Caliber.global®

Address

PO Box 2
6800 AA Arnhem
The Netherlands

Tivolilaan 205
6824 BV Arnhem
The Netherlands

T +31(0)880041900
E info@caliber.global
W www.caliber.global

SUPPLIER INFORMATION SECURITY POLICY CALIBER.GLOBAL

1. INTRODUCTION AND SCOPE

This is the Supplier Information Security Policy of Caliber.global. With this policy, we establish the requirements for securing sensitive information exchanged between Caliber.global and its suppliers. We consider it essential that sensitive data is handled with the utmost care. This policy aims to protect the confidentiality, integrity, and availability of data shared, processed, or stored as part of the supplier relationship. The objective is to mitigate risks associated with unauthorized access, data breaches, and other security incidents, ensuring that supplier practices align with Caliber.global's security standards.

This policy applies to all suppliers that provide goods, services, or other deliverables to Caliber.global and have access to, handle, or process sensitive or confidential information. It encompasses all aspects of information security, including the protection of physical, digital, and intellectual property data.

2. INFORMATION SECURITY REQUIREMENTS

Caliber.global requires its suppliers to comply with the following information security requirements:

2.1 General Security Controls

- Suppliers must implement security controls that are appropriate to the sensitivity of the information being processed, including physical, administrative, and technical safeguards.
- Suppliers are required to maintain an Information Security Management System (ISMS) that aligns with industry standards (e.g., ISO/IEC 27001, NIST, GDPR, SOC2, etc.).

2.2 Data Protection

- Any personal, sensitive, or confidential data shared by Caliber.global must be securely handled and stored according to applicable laws and regulations.
- Suppliers must implement encryption for data in transit and at rest when handling confidential information.
- Supplier systems must be regularly tested for vulnerabilities and patched to protect against cyber threats.

2.3 Access Control

- Suppliers must ensure that access to information is restricted to authorized personnel only. Access permissions should be based on the principle of least privilege.
- Suppliers must implement strong authentication methods (e.g., multi-factor authentication) for accessing systems that handle Caliber.global's information.

2.4 Incident Response

- Suppliers must have an incident response plan in place to detect, report, and mitigate security incidents involving Caliber.global's information.
- In the event of a data breach or security incident, suppliers are required to notify Caliber.global within 24 hours and cooperate fully with the investigation.

2.5 Business Continuity

- Suppliers must ensure that their operations are resilient and can continue in the event of a disaster or other disruptions. This includes maintaining backups of key data and systems and having a tested disaster recovery plan.

2.6 Third-Party Subcontractors

- If the supplier uses third-party subcontractors to perform services involving Caliber.global's data, the supplier must ensure that the subcontractors adhere to equivalent information security standards and sign appropriate confidentiality agreements.

3. COMPLIANCE AND AUDITING

- Suppliers must comply with all relevant legal and regulatory requirements related to information security, data protection, and privacy.
- Caliber.global reserves the right to audit and assess the security practices of suppliers at regular intervals to ensure compliance with this policy. This may include security assessments, penetration testing, and review of internal security policies.

4. TRAINING AND AWARENESS

- Suppliers must ensure that their personnel receive regular training on information security best practices, data protection laws, and the importance of safeguarding confidential information.
- Suppliers are encouraged to promote a culture of security awareness to mitigate the risks associated with human error and insider threats.

5. POLICY ENFORCEMENT

- Failure to comply with the requirements outlined in this policy may result in penalties, including suspension or termination of contracts, and/or legal action where applicable.
- Caliber.global reserves the right to terminate any supplier relationship if it is determined that the supplier has failed to uphold the security standards required under this policy.

6. REVIEW AND UPDATES

- This policy will be reviewed and updated regularly to ensure it remains aligned with the evolving threat landscape, regulatory changes, and best practices in information security.
- Suppliers will be notified of any significant changes to the policy and may be required to sign updated agreements to reflect new terms or requirements.

7. ACKNOWLEDGMENT

Suppliers are required to acknowledge their receipt and understanding of this Supplier Information Security Policy and commit to its adherence by signing the attached Supplier Agreement.