

Cyber Security Requirements for Suppliers

DISCLAIMER: This printed document is an uncontrolled copy and cannot be used unless the content and revision (version) is verified.

Table of Contents

1 Introduction 3
2 Cyber Security Requirements 3
2.1 Information Security Management System (ISMS) 3
2.2 Risk Management 3
2.3 Asset Management 3
2.4 Access Control and Authentication 4
2.5 Supplier Relationships 4
2.6 Incident Response and Reporting 4
2.7 Business Continuity, Disaster Recovery and Backup 4
2.8 Data Protection, Retention, Disposal and Privacy 5
2.9 Encryption 5
2.10 Change Management 5
2.11 Security Monitoring and Logging 5
2.12 Vulnerability management 6
2.13 Network Security 6
2.14 Secure development 6
2.15 Physical security 6
2.16 OT Products and Services 6
2.17 Suppliers providing Industrial Control Systems including SCADA 7
3 Audit Rights 7
4 Supplier Acknowledgment 7

DISCLAIMER: This printed document is an uncontrolled copy and cannot be used unless the content and revision (version) is verified.

1 Introduction

At DOF, cyber security is a critical part of safe and reliable operations. Suppliers must uphold strong cyber security practices to protect DOF's information, systems, people, and operations — and enable DOF to meet its business objectives.

This document outlines the cyber security requirements that all Suppliers, Contractors and Vendors (referred to as "Supplier") must follow to protect the confidentiality, integrity, and availability of DOF's (referred to as "Customer") data and systems.

The Supplier must implement and maintain effective technical and organizational measures to keep Customer data and systems secure and protected from unauthorized access and risks.

Compliance with these requirements is mandatory unless otherwise agreed in writing through a contract, Statement of Work, or Purchase Order explicitly referencing specific deviations.

2 Cyber Security Requirements

2.1 Information Security Management System (ISMS)

The Supplier must implement and maintain an Information Security Management System (ISMS). This system should cover all the requirements of an international cyber security standard, such as ISO 27001 or NIST.

The ISMS must cover:

- Risk management, including risk assessments and treatment plans.
- Documentation of information security policies and procedures.
- Periodic audits and reviews of the ISMS.
- Evidence of continual improvement activities.

The ISMS should be proven to be operating effectively through periodic internal and/or external audits by independent and qualified practitioners. Failure to maintain cyber security standards and/or certifications may be considered a material breach of the Agreement.

2.2 Risk Management

The Supplier shall conduct cyber risk assessments, overseen by qualified personnel and supported by senior management. These assessments must cover all business units, processes, applications, facilities, systems, and third parties involved in delivering Services to the Customer or in storing or accessing Data. The Supplier must ensure that identified risks are addressed, handled and formally recorded according to severity and contract requirements from Customer.

2.3 Asset Management

The Supplier must establish processes for asset identification, classification, and management throughout their lifecycle. The Supplier must keep an up-to-date asset inventory of information systems and infrastructure, including cloud services, and update it regularly or when assets are installed, removed, or updated.

DISCLAIMER: This printed document is an uncontrolled copy and cannot be used unless the content and revision (version) is verified.

2.4 Access Control and Authentication

The Supplier must ensure that only authorized personnel can access the Customer's data. This includes:

- Proper configuration and deactivation of user accounts.
- Implementing strong authentication techniques.
- Monitoring user actions to identify unauthorized access.
- Applying multi-factor authentication (MFA) where appropriate.
- Enforcing least privilege access for all systems.

2.5 Supplier Relationships

The Supplier must ensure that all subcontractors and third-party providers involved in handling Customer data comply with equivalent security and privacy standards.

An up-to-date inventory of all third parties involved in processing personal or sensitive Customer data must be maintained. The Supplier shall conduct regular security reviews or audits to verify third-party compliance.

2.6 Incident Response and Reporting

The Supplier must have a documented and regularly tested incident response process to ensure a consistent and effective approach to manage cyber security incidents. The plan must also include procedures for post-incident analysis and lessons learned.

