20/06/2022

Evac Information Security Requirements for Suppliers

1 General

Information is one of Evac's key assets and under the Agreement, Supplier will access, process, store, create or otherwise utilize Evac's information. This document contains Evac's high-level Information security requirements for such activities.

Supplier shall comply with the requirements set forth herein and in any applicable law or regulation to ensure that Evac information is protected to a sufficient degree during any activities.

This document is not an exhaustive description of relevant information security requirements. Supplier shall therefore, without additional compensation, take any other measures required to maintain an appropriate level of information security.

2 Scope

These information security requirements apply to all Evac's information (including but not limited to project, service, delivery, and product related information as well as personal data) that is managed or otherwise processed by Supplier under the Agreement.

The Supplier is fully responsible for that its eventual subcontractors comply with the same information security requirements as set out in this document. However, Supplier shall not grant access to or share Evac data with its subcontractors or any other third party without prior written approval of Evac.

3 Information Security Policy

Supplier must have an internal information security policy to which the top management has committed and that is implemented across Supplier's organization, including group companies. The policy shall cover relevant areas of common and case by case applicable standards (e.g., ISO27001). The policy shall be regularly assessed and revised.

4 Information Security Organization

Supplier must have a nominated top-level information security responsible person with overall responsibility. Supplier must provide Evac the contact details of the person.

A high-level information security group can, if requested by Evac or Supplier, be established to co-ordinate information security activities between Evac and Supplier.

5 Information Risk Management

The Supplier must have formal information risk management in place and be able to demonstrate that the Supplier can identify, assess, and mitigate risks related to Evac's information. Risk identification and assessment shall be performed on a regular basis (min. annually) and the results shall be used to review and improve information security controls. Supplier shall, on Evac's request, submit the latest information risk identification and assessment report to Evac (at least the parts that concern Evac's information).

6 Information Security Controls

Supplier shall protect Evac's information by implementing necessary information security controls based on risk management, applicable security standards, legislation etc. These controls may include inter alia, as appropriate:

- Security functionality across different hardware/software platforms
- Security controls at application, device and network level
- Cryptographic techniques when applicable (e.g., pseudonymization and encryption)
- Segregation of environments with different security requirements (e.g., production, development, and testing environments)
- Controlling the flow of information between different environments
- Vulnerability management to identify, prioritize and mitigate vulnerabilities in systems
- Security monitoring to identify potential incidents

Appropriate controls shall be in place throughout the information lifecycle, including when information is created, in use, at rest and in transit. In addition, all Evac information must be disposed of in a secure manner.

The controls shall ensure compliance with applicable legislation, concerning especially information security and data protection, business, and contractual requirements.

Supplier shall regularly assess and evaluate the effectiveness of information security controls for ensuring that the implemented security controls are up to date and sufficient to secure Evac's information.

Supplier shall, on Evac's request, submit a description of the implemented information security controls or the latest security audit report to Evac (at least the parts that concern Evac's information).

7 Personnel and Physical Security

Supplier shall limit access to Evac's information only to its authorized and properly trained personnel on a strict need-to-know basis and ensure that those persons have committed themselves to confidentiality. Supplier shall also ensure that its personnel receive information security awareness training at minimum annually.

Supplier shall make sure that only authorized persons have access to Supplier's locations where Evac's information is managed.

8 Working in the Evac Premises

Supplier shall nominate persons who are authorized to work in Evac's premises. If persons are changed, Evac shall be informed within five (5) working days in advance. Evac has the right to deny access to Evac's premises.

When working in Evac's premises, Supplier personnel shall:

- Work or move only in areas designated by Evac
- Follow local security laws and instructions
- Participate in, if required, local security training
- Always wear visible visitor or personal ID card provided by Evac

Supplier's personnel is not allowed to connect to the wired LAN at Evac premises.

If Supplier's personnel need access to systems in the Evac corporate network, a One Evac identity with Multi-Factor Authentication (MFA) is required. These accounts are always personal and cannot be shared within Supplier organization.

If Supplier's personnel are using Evac's system or working physically at Evac's office, the Evac Group Information Security Policy and Practices will apply.

9 Access Management

Supplier shall have a process for requesting, approving, deploying, and removing access rights concerning Evac's information. All such requests shall be logged for audit purposes.

Access to systems containing Evac information shall be protected by Multi-Factor Authentication (MFA) to prevent unauthorized access.

10 Changes in Processing of Evac's Information

All significant changes in processing of Evac's Information by Supplier shall be reported to and approved by Evac.

11 Information Security Reviews

Evac or a third-party auditor appointed by Evac, shall be entitled to audit and inspect that Supplier's level of information security complies with the requirements set out in this document or otherwise agreed by the parties.

Supplier shall co-operate with the auditors performing the audit to ensure that the auditors are able to form an accurate view of Supplier's aforesaid compliance. Supplier is obliged to correct potential findings at its own cost. Any possible audit carried out by Evac shall in no way limit Supplier's liability.

12 Information Security Incidents

Supplier shall have internal processes established for detecting, managing, and responding to information security incidents. Supplier shall without undue delay inform Evac about any information security incident that may affect Evac's Information.

Supplier shall ensure the ability to restore the availability and access to Evac's Information in a timely manner in the event of an information security incident.

Evac has the right to investigate information security related incidents. Supplier shall ensure that there is technical and practical preparedness for such investigation.