |   |   |   |   |   |  |   |
| **14. Systemsicherheitsmanagement** |
| 14.1 - Eine Richtlinie zur Gewährleistung der Sicherheit von Informationssystemen festgelegt?  |   |   |   |   |   |   |  |   |
| 14.2 - Richtlinie zum Schutz und zur Kontrolle der Tätigkeiten der Systementwicklung festgelegt?  |   |   |   |   |   |   |  |   |
| 14.3 - Richtlinie zum Schutz von Daten festgelegt, die für Systemtests verwendet werden?   |   |   |   |   |   |   |  |   |
| **15. Supplier Relationship Management** |
| 15.1 - Richtlinie für den Abschluss von Sicherheitsvereinbarungen mit Lieferanten festgelegt?  |   |   |   |   |   |   |  |   |
| 15.2 - Richtlinie für die Verwaltung der Sicherheit und Dienstleistungen von Lieferanten festgelegt?  |   |   |   |   |   |   |  |   |
| **16. Management von Sicherheitsvorfällen** |
| 16.1 - Richtlinie zur Identifizierung und Reaktion auf Informationssicherheitsvorfälle festgelegt?  |   |   |   |   |   |   |  |   |
| **17. Sicherheitskontinuitätsmanagement** |
| 17.1 - Richtlinie zur Bildung von Informations-sicherheitskon-tinuitätskontrollen festgelegt?  |   |   |   |   |   |   |  |   |
| 17.2 - Richtlinie für den Aufbau von Redundanzen für Informationsverarbeitungsanlagen festgelegt?  |   |   |   |   |   |   |  |   |
| **18. Security Compliance Management** |
| 18.1 - Richtlinie für die Einhaltung von Rechtssicherheitsanforderungen festgelegt?  |   |   |   |   |   |   |  |   |
| 18.2 - Richtlinie für die Durchführung von Sicherheits-Compliance-Überprüfungen festgelegt?  |   |   |   |   |   |   |  |   |

**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.