NTNU

Policy for access control

Type of document	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 5.10, 5.15-5.18, 5.23, 6.5, 6.7, 7.1-7.4, 7.6, 7.8, 8.2, 8.4, 8.5, 8.21
Reference NSMs principles for ICT security	1.3.1, 1.3.2, 2.2.6, 2.3.7, 2.4.1, 2.6.1-2.6.7
Reference Law/Rule	
Reference internal documents	Superior Policy for information security and privacy

1. Purpose

The purpose of this policy is to set premises/conditions for access control to NTNU's information resources to prevent unauthorized access. The policy is independent of the medium of the information and whether it concerns digital or physical access control to locations where information is stored, processed, or transferred.

2. Applies to

The policy for access control applies to those with access and/or permission to one or more information systems owned, developed, operated, or managed by NTNU.

3. General Principles

a. Permission and access to NTNU's digital infrastructure must be based on the need to have an assigned task carried out and are allocated by the principle of "least privilege".
b. NTNU will have permission- and access-control equivalent to the damage unauthorized access can cause.
c. Permission and access to NTNU's digital infrastructure must be trackable.
d. Remote access must be restricted to approved systems.

4. Implementation of Access Control

4.1. Access to Information and Information Systems

a. NTNU must use a central identity database for digital identity. An identity database is a central database that contains/stores digital identities from authoritative sources defined in this document. At NTNU the following systems are authoritative for identity management:

   i. FS (Student system) for identity management of students
   ii. Human Resources and payroll system for identity management of employees
   iii. Separate central database (to be created) for external identities.

b. NTNU must use a central database to allocate a role to an identity. The authoritative system for roles and role-based access is BAS.

c. Guest access to NTNU's ICT infrastructure must be approved by the head of the office or a team leader.

d. NTNU must use a resource domain for access control to the information resources. The access is granted based on the group affiliation of the role in the central database (BAS). NTNU must use one of the following master sources for access control in resource domains:

   i. Microsoft Active Directory (WIN-NTNU-NO)
   ii. LDAP (at.ntnu.no)

e. The owner of the system defines which roles or systems should have access to the information system or the information stored, processed, or transferred via the system.

f. Requirements for logging permission and access must be in accordance with the classification of information within the three areas confidentiality, integrity, and accessibility.

4.2. User Management

Orderly and systematic user management is crucial for implementing secure role-based access control. Errors within user management and identity management will propagate downward in systems for permission control and access control. Therefore, NTNU defines the following principles of how user management should be implied within the organization:

a. NTNU must have personal user accounts for all employees, students, and externals. User accounts are personal and cannot be shared with others.

b. NTNU must have a routine for assigning a person a user account which assures that the person's identity is correct before issuing a user account on NTNU's systems.

c. NTNU can have its own system users for applications and services when this is necessary. These users must be restricted to which systems and services they can access.

d. The privileged access to services, applications, and systems should be granted by the "need-to-use" principle, based on access necessary to accomplish definite functions to a specific role. By privileged access, we hereby mean root/service users on Unix/Linux machines, administrator/service accounts on Windows machines, system accounts in databases, system accounts on network equipment, applications, and communication channels et cetera.

e. Privileged access must be permitted by the direct supervisor through authorization and should be time restricted as much as possible.

f. The maximum time for privileged access is three (3) years, then the person must be re-authorized.

g. Temporary access should be limited to as much as possible in time and space and is given a top limit of one (1) year.

h. Users with privileged access to NTNU's services, applications, and systems must be identified and documented in a central database and connected to either an identity or a process.

i. Privileged access shall be assigned to its own user account, which is dedicated to the purpose or task.

j. Privileged access to systems and applications can be assigned to standard user accounts if the systems or applications access control uses a multi-factor authenticator.

4.3. Users and Authentication

In order to ensure effective access control to NTNU's information resources, the following requirements are placed on those (users) who use and administer these on NTNU's behalf.

a. NTNU imposes requirements on the users to maintain personal passwords or other cryptographic keys, certificates and such, strongly confidential and not share these with others.

b. Authentication information (such as passwords) must be unique for the NTNU services. Reuse of passwords from personal services shall not occur.

c. The user must activate their user account and make a password before services at NTNU can be used.

d. Personal users must make their password via https://bas.ntnu.no.

e. The password should not be written or stored digitally in such a way that it can be connected to an NTNU user account if it gets lost.

f. NTNU requires that users change their password every second year or if:

    i. a suspicion that the user account has been compromised

    ii. an order from the head of the Digital Security Section.

k. Requirements for password length and complexity at NTNU are listed below.

    i. System user: minimum 30 signs with high complexity. With high complexity means lowercase and uppercase letters, numbers, and special sign.

    ii. Domain administrator: Minimum 20 signs with high complexity. With medium complexity means lowercase and uppercase letters, and numbers.

    iii. System administrator: Minimum 20 signs with medium complexity.

    iv. Client administrator: Minimum 20 signs with medium complexity.

    v. Users: Minimum 12 signs with medium complexity.

