



# Policy for Classification of Information

Document type	Topic specific Policy
Managed by	CISO, Digital Security Section
Approved by	Director of Organisation and Infrastructure
Valid from	01.10.2025
Next revision within	01.10.2027
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

All processing and management of information and data at NTNU falls under this policy. Examples of this include research projects, teaching, administration and case management.

## 3. Roles and Responsibilities

The work on information security affects the organisation at all levels. Responsibility and authority for information security follow the regular line management structure. All roles associated with the management system are defined in the [Information Security Policy](#)

For the Policy for Classification of Information, line managers, project managers, and system owners have key roles with corresponding responsibilities.

## 4. 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.

## 5. Asset Assessment and Classification

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

- a. Information stored and produced at NTNU must undergo an asset. This involves determining the value of the object for NTNU and other stakeholders. Examples of information asset 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 only valuable to NTNU, but it also 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. Prioritise information and ICT systems in the event of limited capacity.
  - iv. Simplify the process of building an efficient and cost-effective information architecture.

## 6. Classification in Practice

Data and information processed at NTNU have varying levels of protection. All information and data must be classified with regard to confidentiality in order to select the appropriate tools and infrastructure. Integrity is also important to ensure that data/information is accurate and not altered by mistake. Availability is often the most critical aspect for system owners, who are responsible for the systems themselves, to ensure they function properly. In practice, the integrity and availability of data

will be well maintained if you use one of the solutions presented in the Storage Guide.

## 6.1 Confidentiality Assessment

<i>Classification</i>	<i>Level</i>	<i>Description</i>	<i>Examples</i>
<b>Strictly Confidential</b>	4	<p>Strictly confidential is used when the disclosure of information to unauthorised individuals could cause significant harm to public interests, NTNU, individuals, or partners.</p> <p>The information should only be accessible to employees with strictly controlled rights who have a legitimate need for this information to perform assigned tasks.</p>	<ul style="list-style-type: none"> <li>• Large volumes of special category (“sensitive”) personal data*</li> <li>• Large volumes of health data*</li> <li>• Research data and datasets of high economic value</li> <li>• Directly identifiable health data in medical and health-related research</li> </ul> <p><small>*You must assess what constitutes large volumes of data in your work based on context, quantity, and type of data.</small></p>
<b>Confidential</b>	3	<p>Confidential is used when the disclosure of information to unauthorised individuals could harm public interests, NTNU, individuals, or partners.</p> <p>The information should only be accessible to employees with controlled rights who have a legitimate need for this information to perform assigned tasks.</p>	<ul style="list-style-type: none"> <li>• Special categories of personal data, including health data, confidential information, and trade secrets</li> <li>• Knowledge/research subject to export control</li> <li>• Personnel files</li> <li>• Certain information about infrastructure (e.g., building security and ICT systems)</li> </ul>
<b>Internal</b>	2	<p>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.</p>	<ul style="list-style-type: none"> <li>• Internal case documents</li> <li>• Working documents</li> <li>• Information exempt from public disclosure</li> <li>• Various types of personal data (national ID number, name, email address, employee ID, employment details, etc.)</li> </ul>

			<ul style="list-style-type: none"> <li>• Various types of research data during project phases (unpublished work and research data)</li> <li>• Grades</li> <li>• Exam submissions</li> </ul>
<b>Open</b>	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.	<ul style="list-style-type: none"> <li>• Open source information</li> <li>• Public websites</li> <li>• Course overviews and content</li> <li>• Published research</li> </ul>

## 6.2 Integrity Assessment

<i>Classification</i>	<i>L</i>	<i>Description</i>	<i>examples</i>
<i>Very high</i>	4	<p>It is critical that authentic and valid information is delivered.</p> <p>Unintentional or intentional misinformation could lead to misjudgements or decisions with fatal consequences.</p> <p>Errors in the information can result in loss of life, such as incorrect patient treatment or faulty construction in buildings.</p> <p>Breaches can result in corrupt data in central systems, leading to extensive consequential errors and subsequent significant loss of materials produced at NTNU.</p>	<ul style="list-style-type: none"> <li>• Errors in health records may result in loss of life</li> <li>• Errors in building plans or foundational infrastructure documentation</li> <li>• Errors in risk assessments of critical importance</li> </ul>
<i>High</i>	3	<p>The user of the information relies on it being authentic and valid.</p> <p>Unintentional or intentional misinformation could lead to misjudgements or decisions that could cause significant financial loss,</p>	<ul style="list-style-type: none"> <li>• Master Data</li> <li>• Research data and publications where authenticity is critically important.</li> </ul>

		damage to the reputation, or other harm to NTNU, individuals, or partners.	<ul style="list-style-type: none"> <li>• Errors in personal data of special categories.</li> </ul>
<i>Moderate</i>	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.	<ul style="list-style-type: none"> <li>• Errors in personal data</li> </ul>
<i>Low</i>	1	Errors do not affect decision-making processes.	<ul style="list-style-type: none"> <li>• Working documents where errors in the information do not have negative consequences in the decision-making processes of those using the information.</li> </ul>

### 6.3 Accessibility Assessment

<i>Classification</i>	<i>Level</i>	<i>Description</i>
<i>Very High</i>	4	The information value affects the core operations and is critical for the function of the university.
<i>High</i>	3	The information value affects departments, sections, or shared functions, but not the overall functioning of the university.
<i>Moderate</i>	2	The information value affects only certain isolated systems, services, or functions.
<i>Low</i>	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.

### 6.4 Labelling Requirements

- a. Use sensitivity labeling with tags/labels on documents and emails when the information requires a high level of confidentiality (internal, confidential, strictly confidential, and restricted according to the Security Act).
- b. Use appropriate professional systems or tools to process, store, and manage the information securely and efficiently, in line with the system owner's recommendations.

