Policy for Securing Personal ICT Equipment

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	Open
Reference ISO	ISO27002:2022 5.10, 5.11, 7.9, 7.10, 7.14, 8.1
Reference NSM's principles for ICT-security	
Reference Law/Rule	
Reference internal documents	Superior Information Security Policy

1. Purpose

The purpose of the policy is to ensure control of personal ICT equipment used to access, transport, and/or store NTNU's information assets. Personal ICT equipment includes computers, tablets, mobile phones, smartwatches, and portable storage media, but is not limited to these.

2. Scope

The policy applies to both employees and students at NTNU. It also applies to anyone with access to, or those who process and manage information through, NTNU's ICT infrastructure.

3. General Principles

a. All use of personal ICT equipment must always comply with NTNU's ICT regulations.
b. All personal ICT equipment accessing, transporting, processing, and/or storing NTNU's information assets must be access controlled according to the requirements in the Policy for Access Control.
c. Personal ICT equipment must not be used by anyone other than those authorized to use the equipment.
d. Information classified as "Confidential" or "Strictly Confidential" must not be visible to anyone other than those intended to access the information. For example, "Confidential" or "Strictly Confidential" information should not be displayed if unauthorized persons can see the screen or similar.
e. Information classified as "Strictly Confidential" must not be stored on laptops or mobile phones.

f. Personal ICT equipment and data medium containing information classified as “Internal”, “Confidential”, or “Strictly Confidential” must not be left unattended in public places. Equipment containing information classified as “Confidential” must be treated as carry-on baggage when traveling.
g. When traveling abroad, be aware that certain countries may require encrypted equipment to be decrypted for inspection purposes. In such cases, encrypted material must not be taken to countries that may demand access to its content.
h. Information assets covered by export control legislation must not be brought along when traveling to other countries.
i. When traveling to countries defined as “risk countries” by PST (Norwegian Police Security Service), an additional assessment must be made before bringing work-related ICT equipment. The assessment made in accordance with the current travel routine.
j. When disposing of personal ICT equipment, the "Procedure for Disposal of Storage Media" must be followed.
k. When using personal ICT equipment to access NTNU’s information through public or private networks, the communication must be conducted securely, as defined in the "Policy for Network and Information Transfer" and "Policy for Cryptographic Controls."

4. Roles and Responsibilities

4.1. Head of the IT Division

a. Is responsible for implementing the requirements in the Policy for Securing Personal ICT Equipment within the organization.
b. Must be consulted for changes to this policy.

4.2. Head of the HR and HSE Division

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

4.3. Head of Digital Security Section

a. Must be consulted for changes to the policy.

4.4. Line Manager

a. Is responsible for ensuring that employees have sufficient competence to handle personal ICT equipment used to access, transport, and/or store NTNU’s information assets.
b. Must ensure that the department has procedures that ensure the use of personal ICT equipment for processing, handling, and storing information complies with this policy.

4.5. System Owner

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