Policy for Information Security in Supplier Relations

Document type	Topic specific policy
Managed by	Head of IT Division
Approved by	Director of Organization and infrastructure
Valid from	12.06.2023
Next revision within	12.06.2025
Classification	Open
Reference ISO	ISO27002:2022 5.10,5.19,5.20
Reference NSMs principles for ICT security	1.3.3c, 2.1.4
Reference Law/Rule	eGovernment Regulations (eForvaltningsforskriften)
Reference internal documents	Superior Information Security Policy

1. Purpose

The purpose of this policy is to ensure that NTNU's suppliers protect NTNU's information assets and do not pose a risk to NTNU's information security, i.e., to secure information following requirements of confidentiality, integrity, and availability.

2. Applies to

The policy applies to all procurers and individuals with responsibility for follow-up in supplier relationships.

3. General Principles

a. The information security requirements outlined in NTNU's "Information Security Policy" with underlying topic specific policies and procedures shall apply to external suppliers.
b. External suppliers must receive sufficient training on NTNU's information security requirements when they are granted physical or logical access to ICT infrastructure used to access, transport, or store information assets classified as Internal, Confidential, or Strictly Confidential. NTNU's ICT infrastructure encompasses all equipment, digital information, information systems, and services used for information processing and communication.
c. External suppliers must sign an access agreement before being granted physical or logical access to ICT infrastructure used to access, transport, or store information assets classified as Internal, Confidential, or Strictly Confidential.
d. NTNU must maintain an up-to-date supplier list in an archival system.

e. NTNU must have procedures for managing supplier agreements. Deliverables shall be regularly evaluated and reviewed to ensure compliance with information security requirements.

4. Documentation and Management Requirements

4.1. Documentation Requirements

The supplier list must include the following:

a. Supplier's name.
b. Supplier's contact point for contract execution.
c. NTNU's contact point for contract execution.
d. Duration of the agreement.
e. Link to the agreement, including any changes made after signing the contract.
f. Overview of the areas covered by the agreement.
g. Access rights granted to the supplier for NTNU's ICT infrastructure and/or information assets.
h. The classification level of the information the supplier is given access to.
i. Whether the supplier processes personal data on behalf of NTNU and if a written data processing agreement is in place (with a link to the agreement, if applicable).
j. Whether the services provided by the supplier are considered critical for the operational status of NTNU's ICT infrastructure.
k. Completion of a risk assessment if data containing personal information is to be transferred to the supplier or if the supplier is to be given access to such data during the agreement period.

4.2. Supplier Management

The following information should be included:

a. Allocation of roles and responsibilities in contract management.
b. Information flow between the roles.
c. Necessary control points to verify that the requirements of confidentiality, integrity, and availability (CIA) are met by the supplier.
d. How cooperation with the supplier should be conducted in the event[1] of a serious incident or crisis[2].
e. Ensuring that all information and assets are returned or deleted upon termination of the agreement.

[1]Policy for Digital Incident Management and Disaster Recovery
[2] Policy for emergency at NTNU

5. Roles and Responsibilities

5.1. Head of Financial Division

a. Responsible for maintaining an overview of supplier agreements that may impact information security.
b. Responsible for establishing a routine for supplier management.

5.2. Head of HR and HSE Division

a. Responsible for ensuring that managers and employees are aware of and have sufficient competence to fulfil their responsibilities according to this policy.

5.3. Head of IT Division

a. Must be consulted regarding changes to the policy.

5.4. System Owner

a. Responsible for ensuring all necessary agreements with external suppliers are in place, including data processing agreements if relevant.

5.5. System Administrator

a. Responsible for safeguarding the interests of the system owner regarding the content of the agreement(s) with the supplier(s).
b. Must make internal and external requests according to the contract(s) when needed.
c. Must notify the system owner of any necessary changes to the contract(s).

5.6. Line Manager

a. Must ensure sufficient training in collaboration with the IT Division and HR and HSE Division and signing of all necessary agreements.
b. Must assess and request necessary access rights.