Policy for Operational Security

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 5.8, 5.21, 5.23, 5.30, 7.5, 7.11, 7.12, 8.6-8.9, 8.12-8.17, 8.19, 8.20, 8.25-8.34
Reference NSM's principles for ICT-security	1.1.5, 1.2.1-1.2.4,2.1.1-2.1.3, 2.1.5-2.1.9, 2.2.1-2.2.5,2.2.7,2.3.1-2.3.6,2.3.9 ,2.4.3,2.8.3,2.8.4,2.9.1-2.9.4, 2.10.1-2.10.4, 3.1.1, 3.1.3, 3.2.1-3.2.7
Reference Law/Rule	
Reference internal documents	This policy is subject to the Information Security Policy at NTNU.

1. Purpose

The purpose of this policy is to ensure the stable and secure development and operation of NTNU's information systems, as well as detect issues in the ICT infrastructure. This will be achieved by increasing the quality and ensuring the reliability of services provided by NTNU through targeted measures and requirements.

2. Applies to

The Policy for Operational Security applies to all individuals who have access to, operate, and manage NTNU's information systems, services, and equipment (NTNU's ICT infrastructure).

3. General Principles

a. Systems directly connected to the fixed network must be kept up to date and managed by NTNU IT or specialized IT personnel at department level.
b. Systems permanently connected to the fixed network must log to a central logging solution.
c. Systems temporarily connected to the fixed network must have a defined timeframe for discontinuation.
d. Systems in the production, testing, and development phases must be adequately documented for secure operation and usage.
e. Development and testing of systems must be conducted in separate environments with a defined procedure for transitioning between development, testing, and production.
f. NTNU must have a comprehensive system for both active and passive monitoring of the ICT infrastructure, systems, and services.

g. NTNU must implement measures that detect, protect against, and support centralized management of unwanted software and malware.
h. Additional measures and requirements beyond this policy may be imposed to ensure security based on risk and threat assessments.
i. Password lifetimes for APIs must be changed regularly, every second year at a minimum.

4. Documentation

NTNU must have a comprehensive overview of all systems and services in production, as well as an overview of all systems and services that are in test and/or development. This overview must at least contain software, operation system, hardware, classification, and system owner.

4.1 System Documentation and Operation Procedures

System documentation must describe how the system or service is implemented. It should also contain standard operation routines and associated user documentation when relevant. NTNU must have system documentation for all systems in production, as well as all functional and/or critical systems in test and/or development.
The following requirements apply:

a. The system documentation must describe the setup of systems and services that comply with NTNU's information security policy.
b. The system documentation for a system must include significant elements that the system is composed of and the dependencies between these elements.
c. The system documentation must be regularly maintained and updated when changes are made.
d. The system documentation must be of such quality that it allows for rebuilding the system or service and can be used for troubleshooting during incidents.
e. Information about system(s) with a link to the documentation must always be up to date in the IT Service Portal.

4.2 User Documentation

a. User documentation should describe the secure and recommended use of NTNU's information systems that preserve with NTNU's information security policy.

5. Safe Development

a. The requirements for information security in an ICT system apply regardless of whether the system is developed through customization or if it involves adaptations in a standardized ICT system.
b. Procedures for designing, developing, and managing ICT systems at NTNU should be based on the recommended policies from the Norwegian Data Protection Authority for developing software with embedded privacy, according to checklist[1].
c. Leaders of departments involved in designing, acquiring, developing, and/or managing ICT systems at NTNU must be able to document how they have systematically approached the

[1] Checklist https://www.datatilsynet.no/regelverk-og-skjema/veiledere/programvareutvikling-med-innebygd-personvern/.

recommendations for secure development in each area of the Norwegian Data Protection Authority's policies for software development with embedded privacy. Alternatively, a corresponding systematic approach must be developed and implemented for all relevant areas within their responsibility.

d. Development, testing, and production occur in separate, distinct environments.
e. NTNU must establish appropriate physical and logical security measures for development environments in system development that cover the entire development process.
f. Development and testing related to information systems with information classified at level 3 or 4 according to NTNU's "Policy for Information Classification" should be carried out on dedicated and secured networks.
g. Systems in testing or development must not be connected to the internet unless there are specific requirements for exceptions.
h. Production data containing personal information must not be transferred to development or testing unless there is a legal basis to do so.
i. Sensitive data must not be transferred to development without conducting a risk assessment and obtaining approval from the risk owner.
j. Authentication mechanisms and users in testing and development must be separated from production and be controlled and traceable.
k. NTNU must oversee and monitor activities related to outsourced system development to ensure that information security requirements are upheld.