In the event of any actual or suspected incident that compromises or may compromise the security, confidentiality, integrity, or lawful processing of Customer data or systems, or the safeguards implemented to protect them, the Supplier must:

- Notify the Customer within 24 hours of discovery or in accordance with GDPR Article 33 and NIS2 Article 23
- Cooperate fully with the Customer during incident investigation, including providing relevant logs, records, reports, and other required information
- Take all necessary actions to comply with applicable laws and to support the Customer’s obligations
- Recreate any lost Customer data without cost to the Customer
- Provide a corrective action plan within 10 days, outlining measures to prevent recurrence

The Supplier must not notify regulators, customers, or third parties on behalf of the Customer unless explicitly authorized in writing. Any such communications must be reviewed and approved by the Customer prior to release. The Supplier shall participate in coordinated response efforts with the Customer and contribute to incident reviews and improvement activities following any confirmed incident.

The Customer reserves the right to collaborate with the Supplier in investigating any incident affecting or posing a risk to Customer data or systems.

2.7 Business Continuity, Disaster Recovery and Backup

The Supplier must maintain documented and tested Business Continuity and Disaster Recovery Plans based on industry standards (e.g., ISO 22301, ISO 27031). Plans must be reviewed annually, shared with relevant staff, and tested at least once per year.

Critical data must be backed up securely, on a defined schedule, and tested regularly to ensure recovery. Backup failures must trigger alerts and be addressed promptly.

2.8 Data Protection, Retention, Disposal and Privacy

The Supplier must implement appropriate technical and organizational measures to protect Customer Data from loss, unauthorized access, disclosure, or unlawful processing, in accordance with relevant applicable data protection and privacy laws regulations, such as General Data Protection Regulation (GDPR) and Lei Geral de Proteção de Dados (LGPD). The Supplier shall:

- Establish and maintain secure baseline configurations for all systems used to deliver the service
- Apply internationally recognized hardening standards (e.g., CIS, NIST, SANS, BSI, ISF)
- Enable audit logging to track user activity
- Retain data only as required by legal, regulatory, or contractual obligations
- Ensure timely and secure deletion of all Customer information when no longer needed, including electronic data, paper records, and physical media

Suppliers handling payment card data must be PCI DSS compliant.

2.9 Encryption

If Customer Data is part of the service, the Supplier must ensure that it is encrypted both at rest and in transit. The Supplier shall:

- Use strong and current encryption standards and secure cryptographic protocols
- Apply quantum-resistant encryption where feasible
- Manage encryption keys securely in line with industry best practices

All information and systems used to deliver the service must have appropriate access controls and encryption mechanisms aligned with internationally recognized standards. Protection levels must reflect the data classification and applicable regulatory requirements.

2.10 Change Management

The Supplier must maintain a documented Change Management Process that ensures that proposed changes applications or systems; are validated, authorised, tested in a non-production environment and approved prior to deployment.

2.11 Security Monitoring and Logging

The Supplier must ensure that all information systems used to deliver services to the Customer are continuously monitored (24/7) for unauthorized access, anomalous activity, and other security events.

System logs must:

- Be retained for a minimum of 12 months
- Include records of access attempts, configuration changes, and security-related events
- Be detailed enough to support forensic investigations
- Comply with applicable regulatory requirements and approved business needs

The Supplier shall implement accepted methods and procedures to manage and control network performance baselines, ensuring visibility into normal versus abnormal behaviour across relevant systems.

DISCLAIMER: This printed document is an uncontrolled copy and cannot be used unless the content and revision (version) is verified.

