Formular

Informationssicherheitsleitlinie für Lieferanten

Die Bedeutung der Informationssicherheit nimmt stetig zu. Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Werte sind in allen Prozessen sicherzustellen. Die Firma Thöni hält ein TISAX Label (VDA ISA Fragenkatalog) als Standard für Informationssicherheit. Wir arbeiten an der stetigen Verbesserung unseres Managementsystems für Informationssicherheit. Von unseren Lieferanten erwarten wir, dass Grundlagen der Informationssicherheit eingehalten werden. Dazu zählen unter anderem, aber nicht ausschließlich, die im folgenden genannten Punkte:

Organisation der Informationssicherheit
Das Unternehmen definiert und lebt Richtlinien, Prozesse und Verantwortlichkeiten, welche die Informationssicherheit garantieren, kontrollieren und verbessern.

Bewertung des Schutzbedarfes
Alle Informationssicherheitswerte, Informationen und verarbeitende Systeme des Unternehmens sind definiert, das Schutzbedürfnis in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit geprüft und entsprechende Maßnahmen abgeleitet. Die Maßnahmen werden regelmäßig auf Wirksamkeit überprüft.

Geheimhaltung und Schutz der Daten
Beim Austausch von vertraulichen Informationen zwischen Unternehmen werden entsprechende Geheimhaltung und Maßnahmen zum Schutz der Daten garantiert.

Legal Compliance
Alle relevanten Gesetze und Richtlinien in Bezug auf Informationssicherheit werden eingehalten. Dafür werden diese regelmäßig auf Aktualisierungen überprüft und die darauf basierenden internen Prozesse gegebenenfalls angepasst.

Zugriffskontrolle und Kryptografie
Methoden zur Benutzer-Authentifikation (z.B. Passwort, 2-Faktor-Authentifikation) sind definiert und umgesetzt.. Berechtigungskonzepte für schützenswerte Informationen, Systeme und Applikationen sind ausgewiesen. Geeignete Maßnahmen zur Verschlüsselung der personenbezogenen bzw. schutzbedürftigen Informationen werden definiert, dokumentiert und regelmäßig auf Aktualität und Sicherheit überprüft.

Physische und umgebungsbezogene Sicherheit
Auf dem eigenen Betriebsgelände ist der Zugang zu sicherheitsrelevanten Informationen und Anlagen nur den berechtigten Personen möglich. Für das Betriebsgelände sind Sicherheitszonen definiert und jeweils geeignete Maßnahmen zum Schutz der Informationen umgesetzt.

Datenschutz
Durch das Einhalten der Gesetze, Vorschriften und möglichen Vertragsbestimmungen zum Datenschutz ist garantiert, dass personenbezogene, sensible Daten jederzeit sicher sind. Sollten Datenschutzübertretungen oder -vorfälle eintreten, werden diese sofort telefonisch (+43 5242 69 030) und schriftlich (compliance@thoeni.com) an die Thöni Industriebetriebe gemeldet, inklusive Angabe der Notfallpläne.

Lieferantenbeziehungen
An Sublieferanten und -unternehmen sind die Anforderungen der Informationssicherheit weitergegeben. Thöni wird bei Vorfällen bei Sublieferanten und -unternehmen unverzüglich telefonisch (+43 5242 69 030) und schriftlich (compliance@thoeni.com) informiert.

Datensicherungen
Schutzbedürftige Daten sind gegen Zerstörung, Verlust und unberechtigten Zugriff oder Veränderung zu schützen. Dies passiert unter anderem durch Erstellen eines Datensicherungskonzepts, dem Durchführen der Datensicherungen und dem sicheren Aufbewahren der Datensicherungen, getrennt von den produktiven Systemen.

Schutz vor Malware
Technische Schwachstellen sind durch geeignete, technische Maßnahmen, wie etwa Virenschutzprogramme, Patchmanagement und laufende Information zu den aktuell bekannten Angriffsszenarien, geschützt.

Protokollierung
Die Eingabe, Veränderung und Entfernung von Daten in IT-Systemen sind überwacht. Dazu zählen untern anderem die Protokollierung der Berechtigungsvergabe, Überprüfung der Benutzerberechtigungen und die Auswertung der Benutzer- und Systemaktivitäten.

Netzwerksicherheit
Ein Netzwerkmanagement ist aufgesetzt, für externe Verbindungen und Verbindungen zwischen einzelnen Systemen ist eine starke Benutzerauthentifizierung vorhanden, Sicherheitsgateways werden benutzt, Diagnose- und Konfigurationsports sind geschützt und sensitive, sensible Systeme isoliert.

Bewusstseinsbildung
Regelmäßige Schulungen zu möglichen Angriffsszenarien, den persönlichen Möglichkeiten zur Verteidigung und Abwehr der Attacken und den Umgang mit sensiblen Daten im Unternehmen werden durchgeführt und auf Wirksamkeit überprüft.

Verhalten bei Informationssicherheitsvorfällen
Jegliche Vorfälle, die die Informationssicherheit betreffen (z.B. Befall von Systemen mit Mal- oder Ransomware, erfolgreiche Hacker- oder Phishingangriffe) sind innerhalb von 24 Stunden telefonisch (+43 5242 69 030) und schriftlich (compliance@thoeni.com) an die Firma Thöni Industriebetriebe zu melden. Gesetzte Maßnahmen werden kommuniziert und dokumentiert.

Business Continuity Management
Für den Fall, dass durch einen Angriff schützenswerter Informationswerte gefährdet sind, sind Notfallpläne vorhanden, die das Weiterführen des Betriebes sicherstellen. Kritische Komponenten sind redundant, Notfallmaßnahmen werden regelmäßig auf Wirksamkeit überprüft.

Überprüfung und Verbesserung
Die genannten Maßnahmen werden regelmäßig auf Wirksamkeit überprüft. Registrierte Schwachstellen werden geschlossen, um das System als Ganzes kontinuierlich zu verbessern. Prüfungen des Systems können auch durch Thöni beim Lieferanten oder Dienstleister durchgeführt werden. In diesem Fall hat der Lieferant oder Dienstleister vollumfänglich zu kooperieren und alle notwendigen Unterlagen zur Verfügung zu stellen.