Lieferanten-Sicherheitsrichtlinie

Inhaltsverzeichnis

1. Über das Verfahren 1

1.1. Ziel und Zweck 1

1.2. Anwendungsbereich (Betroffene Lieferanten und Geschäftsbeziehungen) 1

1.3. Zuständigkeiten 1

2. Sicherheitsrichtlinie für Lieferanten 1

2.1. Sicherheitsvorschriften 1

2.2. Rückgabe von Werten 2

2.3. Meldung von Sicherheitsvorfällen 2

2.4. Awareness-Trainings 2

2.5. Überprüfung der Sicherheitsvorgaben 2

1. Über das Verfahren

1.1. Ziel und Zweck

Das Dokument legt die Sicherheitsvorschriften für Lieferanten fest.

1.2.Anwendungsbereich (Betroffene Lieferanten und Geschäftsbeziehungen)

Unter folgenden Bedingungen müssen die Zusatzvereinbarungen über Informationssicherheit abgeschlossen werden:

- wenn der Lieferant Zugriff auf interne Dokumente und Informationen erhält oder
- wenn der Lieferant mit der Verarbeitung von Daten beauftragt wird, die schützenswert sind, oder
- wenn die Risikoanalyse ergibt, dass der Vertrag Auswirkung auf die Gewährleistung unseres Informationssicherheitsniveaus haben kann und die Vereinbarung das Risiko reduzieren kann.

Folgende Ausnahmen bestehen:

- Erfüllt der Vertrag / die Leistungsbeschreibung bereits die Sicherheitsanforderungen (Bewertung durch den Informationssicherheitsbeauftragten (ISB), muss nicht auf die Zusatzvereinbarung bestanden werden.

1.3.Zuständigkeiten

Zuständig für die Einhaltung der Richtlinie sind alle Lieferanten, die in genannten Anwendungsbereich fallen, Mitarbeiter des Unternehmens, die diese Lieferanten beauftragen, als auch der ISB.

2. Sicherheitsrichtlinie für Lieferanten

2.1.Sicherheitsvorschriften

Technisch
- Nutzung aktueller Hard- und Software, die ebenfalls regelmäßig aktualisiert wird
- Einsatz anerkannter, in der Branche üblicher, Sicherheitssoftware wie Firewall und Virenscanner, um Schadsoftware abzuhalten
- Nutzung sicherer Verbindungen zur Dateiübertragung (mindestens TLS 1.2 Transportverschlüsselung)

Organisatorisch
- Nutzung eines Rechtekonzepts (siehe Dokument: SharePoint_Permission), um bereitgestellte Informationen nur zuständigen Mitarbeitern zugänglich zu machen
- Meldung von erkannten Sicherheitslücken an den Auftraggeber
- Verwendung sicherer Passwörter zum Schutz eigener IT-Systeme
- Betrieb eines Zugangskontrollkonzepts für Räumlichkeiten (siehe Dokument: TARA-Liste_Reiter_Räume)
- Umsetzung weiterer Sicherheitsmaßnahmen, soweit dies eingefordert wird

Zugriff auf Informationen
- Der Vertragspartner gewährt jederzeit Zugriff, auf die im Rahmen des Vertrages erhobenen und gespeicherten Informationen.
- Der Vertragspartner hat das Recht, auf Informationen der durch Automotive Quality Institute (AQI) GmbH definierten Klassifizierung im jeweiligen Arbeitsbereich zuzugreifen, um den Vertrag zu erfüllen.

2.2. Rückgabe von Werten

Endet das Vertragsverhältnis, sind alle Daten oder bereitgestellte Informationen und Zugänge unverzüglich zu übergeben oder nach Rücksprache sicher zu vernichten

2.3.Meldung von Sicherheitsvorfällen

Der Vertragspartner meldet Sicherheitsvorfälle sowie verdächtige Ereignisse in eigenen Systemen unverzüglich, sobald Sie Daten der Automotive Quality Institute (AQI) GmbH betreffen könnten. Das AQI kann bei der Analyse von Sicherheitsvorfällen beratend hinzugezogen werden.

2.4. Awareness-Trainings

Der Vertragspartner verpflichtet sich, regelmäßige Awareness-Trainings für Informationssicherheit in betroffenen Arbeitsbereichen durchzuführen. Der ISB des AQI kann hierbei beratend hinzugezogen werden.

Kann ein Unternehmen ihre Sicherheitsanforderungen in der Praxis nicht umsetzen, unterstützt das AQI, durch das Bereitstellen von Schulungsunterlagen, bei der Umsetzung.

2.5. Überprüfung der Sicherheitsvorgaben

Der Vertragspartner verpflichtet sich, Überprüfungen der hier getroffenen Maßnahmen regelmäßig als auch außerplanmäßig zuzulassen. Hierzu gehört unter anderem und nicht ausschließlich:

- Die Bereitstellung von Informationen wie Prozessbeschreibungen oder Arbeitsanweisungen, um die Überprüfung selbiger zu ermöglichen.
- Die Bereitstellung von Informationen über das Informationssicherheitsniveau wie z. B. Anzahl von Sicherheitsvorfällen, Konfiguration von IT-Systemen oder eine Aufstellung selbst ausgelagerter Tätigkeiten, die die Informationssicherheit beeinflussen können.
- Die Gewährung des Zugangs zu Geschäftsräumen, um Vor-Ort-Audits durchzuführen. Dieser Punkt trifft jedoch nur zu, wenn der Vertragspartner regelmäßig besonders sensiblen Daten vom AQI verarbeitet.