Policy for Risk Management in Information Security

Document type	Topic specific policy
Managed by	Head of Division for Governance and Management Systems
Approved by	Director of Organization and infrastructure
Valid from	20.06.2023
Next revision within	20.06.2025
Classification	Open
Reference ISO	ISO27005:2011
Reference NSMs principles for ICT-security	1.1.3, 1.1.4, 2.1.10
Reference Law/Rule	The Personal Data Act
Reference internal documents	Superior Policy for information security

1. Purpose

The purpose of this policy is to help prevent unwanted incidents or deficiencies in information security at NTNU that may have consequences for students, employees, and/or society in general.

2. Applies to

The policy applies to everyone with responsibility for a process, project, procurement, development, or operation of a system. This includes leaders, system owners, process owners, project leaders, and those responsible for research.

3. General Principles

a. NTNU must have an approach to information security that is based on risk assessments.
b. NTNU's aim with risk management is to assess risks and address unacceptable risks through measures. The remaining risks must be accepted by a leader.
c. Systems and processes involving the processing of information assets must undergo risk and vulnerability assessments (ROS). This must be done at least every second year, and/or upon significant changes in organisation, processes, ICT systems, or threat landscape. This is to ensure an up-to-date understanding of risks and vulnerabilities.

4. Risk and Vulnerability Analysis

Risk is defined as one or more undesirable scenarios described by the combination of potential consequences and their associated likelihood. Control of risk is performed through risk management. Risk management is an important principle in internal control and refers to

a coordinated set of activities and methods used to guide the organization and control the various risks that can impact goal attainment.

The risk management process is standardized by the ISO/IEC 27005:2011 standard and NTNU mainly follows this process for information security.

a. **Establish context** for the risk assessment, this means to determine the object of the assessment and decide what is not included. As a part of this step, specific risk criteria are elaborated for the current risk assessment, where Confidentiality, Integrity, and Accessibility must be included.
b. **Risk identification** to identify and assess values, threats, and vulnerabilities in the ICT system or work process through three activities:
    i. Value assessment comes first as it determines the protection requirements for the solution. For example, a system handling sensitive personal data will have specific requirements for data management, which sets the premise and security level for the rest of the assessment.
    ii. The next step is threat assessment, aiming to identify the most relevant threats that are motivated to compromise our information values. A threat is a source of risk typically associated with planned actions intending to harm systems or organizations. In addition to estimating the threat's motivation and capability to attack, the frequency of the threats occurring at NTNU must be assessed.
    iii. The existing security mechanisms (controls and measures) used in the solution are then mapped and evaluated. Controls and measures are assessed based on the values they aim to protect.
    iv. The next step is to identify and assess vulnerabilities in the ICT system or work process that can be exploited by a threat to gain access to a value.
    v. The results of the value, threat, and vulnerability activities are used to identify the existing risk and the potential unwanted incidents and consequences it can lead to (risk scenario).
c. **Risk analysis** is conducted to estimate the consequences and associated likelihood of identified scenarios. The analysis aims to identify the most severe risks that need to be prioritized.
d. **The first decision point** is whether the risk assessment is comprehensive enough to proceed. In some cases, the assessors may have identified areas of significant uncertainty and therefore need to conduct a more thorough investigation to achieve a satisfactory risk assessment.
e. **Risk management** is the process of modifying risk with the intention of making it acceptable. This is done by selecting measures that reduce the risk to an acceptable level. There are primarily four approaches to risk management: (i) risk reduction, (ii) risk avoidance, (iii) risk transfer/sharing, and (iv) risk acceptance as is. The decision on prioritizing measures is based on cost-benefit analysis, where the effectiveness in

terms of risk reduction and the cost of the measure is evaluated. In some cases, it may be possible to increase the risk to take advantage of an opportunity.

f. **The risk owner (responsible manager in the line organization) assesses whether the residual risk is acceptable.** If the risk owner does not accept the remaining risk after the planned risk-reducing measures have been implemented, new measures must be evaluated and implemented until an acceptable risk level is achieved.
g. **Risk monitoring and evaluation.** The risk assessment is reviewed every two years, and if there are significant changes to the system or process.

