Policy for Network and Information Transfer

Type of document	Topic specific policy
Managed by	Head of IT Division
Approved by	Director for Organization and Infrastructure
Valid from	12.06.2023
Next revision within	12.06.2025
Classification	No
Reference ISO	ISO 27002:2022 5.14, 8.12, 8.21 – 8.23
Reference NSMs principles for ICT-security	2.3.10, 2.5.1-2.5.6, 2.5.8, 2.7.4
Reference Law/Rule	Act relating to the processing of personal data (The Personal Data Act), Act relating to Control of the Export of Strategic Good, Services, Technolgy, etc.
Reference internal documents	This topic spesific policy is subject to the Policy on Information Security.

1. Purpose

The purpose of this policy is to secure information against loss or misuse during transfer between internal systems at NTNU, electronic transmission of information to external parties, or transfer of information to other media that can be used to store data (storage media) that is not part of NTNU's protected ICT infrastructure. NTNU's ICT infrastructure refers to all equipment, digital information, information systems, and services used for information processing and communication.

2. Applies to

The "Policy for Network and Information Transfer" applies to all individuals who have access to, and/or process and manage information through NTNU's network.

3. General Principles

a. Measures should be implemented to enhance the ability to detect attacks and reduce the attack surface within the network.
b. Information in transactions to and from application services should be protected to prevent incomplete transmission, incorrect routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, or repetition.
c. When using external systems, a data processing agreement approved by Division for Governance and Management Systems must be established.
d. Research and knowledge that can be misused should be subject to export control following the Export Control Act and regulated by the "Policy for Control of Knowledge Transfer."[1]
e. During verbal communication outside of NTNU premises, participants must be aware of their surroundings and the content of their communication to prevent classified information from being compromised.

4. Network

4.1. Network Controls

NTNU’s data network is defined as the network owned and operated by NTNU on all campuses. This includes the core network and all network components connected to it. It also includes all internet connections in and out of NTNU, as well as any leased lines between NTNU and partners. To secure access to this network, the following controls must be implemented:

a. Client networks should have authentication for both wired and wireless networks (IEEE 802.1x).
b. Firewalls must be used to control network traffic, including firewalls on servers.
c. Firewall logs must be managed according to the requirements in the "Operational Security Policy."
d. External access to the network zones Intern, Confidential, and Strictly Confidential must be through encrypted connections with secure authentication, which can be achieved using e.g., VPN and/or Microsoft Direct Access. The solutions must have multi-factor authentication to prevent logging in with just a username and password.

4.2. Security of Network Services

The following measures should be implemented to secure NTNU’s data network:

a. Network equipment must be physically secured based on the requirements in the "Policy for Physical Security of ICT Infrastructure."
b. Network components must be configuration-managed to always ensure an up-to-date network.
c. Redundant connections must be established where availability requirements demand it.

[1] https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/om-eksportkontroll/kunnskap/id2500543/

d. The quality of network service should be clearly defined, whether provided by NTNU IT or external vendors.

4.3. Network Segregation

Network segregation is a prerequisite for achieving a higher level of information security. The following requirements are set:

a. User equipment must be isolated in separate zones. Where possible or appropriate, clients should also be separated from each other to avoid client-to-client infections (Private VLAN).
b. The network must be able to isolate compromised user equipment.
c. The network must have separate zones for user equipment with different security levels based on the following classification:
    - Unknown devices – for open information only
    - Registered private devices – for up to internal information.
    - Managed devices – for up to confidential information
    - Managed devices with higher access control – for up to strictly confidential information
d. Servers must be placed in network zones based on the classification of information.
e. Separate network zones must be established for open, internal, confidential, and strictly confidential information.
f. Network segregation must be enforced through firewalls.
g. Network traffic from servers in the internal, confidential, and strictly confidential zones must only reach the internet via a proxy.
h. Laboratory equipment must be placed in a separate zone and must not be directly accessible from the internet.

5. Information Transfer

a. All information transfers involving Confidential and Strictly Confidential classified information must have mechanisms to verify integrity.
b. Transactions of Confidential or Strictly Confidential classified information must be encrypted or otherwise secured to ensure information security2
c. Audit logging must be implemented for transactions containing personal data and Confidential or Strictly Confidential classified information. The log must meet the requirements for change tracking and access.
d. When transferring contract-regulated/legal-regulated information to an external party, a data or information processing agreement must always be in place.

5.1. Electronic Messaging Exchange

The following requirements apply to transfers via email or other electronic messaging systems:

[2] Policyfor use of cryptographic controls

a. Confidential or Strictly Confidential information transmitted via email or other electronic messaging services must be encrypted according to the "Policy for the Use of Cryptographic Controls."

5.2. Confidentiality or Non-Disclosure Agreements

The following requirements apply to confidentiality or non-disclosure agreements when processing classified information:

a. When transferring Intern, Confidential, or Strictly Confidential classified information to an external party, a signed agreement must be in place to protect NTN's rights and obligations related to information transfer.
b. NTNU employees must be bound by confidentiality agreements for personal data where confidentiality is necessary.
c. Confidentiality agreements must also cover other information with relevance to information security.

6. Roles and Responsibilities

6.1. Head of the IT Division

a. Is responsible for implementing the requirements of the "Network and Information Transfer Policy" in the organization.

6.2. Head of HR and HSE Division

a. Is responsible for ensuring that NTNU has established satisfactory confidentiality agreements that meet the information security requirements outlined in this policy.
b. Is responsible for ensuring that managers are aware of and possess sufficient competence to fulfil their responsibilities according to this policy.

6.3. Head of IT Infrastructure Section

a. Is responsible for developing procedures that uphold information security in all phases of IT operations.
b. Is responsible for ensuring that systems are operated and decommissioned following this policy.

6.4. Head of Digital Security Section

a. Is responsible for setting requirements for securing information within the network or information transferred to others.
b. Is responsible for providing policies to secure the network.
c. Is responsible for implementing measures to reduce network vulnerabilities.

6.5. Line Manager

a. Is responsible for utilizing confidentiality agreements within their unit following the requirements of this policy.

6.6. System Owner

a. Is responsible for developing, implementing, operating, and decommissioning systems for which they are the system owner, following the requirements of this policy.

6.7. Project Manager

a. Is responsible for utilizing confidentiality agreements in the project in accordance with the requirements of this policy.

b. Is responsible for ensuring that information transferred during the project period is secured according to this policy.