6. Operations and Monitoring

6.1 Change Management

Change management is an established process for managing changes in services, systems, and applications operated by NTNU. The process must be based on the ITIL framework. To ensure information security, the following requirements for change management must be adhered to:

a. NTNU must have change management for all systems in production.
b. NTNU must register changes that can affect security.
c. NTNU must have a routine that describes the transition from development to testing and from testing to production.
d. NTNU must have a routine for change management of significant changes to ICT systems.
e. NTNU should have change management for systems in testing and development.

6.2 Capacity Management

To avoid unnecessary resource consumption, there are requirements for capacity management:

a. At specified intervals, resource consumption, systems, and services must be evaluated to identify what can be discontinued or consolidated.
b. Procedures must exist for decommissioning systems/services, optimizing and releasing resources, as well as cleaning up and securely deleting data.

6.3 Configuration Management

Components in services and systems must be centrally configured and updated. The following requirements are set:

a. Configuration management must be based on FitSM for configuration management.
b. Systems and applications in production must be managed through central configuration tools.
c. Disposal of IT equipment must follow procedures for disposing of storage media.

6.4 Technical Vulnerability Management

To protect information and digital infrastructure, a process for vulnerability management must be established. The following requirements are set:

a. NTNU must have a routine for technical vulnerability and attack surface monitoring.
b. NTNU must perform vulnerability risk assessments and implement necessary measures to limit the risk of negative impact on the organization.
c. NTNU must have procedures for security updates of operating systems, software, and hardware on all equipment connected to or part of NTNU's digital infrastructure.
d. Systems directly connected to the fixed network or permanently connected to NTNU's network must have central vulnerability monitoring where possible.

6.5 Protection Against Physical Events

a. Areas containing infrastructure that represents high vulnerability/risk to the availability of critical or major parts of NTNU's information sources must have physical protection against natural disasters, sabotage, and accidents.
b. For areas containing infrastructure that represents high vulnerability/risk to the availability of critical or major parts of NTNU's information sources, a continuity plan must be developed and tested to be activated during critical events.
c. Power and data cables must be protected against interception and damage.

6.6 Protection Against Malware

NTNU must have measures that detect, protect against, and support centralized management of unwanted software and malware. The following requirements apply:

a. NTNU must continuously assess measures against malware based on risk and vulnerability assessments, as well as the threat landscape against NTNU.
b. NTNU must have updated and centrally managed anti-malware agents on all clients, servers, and devices permanently connected to the network.
c. NTNU requires that devices that connect to networks must have installed security updates and have up-to-date malware protection.

6.7 Backup

There are requirements for establishing backups where necessary to ensure information security. The following requirements are:

a. A backup must be established based on the system's classification and external or internal backup requirements.
b. Backup must be secured so that it is not stored in the same room or near the system being backed up.

c. It must be possible to make an encrypted backup if the classification indicates this.
d. The backup solution must support differentiated security levels.
e. Backups must have access control following the principles and requirements in the policy for access control.
f. Access to backed-up data must be logged.
g. Backup must function appropriately and be regularly verified according to operational procedures.
h. Regular restoration tests from backups must be conducted.
i. Software defined as critical for the organization according to the "Policy for Classification of Information Objects" must be backed up to ensure recovery.

6.8 Log Collection and System Monitoring (Event Management)

Efficient and secure operation of ICT infrastructure depends on knowing the status of systems, services, and infrastructure to detect abnormal activity or deviations from normal operation. NTNU must have a comprehensive system for both active and passive monitoring of ICT infrastructure, systems, and services. Logging and monitoring are the basis for operational security and good service quality.

