Secure Supplier Policy
Vertragsergänzungen

Status: June 2025

Inhalt

Status: June 2025

1. Deutsch

Vossloh betreibt ein umfassendes Informationssicherheitsmanagementsystem (ISMS) und behält sich das Recht vor, die Einhaltung der festgelegten Sicherheitsstandards für Lieferanten und Dienstleister durch Audits und Überprüfungen sicherzustellen. Diese Audits dienen dem Schutz sensibler Informationen und der Minimierung potenzieller Schwachstellen.

Die Bewertung der Lieferanten erfolgt in drei Kategorien, die sowohl die Kritikalität der Dienstleistungen als auch den Grad der Integration berücksichtigen:

1. **Level 1**: Kritische Dienste (hohe Integration) – Core-Dienste, die persönliche oder vertrauliche Daten verarbeiten.
2. **Level 2**: Signifikante Dienste (mittlere Integration) – Wichtige Unterstützungsdienste, die keine personenbezogenen Daten verarbeiten.
3. **Level 3**: Unbedeutende Dienste (geringe Integration) – Andere Unterstützungsdienste, die keine sensiblen Daten verarbeiten.

Je nach Kritikalität der Dienstleistung können verschiedene Maßnahmen ergriffen werden. Für kritische Lieferanten sind umfassende Anforderungen an die Informationssicherheit erforderlich, einschließlich verbindlicher Vertragsbedingungen, Geheimhaltungsvereinbarungen und Nachweise über die Einhaltung von Standards wie ISO 27001. Bei signifikanten Diensten sind grundlegende vertragliche Anforderungen und Sicherheitsüberprüfungen notwendig, während für unkritische Dienste lediglich minimale Anforderungen und grundlegende Vertraulichkeitsmaßnahmen gelten.

Die Einhaltung dieser Anforderungen ist entscheidend, um die Sicherheit und Vertraulichkeit unserer Daten zu gewährleisten. Diese Maßnahmen werden entsprechend der Bewertungsstufe des Lieferanten in den jeweiligen Analysen festgehalten

2. Englisch

Vossloh operates a comprehensive Information Security Management System (ISMS) and reserves the right to ensure compliance with established security standards for suppliers and service providers through audits and reviews. These audits serve to protect sensitive information and minimize potential vulnerabilities.

The assessment of suppliers is conducted in three categories, considering both the criticality of the services and the degree of integration:

1. Level 1: Critical services (high integration) – core services that process personal or confidential data.
2. Level 2: Significant services (medium integration) – important support services that do not process personal data.
3. Level 3: Insignificant services (low integration) – other support services that do not process sensitive data.

Depending on the criticality of the service, different measures may be taken. For critical suppliers, comprehensive requirements for information security are necessary, including binding contractual terms, non-disclosure agreements, and proof of compliance with standards such as ISO 27001. For significant

services, basic contractual requirements and security reviews are necessary, while for insignificant services, only minimal requirements and basic confidentiality measures apply.

Compliance with these requirements is essential to ensure the security and confidentiality of our data. These measures will be documented according to the assessment level of the supplier in the respective analyses.