4.1. Risk Criteria

Risk criteria are the criteria used when deciding on acceptable risk. Such criteria can be expressed in words, numerical, or based on combinations. The criteria are based on regulations, standards, experiences, or theoretical knowledge.

a. For risk assessments, criteria must be drawn up within confidentiality, integrity, and accessibility.
b. The following consequences of a breach of information security must be considered:
    i. Damage to materials or individuals
    ii. Economics
    iii. Reputation
    iv. Protection of personal data

4.2. Acceptance of Risk

Acceptable risk is when risk is accepted in a given context based on the current values in the organization. What is defined as an acceptable risk can change over time and vary in different areas. A limit for unacceptable risk is defined based on risk criteria. Risks that are considered unacceptable should be reduced as much as practicable. The decision of what is perceived as practically possible will most likely be based on a benefit/cost assessment. This will determine if, and to what extent, the risk-reducing measures will be implemented. Acceptance of risk must be presented to and decided by the line manager. The line manager can accept a risk if the consequences can be tolerated within their unit. If the consequences go beyond this, the acceptance of risk must be submitted on a higher line level. Acceptance of risk is done by approving the risk and vulnerability analysis with a date. The signing date sets the validity period for the risk and vulnerability analysis.

When identifying unacceptable risks that may have consequences beyond the scope of the current risk and vulnerability analysis and/or result in significant consequences beyond their decision authority, this risk must be reported upwards in the line.

Risks that are not accepted:

a. Consequences that lead to violations of laws and regulations.

b. Consequences that may cause greater damage to NTNU as an organization.

4.3. Checkpoints, Measures, and Routines

a. All risk criteria must have established checkpoints and measures in terms of the determined risk acceptance.
b. All risks must have determined routines for the assessment of checkpoints and measures.
c. Handling discrepancies must be a part of the risk management process.

4.4. Scope of Risk Assessment

The scope of the risk assessment is decided based on the system/process requirements for confidentiality, integrity, and accessibility.

Level	Confidentiality	Integrity	Accessibility
Level 1	**Open:** Simple assessment of risk to ensure the right level.	**Low:** Simple assessment of risk to ensure the right level.	**Low:** Simple assessment of risk to ensure the right level.
Level 2	**Internal:** Simple assessment of risk and necessary risk-reducing measures.	**Moderate:** Simple assessment of risk and necessary risk-reducing measures.	**Moderate:** Simple assessment of risk and necessary risk-reducing measures
Level 3	**Confidential:** Carry out risk and vulnerability analysis and necessary risk-reducing measures in accordance with the analysis. Consider additional requirements for access management, logging, and revision.	**High:** Carry out risk and vulnerability analysis and necessary risk-reducing measures in accordance with the analysis. Consider additional requirements for verification of information, e.g., checksum. Consider additional requirements for access management, logging, and revision.	**High:** Carry out risk and vulnerability analysis and necessary risk-reducing measures in accordance with the analysis. Consider additional requirements for load balance, redundancy, and restore.
Level 4	**Strictly confidential:** Carry out risk and vulnerability analysis and necessary risk-reducing measures in accordance with the analysis. Consider additional requirements for access management, logging, and revision., e.g., multi-factor authentication.	**Very high:** Carry out risk and vulnerability analysis and necessary risk-reducing measures in accordance with the analysis. Consider additional requirements for verification of information, e.g., checksum. Consider additional requirements for access management, logging, and revision.	**Very high:** Carry out risk and vulnerability analysis and necessary risk-reducing measures in accordance with the analysis. Consider additional requirements for load balance, redundancy, and restore.

NTNU

5. Roles and Responsibilities

5.1. Director of Organization and Infrastructure

a. Is responsible for ensuring that all work related to information security follows an approach based on risk management.
b. Is responsible for developing overriding acceptance criteria for information security and ensuring that these are known in the organization.

5.2. Head of Division for Governance and Management Systems

a. Is responsible for reporting the work with overriding risk management.

5.3. Head of HR and HSE Division

a. a. Is responsible for ensuring that managers are familiar with and have sufficient competence to take care of their responsibilities following this policy.

5.4. Line Manager

a. Responsible for developing a risk matrix with acceptance criteria for their area of responsibility.
b. Must ensure that employees are provided with sufficient training to conduct a risk assessment.
c. Must ensure that a risk assessment is conducted for their area of responsibility.

5.5. Process Owner

a. Is responsible for developing a risk matrix with acceptance criteria for the work process.
b. Is responsible for establishing a process for risk assessment as a supporting process in the work process.
c. Must ensure that sufficient risk assessment of the process is conducted.

5.6. System Owner

a. Is responsible for developing a risk matrix with acceptance criteria for the system.
b. Is responsible for establishing a process for risk assessment as a supporting process if changes in the system.
c. Must ensure that sufficient risk assessment of the system is conducted.

5.7. Project Leader

a. Is responsible for developing a risk matrix with acceptance criteria for the project.
b. Is responsible for establishing a process for risk assessment as a supporting process in the project.