6.8.1 Logging at NTNU

a. All systems permanently connected to NTNU's network must log in to a central logging solution.
b. A local copy of the log must be retained for 7 days.
c. Logs must be centrally analysed to detect errors, availability, and security incidents.
d. Collection, processing, and storage of system and application logs must be done on a separate central platform. This platform must be separated from other systems and located in NTNU's data centre.
e. All systems/services connected to NTNU's fixed network must ensure the correct time and date and use the NTNU network-based time server.
f. Logs must be stored encrypted on hardware separate from other IT systems with strict access control.

6.8.2 Operational Monitoring at NTNU

a. NTNU must have central operational monitoring of systems and applications in production.
b. Systems in production must monitor at a minimum:
   - Performance and resource utilization (CPU, disk, bandwidth, etc.)
   - Status of services to a degree that can be used to calculate service quality.
c. The central monitoring platform must be independent of other systems.

7. Roles and Responsibilities

7.1 Head of the IT Division

a. Responsible for implementing the requirements in the "Policy for Operational Security" in the organization.

b. Responsible for reporting on the degree of implementation, effect and efficiency of secure development work.

7.2 Head of HR and HSE Division

a. Responsible for ensuring that managers are familiar with and have sufficient competence to fulfil their responsibilities according to this policy.

7.3 Head of Digital Security Section

a. Responsible for ensuring that the unit has sufficient competence and tools to meet the requirements in the "Policy for Operational Security".
b. Responsible for systems and procedures for technical vulnerability management in the organization.
c. Responsible for establishing a central logging system in the organization.
d. Responsible for providing central solutions for malware protection in the organization.
e. Responsible for central security monitoring and analysis.
f. Responsible for approving changes that may affect the security of NTNU.
g. Can impose additional security measures on the organization beyond what is mentioned in this policy based on threat and risk assessments.

7.4 Head of IT Development Section

a. Responsible for developing procedures that ensure information security in all phases of ICT development.
b. Responsible for ensuring that employees have the competence to meet the requirements for secure development according to this policy.

7.5 Head of IT Infrastructure Section

a. Responsible for ensuring that the unit has sufficient competence and tools to meet the requirements in the "Policy for Operational Security".
b. Responsible for central operational monitoring of the organization.
c. Responsible for backing up shared systems and infrastructure.
d. Responsible for implementing mandated security controls in the infrastructure promptly and without undue delay.

7.6 Head of IT Management Section

a. Responsible for developing procedures that ensure information security in all phases of ICT governance.
b. Responsible for ensuring that employees have the competence to meet the requirements for secure development according to this policy.

7.7 Head of IT Support Section

a. Responsible for ensuring that the unit has sufficient competence and tools to meet the requirements in the "Policy for Operational Security".

7.8 Head of Transaction Services Section

a. Responsible for developing procedures that meet the requirements for information security in supplier agreements and contract management

7.9 System Owner

a. Is responsible for the requirements of regular quality assurance of information security throughout the entire lifecycle of the ICT system.
b. Is responsible for ensuring that systems and services are delivered according to the requirements stated in the policy.
c. Is responsible for registering the system in NTNU's central overview of IT systems - IT Service Portal.
d. Is responsible for keeping the documentation updated and accurate.
e. Is responsible for ensuring that the requirements for functionality and user interface of the IT system do not conflict with the requirements for information security.
f. Is responsible for ensuring the availability of relevant training material for secure and efficient use of the system.
g. Is responsible for subjecting the IT system to internal control.

7.10 System Manager

a. Is responsible for managing the system according to the information security requirements documented by the system owner in the IT Service Portal and other available documentation related to development, operation, and management.
b. Must provide advice and content for training and ensure its availability where relevant.
c. Must ensure that all development, operation, and management activities comply with the current policies for these areas.
d. Is responsible for acceptance testing before the IT system is put into production, including the development of criteria, test plan, and execution of acceptance testing.

7.11 System Developer

a. Is responsible for secure coding, with particular responsibility for testing, detecting, and reporting discrepancies or suspected vulnerabilities.