

Sicherheitspolitik für Zulieferer

Objekt: Sicherheitspolitik für Lieferanten ***Datum***: [Datum einfügen] ***Verantwortlich***: CISO, Beschaffungsteam, Geschäftsleitung

Diese Politik legt die Leitlinien für die Gewährleistung der Sicherheit von Informationen, Systemen und Infrastrukturen bei allen Interaktionen mit Drittanbietern und Partnern gemäß Artikel 21 Absatz 2 Buchstabe D der NIS2-Richtlinie fest.

1. Zweck der Politik

Mit dem Sicherheitsplan für Lieferanten soll sichergestellt werden, dass alle Lieferanten und Partner die Sicherheitsanforderungen der Organisation einhalten und die mit Dritten verbundenen Risiken minimiert werden.

2. Umfang der Anwendung

Diese Richtlinie gilt für alle Lieferanten, Partner und Dritte, die Dienstleistungen, Produkte oder Zugang zu Unternehmensdaten und -systemen anbieten. Sie gilt auch für alle internen Mitarbeiter, die am Lieferantenmanagement beteiligt sind.

3. Sicherheitsanforderungen für Zulieferer

Die Lieferanten müssen die folgenden Sicherheitsanforderungen einhalten:

- *Datenschutz***:

Die Lieferanten müssen sicherstellen, dass die Unternehmensdaten vor unbefugtem Zugriff geschützt sind und in Übereinstimmung mit den geltenden Vorschriften verarbeitet werden.

- *Zugangskontrollen***: Der Zugang zu den Systemen des Unternehmens muss eingeschränkt und nur dem dafür vorgesehenen Personal gestattet sein.

- *Reaktion auf Vorfälle***: Die Lieferanten müssen über Verfahren für den Umgang mit Sicherheitsvorfällen verfügen und das Unternehmen im Falle eines Verstoßes unverzüglich benachrichtigen.

Firmenlogo

Sicherheitspolitik für
Zulieferer

Geprüft von:
Freigegeben von: _____

4. ****Audit und Überwachung****: Die Lieferanten müssen regelmäßige Audits der implementierten Sicherheitskontrollen ermöglichen.

4. Vertragsmanagement und Sicherheitsklauseln

Alle Verträge mit Zulieferern und Partnern müssen spezielle Klauseln zur Informationssicherheit enthalten, einschließlich Datenschutzanforderungen, Verfahren zur Reaktion auf Vorfälle und Audits zur Einhaltung der Vorschriften.

5. Risikobewertung für Zulieferer

Bevor eine Zusammenarbeit mit einem Lieferanten aufgenommen wird, muss eine Risikobewertung durchgeführt werden, um den Grad der Gefährdung durch Cyber-Sicherheitsrisiken zu bestimmen.

6. Überwachung und Überprüfung

Die Einhaltung der Sicherheitsanforderungen durch die Lieferanten muss regelmäßig überwacht werden, und die Richtlinie muss regelmäßig überprüft und aktualisiert werden, um sicherzustellen, dass sie weiterhin mit den geschäftlichen und gesetzlichen Anforderungen übereinstimmt.