IT-Sicherheits-richtlinie für ORGANISATION X.

CyberPilot

IT-Sicherheits-richtlinie für ORGANISATION X.

Diese Richtlinien können als Inspiration für Ihre eigenen IT-Sicherheitsrichtlinien dienen und direkt für Ihr Unternehmen kopiert und implementiert werden – das hängt ganz von Ihnen ab.

Beachten Sie jedoch, dass Sie das X gegen den Namen Ihrer Organisation austauschen müssen.

Zweck

Die Sicherheitsrichtlinie definiert den Rahmen für das Informationssicherheitsmanagement in X.

Gültigkeit

Die Sicherheitsrichtlinie gilt für alle Mitarbeiter in X und den gesamten Zugriff auf die Informationssysteme von X.

Ziele

- X arbeitet aktiv mit dem Informationssicherheitsmanagement zusammen, um Verfügbarkeit, Systeme und Daten sicherzustellen.
- X bemüht sich, ISO 27001: 2013 / ISO27002: 2013 einzuhalten.
- X verwendet einen risikobasierten Ansatz, bei dem das Schutzniveau und die Kosten auf der Geschäftsrisiko- und Folgenabschätzung basieren müssen, die mindestens einmal jährlich durchgeführt werden muss.
- Ein IT-Sicherheitshandbuch muss erstellt und kontinuierlich aktualisiert werden. Dieses Handbuch wird Beschreibungen der durchgeführten Maßnahmen zur Informationssicherheit sowie Verweise auf relevante Richtlinien und Verfahren enthalten.
- X zielt darauf ab, die einschlägigen Rechtsvorschriften einzuhalten, einschließlich der GDPR.
- X beabsichtigt, Vereinbarungen mit externen Parteien einzuhalten, einschließlich Datenverarbeitungsvereinbarungen.
- X ist bestrebt, eine jährliche Erklärung zu erstellen, d.h. ISAE3402, ISAE3000, ISO-Zertifikat usw.
- Diese IT-Sicherheitsrichtlinien werden jährlich überprüft.

Organisation und Verantwortlichkeiten

- **Der Verwaltungsrat** trägt die letztendliche Verantwortung für die Informationssicherheit in X.
- **Der Vorstand** ist für die Managementprinzipien verantwortlich und delegiert spezifische Verantwortlichkeiten für Schutzmaßnahmen, einschließlich des Eigentums an

Informationssystemen.

- **Eigentum** ist für jedes kritische Informationssystem festgelegt. Der Eigentümer legt fest, wie Schutzmaßnahmen in Übereinstimmung mit den Sicherheitsrichtlinien angewendet und verwaltet werden.
- **Die IT-Abteilung** konsultiert, koordiniert, kontrolliert und berichtet über den Sicherheitsstatus. Die IT-Abteilung erstellt Richtlinien und Verfahren.
- **Der einzelne Mitarbeiter** ist dafür verantwortlich, die Sicherheitsrichtlinien einzuhalten und in der „IT-Nutzungsrichtlinie" darüber informiert zu werden.

Verzicht

Ausnahmen von den Richtlinien zur Informationssicherheit von X werden von der IT-Abteilung auf der Grundlage der vom Vorstand festgelegten Richtlinien genehmigt.

Berichterstattung

- Die IT-Abteilung informiert den Vorstand über alle relevanten Sicherheitsverletzungen.
- Der Status der Ausnahmeregelungen ist im Jahresbericht der IT-Abteilung an die Geschäftsleitung enthalten.
- Der Vorstand überprüft jährlich den Sicherheitsstatus und erstattet anschließend dem Verwaltungsrat Bericht.

Verstoß

Vorsätzliche Verstöße und Missbräuche werden von der IT-Abteilung der Personalabteilung und der nächstgelegenen Autorität mit Führungsverantwortung gemeldet.

Verstöße gegen die IT-Sicherheitsrichtlinien und gegen unterstützende Richtlinien können arbeitsrechtliche Konsequenzen haben.