2.12 Vulnerability management

The Supplier must maintain a documented vulnerability management process. This must include:

- Regular scanning and monitoring for known vulnerabilities and zero-day threats
- Risk-based prioritization, with critical patches applied within 30 days
- Timely patching of all relevant assets, as per vendor guidance or agreement with the Supplier's cyber security contact
- Notification to users when patching is required
- An up-to-date asset and patch register to track applied patches and identify gaps

2.13 Network Security

The Supplier must ensure that all internet-connected assets used to store, transmit, or process Customer Data are protected by appropriate cyber security controls, such as firewalls and network segmentation.

If the Supplier conducts penetration testing on systems related to the service, it must take necessary precautions to ensure the confidentiality, integrity, and availability of Customer services are not impacted.

2.14 Secure development

The Contractor must ensure security is integrated into the development lifecycle. This includes:

- Adopting secure coding practices.
- Conducting regular security assessments, such as code reviews and security testing.

2.15 Physical security

If access to Customer premises is required, the Supplier shall ensure that only authorized personnel are granted entry, and only to approved areas. Unauthorized access to other parts of the premises is strictly prohibited.

The Supplier must ensure that all locations processing or storing Customer Data are protected by effective physical security controls aligned with standards such as ISO/IEC 27001, IEC 62443, or equivalent. This obligation extends to all subcontractors involved in service delivery.

2.16 OT Products and Services

Where the Supplier provides products or services involving Industrial Control Systems (e.g. SCADA, PLCs), the following requirements apply:

- Proposed support timelines must be included in the Supplier's offering.
- The Supplier must notify the Customer of any product security issues within 30 days of discovery, including issues in dependencies, and provide a timely response with either a patch or a mitigation plan.
- Products must be delivered in a hardened state, free from known vulnerabilities or with available, cost-free patches. Hardcoded passwords must not be used.
- All products must be scanned and verified as free from known malware.
- For computing devices, the Supplier must provide documentation on secure configuration, including:
    - Securing network connections and remote communication features
    - Disabling unnecessary ports, protocols, and services
    - Enforcing credential-based access and least-privilege configurations

DISCLAIMER: This printed document is an uncontrolled copy and cannot be used unless the content and revision (version) is verified.

- Replacing default credentials

These requirements apply to all embedded firmware, BIOS, and software components, including third-party and open-source software.

The Customer reserves the right to perform independent security testing and scanning of Supplier-provided equipment.

The Supplier must provide backup and recovery procedures, and where integration with Customer systems occurs, supply network diagrams and asset inventories.

2.17 Suppliers providing Industrial Control Systems including SCADA

If the agreement includes Industrial Control Systems (ICS), including SCADA, the following requirements apply:

- **Safety Awareness**: Supplier personnel must be trained annually and comply with both Supplier and Customer safety regulations.
- **ICS Access**: If authorized, access to Customer ICS systems must:
  - Use up-to-date, vendor-supported systems with antivirus, patches, and physical security
  - Be documented, including connection details and named personnel
  - Be removed when no longer needed, with timelines and scope shared with the Customer
- **Remote Access**: Only approved Customer remote access solutions may be used. Any deviation must be authorized and include strong authentication and security controls.
- **Disconnection Plans**: Supplier and Customer must prepare disconnection and recovery plans in case of emergency shutdowns.
- **Maintenance Devices**: Equipment used for ICS maintenance must be malware-free and not pose a risk to ICS operations.
- **System Changes**: All modifications must include a documented change plan before work starts and a final change record after completion.

3 Audit Rights

The Customer reserves the right to audit the Supplier's compliance with security, privacy, and contractual obligations at any time with reasonable notice. Audits may be conducted by the Customer or a third-party auditor under confidentiality obligations.

The Supplier must fully cooperate, provide access to relevant systems, documentation, personnel, and premises, and remediate any findings within an agreed timeframe. Upon request, the Supplier shall also share results from internal or external audits and penetration tests.

The Supplier shall support audits by regulators or authorities in jurisdictions where the Customer operates.

4 Supplier Acknowledgment

The Supplier acknowledges that failure to meet these requirements may lead to consequences, including penalties or termination of the contract. Compliance will be monitored through regular audits and reviews.