INSERT LOGO

Supplier Security Policy

Classification: Internal

This document may only be shared internally without prior confirmation from the owner.

Version	Approved By	Owner	Date Last Updated	Review Frequency	Next Review	Comments

Contents

Purpose of This Document

This document outlines the policy for managing supplier and partner relationships in line with the Information Security Management System (ISMS) and relevant legal/regulatory standards.

It guides selecting appropriate suppliers and helps ensure the contracts with them include the clauses that [Company Name] requires to ensure Information Security compliance.

Scope

This policy aligns with the broader context of [Company Name]'s Information Security Management System (ISMS). It is designed to integrate seamlessly with the overall ISMS framework and contribute to the organisation's information security objectives.

This policy pertains to all suppliers and partners influencing [Company Name]'s data confidentiality, integrity, and availability.

Primary users include top management and individuals overseeing [Company Name]'s supplier and partner relationships.

Relationships with Suppliers and Partners

Risk Identification

- As outlined in the SaaS Policy, risks associated with suppliers, partners, ICT, and product supply chains are pinpointed during the risk assessment.
- The IT Director or Head of Applications and Software determines if further risk assessments are needed for individual suppliers or partners, considering contract size, data sensitivity, or service criticality.

Screening

The [Insert Role Here – Such as IT Director] evaluates the necessity and depth of background checks on suppliers or partners.

Criteria include:

- Contract size.
- Data sensitivity.
- Service criticality.

Potential verification methods might encompass client testimonials, credit checks, or onsite audits. This non-exhaustive list adjusts to supplier or partner risk profiles.

The goal is to verify the suppliers' or partners' trustworthiness in safeguarding [Company Name]'s data.

INSERT LOGO

Contracting

- The Security Officer, with legal counsel, determines the security clauses for contracts with suppliers or partners based on risk outcomes.
- Every contract mandates confidentiality clauses and asset return terms upon contract end. Contracts should also outline service levels, especially for cloud service providers.
- The Security Officer might also necessitate specific supplier or partner employees to sign confidentiality or non-disclosure agreements for [Company Name] work.
- A designated contract owner monitors the supplier or partner's compliance and is the primary liaison throughout the contract's life.

Training & Awareness

- The contract owner, with the Security Officer, identifies those needing security training from the supplier or partner. The training, overseen by the Security Officer, should be regular, encompassing crucial security protocols, and be updated when significant security or supplier role changes occur.
- Suppliers and partners should verify staff training completion, showcasing their commitment to [Company Name]'s security standards.

Monitoring & Review

- All suppliers will be evaluated using the Supplier Performance Review record, which will be maintained for the duration of their engagement with [Company Name].
- The contract owner routinely evaluates supplier or partner service levels and security clause adherence.
- An annual audit of the supplier or partner is essential, with onsite audits for high-risk entities.
- The Security Officer must be promptly informed of any security incidents.
- Metrics will be established to evaluate the performance of this Supplier Security Policy. A process for conducting internal audits focused on supplier security management will be implemented to ensure ongoing compliance and effectiveness.

Commented [A1]: See R5 - Supplier Performance Review record.

Contract Changes or Termination

- Proposals to amend or end contracts with suppliers or partners originate from the contract owner and are assessed by the IT Director.
- If approved, the Security Officer conducts a fresh risk assessment to comprehend security implications and potential new risks.
- A clear exit strategy, considering business continuity and data security, is crucial during terminations.

Access Termination & Asset Return

- Post-contract change or termination, partner or supplier employee access must be annulled within 24 hours, aligned with the Access Control Policy.
- Asset return, including equipment, software, or data, should be completed within 7-14 days post-termination, with any deviations formally agreed upon.

Managing Contracts & Reviews

- Expired contracts with suppliers or partners are retained for five years and stored in [Location].
- Monitoring and review records are also preserved for five years post-review and housed in [Location].

Contractual Security Provisions

Based on risk assessments, contracts with suppliers and partners should factor in the following security elements:

Security Clauses for Contracts

The following is a list of clauses that should be checked in any agreement [Company Name] undertakes with a third party.

Compliance with [Company Name] Policies & Procedures

Suppliers must align with [Company Name]'s ISMS and associated security standards. Any supplementary security directives from [Company Name] during the contract's term must also be adhered to.

Confidentiality

Suppliers must preserve the confidentiality of [Company Name]'s sensitive data, including customer details, trade insights, intellectual assets, etc. Disclosure to third parties requires [Company Name]'s explicit written agreement.

Ensure a Non-Disclosure Agreement (NDA) is in place.

Incident Notification

Suppliers must swiftly report any security breaches affecting [Company Name]'s data's safety or integrity. They should also assist [Company Name] in incident inquiries and implement preventive measures against future breaches.

Access control

Controlled Access Suppliers should permit access to [Company Name]'s assets solely to validated individuals, employing robust authentication processes and maintaining credential secrecy.

Data Safeguarding

Suppliers should adopt suitable technical and organisational strategies to prevent unauthorised data actions, encompassing data encryption, protected storage, and routine backups.

Staff Vetting

Employees of suppliers accessing [Company Name]'s data should undergo background screenings, sign confidentiality agreements, and receive periodic security training.

Security Review Allowance

[Company Name] should be able to assess the supplier's security adherence periodically. Suppliers must grant full access and cooperation to [Company Name] during such assessments.

Oversight of Subcontractors

If suppliers engage subcontractors for [Company Name], they must ensure these subcontractors observe the same security guidelines and monitor their compliance.

System Update Obligation

Suppliers are tasked with ensuring their systems' security by updating them as needed. They should notify [Company Name] of significant system alterations impacting data security.

Business Resilience

Suppliers should maintain contingency and recovery strategies to guarantee service continuity for [Company Name] and be ready to share these plans with [Company Name] upon request.

Contract Conclusion Measures

Suppliers must return all [Company Name]-owned assets and erase any data replicas at a contract's end unless legal stipulations or [Company Name]'s written consent dictate otherwise.