Risikomanagement-Politik

*Objekt**: Risikomanagementpolitik**Datum**: [Datum einfügen]**Verantwortlich**: CISO, Risikomanagementteam, leitende Angestellte

Diese Risikomanagementpolitik wurde in Übereinstimmung mit Artikel 21 Absatz 2 Buchstabe A der NIS2-Richtlinie entwickelt. Ziel des Dokuments ist es, einen Rahmen für die Identifizierung, Bewertung und Verwaltung von Informationssicherheitsrisiken zu schaffen und die Integrität und Verfügbarkeit von Unternehmensdaten zu schützen.

1. Zweck der Politik

Mit dieser Politik soll sichergestellt werden, dass die Organisation einen strukturierten und systematischen Ansatz für das Risikomanagement verfolgt, um die Auswirkungen von Bedrohungen der Cybersicherheit zu minimieren und die Kontinuität des Geschäftsbetriebs zu gewährleisten.

2. Umfang der Anwendung

Diese Richtlinie gilt für alle Mitarbeiter, Dienstleister und Dritte, die auf die IT-Ressourcen und Daten der Organisation zugreifen, sie verwalten oder verarbeiten.

3. Grundsätze des Risikomanagements

ie folgenden Grundsätze des Risikomanagements müssen von der Organisation übernommen werden:1. **Risikoermittlung**: Ermittlung von Informationssicherheitsrisiken bei allen Geschäftstätigkeiten.
2. **Risikobewertung**: Bewertung der Auswirkungen und der Wahrscheinlichkeit der identifizierten Risiken unter Verwendung einer Risikoskala.
3. **Risikobehandlung**: Implementierung von Kontrollen und Maßnahmen zur Abschwächung oder Beseitigung der identifizierten Risiken.

4. **Überwachung und Überprüfung**: Kontinuierliche Überwachung der Risiken und periodische Überprüfung der getroffenen Maßnahmen.

4. Risikobewertung

Die Organisation muss regelmäßig Risikobewertungen durchführen, um neue Bedrohungen zu erkennen und die Wirksamkeit der bestehenden Sicherheitskontrollen zu bewerten.
ei den Bewertungen sollten berücksichtigt werden:- Risiken der Informationssicherheit.
- Operative Risiken.
- Rechtliche und Compliance-Risiken

5. Restrisikomanagement

Nach der Umsetzung von Maßnahmen zur Risikominderung muss die Organisation Restrisiken formell ermitteln und akzeptieren. Diese Risiken müssen mit Plänen zur Aufrechterhaltung des Geschäftsbetriebs verwaltet und regelmäßig überprüft werden.

6. Überwachung und Überprüfung der Politik

Die Risikomanagementpolitik muss regelmäßig überprüft und aktualisiert werden, um sicherzustellen, dass sie mit den Unternehmenszielen und den Veränderungen in der Bedrohungslandschaft übereinstimmt.