Policy for Classification of Information

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	No
Reference ISO	ISO27002:2022 5.9,5.10,5.12,5.13,8.12
Reference NSMs principles for ICT-security	2.7.5
Reference Law/Rule	Act relating to national security (Security Act) (Sikkerhetsloven), Act relating to the processing of personal data (The Personal Data Act) (Personvernloven),(Sikkerhetsinstruksen [The Safety Instruction]
Reference internal documents	Policy for Information Security

1. Purpose

The purpose of classifying information assets is to have an overview of the information managed by NTNU.

2. Applies to

This policy applies to all individuals who have access to, process and manage information at NTNU, e.g., NTNU's information systems, services, and equipment (NTNU's ICT infrastructure).

3. General Principles

a. To meet the requirements for proper handling of information assets, information objects produced and managed by NTNU should be classified.
b. The classification of information produced or accessed within an ICT system or process establishes requirements for securing the ICT system and the workflow involving the use, transport, or storage of the information.
c. Information/information objects should be classified and labelled as level 1, 2, 3, or 4 within the categories of Confidentiality, Integrity, and Availability to determine the appropriate protection and treatment of the information object.

4. Value Assessment and Classification

An information value refers to information that is defined as something we, as individuals, NTNU, or society, want to protect. Information values can be divided into primary information values, the information itself, and secondary information values, which include premises, systems, and individuals who handle and store information.

a. Information stored and produced at NTNU must undergo a value assessment[1]. This involves determining the value of the object for NTNU and other stakeholders. Examples of information values at NTNU include:
    i. Research – valuable to NTNU as a university, to researchers, and potentially to society.
    ii. Documentation – System documentation, plans, etc.
    iii. Systems – Some systems are valuable because we depend on them to perform our work, while others are used to store valuable data.
    iv. Personal data – This is not valuable to NTNU, but it is valuable to the individuals involved. As a result, NTNU is required to store personal data in a specific manner.
    v. Physical areas – Labs, archive rooms, server rooms, etc., where information and research are created, processed, and stored.
b. Based on the value assessment, the information object is classified according to internal and external requirements for confidentiality, integrity, and availability.
    i. *Confidentiality* implies access control, which means ensuring that information and information systems are only accessible to those with a legitimate need.
    ii. *Integrity* means ensuring that information is accurate, valid, and complete, and cannot be unintentionally or maliciously modified.
    iii. Ensuring *availability* means that information and information systems are available within the specified availability requirements.
c. The requirements for accurate classification of information values come from various parties and have different goals:
    i. Have an overview of the values possessed by NTNU.
    ii. Determine which information/system/object is most important for achieving NTNU's goals, complying with applicable regulations, and fulfilling contractual agreements.
    iii. Prioritize information and ICT systems in the event of limited capacity.
    iv. Simplify the process of building an efficient and cost-effective information architecture.

4.1 *Accessibility* Assessment

Classification	*Level*	*Description*
Very High	4	The information value affects the core operations and is critical for the function of the university.
High	3	The information value affects departments, sections, or shared functions, but not the overall functioning of the university.
Moderate	2	The information value affects only certain isolated systems, services, or functions.
Low	1	The information value is isolated and only affects a single system, service, or a small number of users and has no impact on the functioning of the university or important functions.

[1] NSMs «Veiledning i verdivurdering av informasjon»

NTNU

4.2 Integrity Assessment

Classification	*Level*	*Description*
Very high	4	It is critical that authentic and valid information is delivered. Unintentional or intentional misinformation could lead to misjudgements or decisions with fatal consequences. Errors in the information can result in loss of life, such as incorrect patient treatment or faulty construction in buildings. Breaches can result in corrupt data in central systems, leading to extensive consequential errors and subsequent significant loss of materials produced at NTNU.
High	3	The user of the information relies on it being authentic and valid. Unintentional or intentional misinformation could lead to misjudgements or decisions that could cause significant financial loss, damage to the reputation, or other harm to NTNU, individuals, or partners. This can include, but is not limited to, basic data, research data, and publications where authenticity is crucial.
Moderate	2	The user of the information expects it to be authentic and valid Errors in the information can result in moderate financial damages and/or reputational damage to NTNU, individuals, or partners.
Low	1	Errors do not affect decision-making processes. Working documents where errors in the information do not have negative consequences in the decision-making processes of those using the information.

4.3 *Confidentiality* Assessment

Classification	***Level***	***Description***
Strictly Confidential	4	Strictly confidential is used when the disclosure of information to unauthorized individuals could cause significant harm to public interests, NTNU, individuals, or partners. The information should only be accessible to employees with strictly controlled rights who have a legitimate need for this information to perform assigned tasks. Examples of information in this category: Large amounts of special categories ("sensitive") personal data, large amounts of health information, knowledge/research subject to export control.

Confidential	3	Confidential is used when the disclosure of information to unauthorized individuals could harm public interests, NTNU, individuals, or partners. The information should only be accessible to employees with controlled rights who have a legitimate need for this information to perform assigned tasks. Examples of information: Special categories of personal data (previously known as "sensitive personal data"), including health information, confidential information.
Internal	2	Internal is used for information that is limited to be accessible to employees to carry out assigned tasks. The information may be accessible to external parties with controlled access rights. Examples of information: Working documents, information exempt from public disclosure, various types of personal data.
Open	1	Open information that is accessible to everyone without specific access rights. Information that does not harm anyone or anything and is available to all. Examples of information: Open-source information, public websites, course overviews and content.

4.4 Labelling Requirements

a. When labelling information values, the labelling should be visible.
b. For high confidentiality requirements (Confidential/Strictly Confidential), the information value should be labelled with the classification. The following labels should be used:

c. Information values classified as Internal may be labelled with the following marking:

5. Roles and Responsibilities

5.1. Head of HR and HSE Division

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

5.2. Head of IT Division

a. Must be consulted regarding changes to the policy.

5.3. Head of Digital Security Section

a. Must be consulted regarding changes to the policy.

5.4. Line Manager

a. Is responsible for ensuring that employees have sufficient competence to classify information produced within the department and that information classification is part of the work routines.
b. Must ensure that the department has procedures to secure information processed, manipulated, and stored in ICT systems approved for using, transporting, or storing the information according to its classification.
c. Must ensure that the department has procedures for the secure storage of information made available on paper, following the information's classification.

5.5. System Owner

a. Must specify which classifications of information the ICT system is approved to use, transport, and/or store.