4.4. Authenticator Mechanism

Authentication mechanisms are programs or routines that define or control users' and/or user groups' access to a machine or specific information. To maintain effective access control at NTNU, mechanisms for authentication of users, systems, and services must be implemented securely to prevent circumvention of authentication and thereby grant access to internal, confidential, or strictly confidential information or misuse of NTNU's information resources. NTNU sets the following requirements for authentication mechanisms:

a. All authentications must always occur over a secure connection (e.g., by using TLS). A secure connection is a connection where both confidentiality and integrity are ensured in the communication.
b. Authentication information must only be validated after all information is received in the system, and during authentication, the system should not provide information about which authentication data is correct or incorrect.
c. Authentication mechanisms must have an internal function that limits the possibility of systematically surmising the authentication data.
d. Information that has a classification level 4[1] must be accessed with a multifactor according to security level 3[2]. Multifactor authentication is when the user must provide multiple separate and independent pieces of evidence for their identity.
e. By default, services, systems, and applications must not display system or application identifying information before successful authentication.
f. Banners that identify the system owner must be added and provide a warning that it is only for authenticated users.
g. The authenticator mechanism must log all successful and unsuccessful authenticator attempts.
h. Authentication mechanisms must log a security event if there is an attempted or successful intrusion.
i. The log must be made into a central log service. This also applies to cloud-based mechanisms.
j. Standard settings for the authenticator mechanism must not show the password in clear text in the password bar.
k. As a standard, the authenticated inactive sessions should always expire after an appropriately defined time. With the exemption of verification codes for one-time passwords or other temporary mechanisms.
l. Authentication mechanisms must save passwords or other authentication data separate from the application.
m. The standard password set by the supplier must always get changed before the equipment is used and connected to NTNU's infrastructure.
n. Temporary passwords or authenticator mechanisms must be uniquely generated each time.

[1] Policy for information classification
[2] https://eid.difi.no/nb/sikkerhet-og-informasjonskapsler/ulike-sikkerhetsniva

o. Temporary passwords or authenticator mechanisms must be conveyed to the user through a secure connection where the receiver can confirm that the message is received.

4.5. Software for System Operations and Administration

The following requirements apply to software used for the administration of services, applications, and systems, such as configuration management tools, user administration, and other system tools:

a. Tools used for system administration must be identified and employ authentication.
b. Tools for system administration must be segregated from other applications.
c. Tools for system administration must be restricted to privileged administration accounts, by the principle for privileged access.
d. All use of system administration tools must be logged in to a central log service.
e. All system administration tools that are not used for the operation of service, application, or system must be deactivated or uninstalled if necessary.
f. System administration tools must not be accessible to users who are not authorized for system administration.

4.6. Network, Systems, and Services at NTNU

Requirements are set for accessing and managing networks, systems, and services that are part of NTNU’s ICT infrastructure. NTNU’s ICT infrastructure includes all equipment, digital information, information systems, and services used for information processing and communication. A cloud service is, in practice, an extension of NTNU’s ICT infrastructure.

a. Two-factor authentication must be used for accessing externally accessible services in NTNU's ICT infrastructure.
b. Networks, systems, and services shall have access control based on the classification, to protect information and information resources against unauthorized access.
c. NTNU may have system-specific procedures for authorizing access to specific networks, systems, and services. These procedures must be based on classification and defined by the system administrator.
d. NTNU must have proper access control to networks, systems, and services based on classification, and risk and vulnerability assessment.
e. Internal systems must only be accessible and reached via a Virtual Private Network (VPN) or similar solutions approved by the Digital Security Section.
f. Applications must be isolated from each other wherever possible.
g. Access to administer systems with security level 3[3] or higher must only be done from dedicated workstations, networks, or servers approved by the head of the Digital Security Section for this purpose.

[3] Different levels of security | eid.difi.no

4.7. Access Control to Source Code

Requirements are set for access control to source code, and parts of the information systems developed by NTNU. This applies to the source code of central components:

a. Based on the classification, source code, and libraries must have access control and be restricted to authorized persons. This applies particularly to:

i. Core systems for dataflow, authentication, and other critical services at NTNU.

ii. Source code that is protected by copyright.

iii. Source code for NTNU that contains plain text authentication data or other sensitive information.

b. Every access-controlled source code must have:

i. Centralized logging of all changes.

ii. Centralized logging of all accesses.

4.8. Physical Security of Areas Providing Access to NTNU’s Information Assets

To ensure information security, the physical security of areas must adhere to the following requirements:

h. Areas containing ICT infrastructure and/or information requiring protection must be divided into zones.

i. The zones must be protected with appropriate access controls to ensure that only authorized personnel are granted access.

j. When evaluating access control and authorization, consideration must be given to the information and equipment present in the respective area according to the applicable procedures.

k. All personnel must be able to disclose their identity when present in NTNU's restricted access areas. As per the table below, this requirement always applies for areas classified as YELLOW, RED, and BLACK, and for areas classified as GREEN when the access control system is activated.

Security level	Security
BLACK Restricted parts of data rooms, data systems, archive rooms, or other areas that provide access to information that is critical for NTNU to protect against unauthorized access or alteration. The BLACK area should be located within the RED area	The black zone must be established within an area defined as the RED zone and equipped with adequate perimeter security. Locked 24 hours/day. Access card + PIN code or key with very limited access. External individuals must only be granted access by special agreement, training in NTNU's information security requirements, signed confidentiality agreement, and under the supervision of an authorized NTNU employee. Everyone must wear visible access cards. There are requirements for door alarm systems, as well as interior motion sensors and video surveillance at the entrance. The room must be properly labelled and have instructions for access if desired.

	An annual review of the risk and vulnerability analysis (ROS analysis) must be conducted to assess security measures for the area. During the review, the following must be revised: • Access during events such as fire, terrorism, etc. • Access revision.
RED Restricted areas that require special authorization, such as data rooms/archives with confidential information, and/or information that is crucial for NTNU to protect against unauthorized access or alterations. The RED zone must be established within a YELLOW zone.	Locked 24 hours/day. Access card + PIN code or key with limited access. External individuals must only be granted access upon special agreement and training in NTNU's information security requirements. A confidentiality agreement must be signed. All individuals must visibly display their access card. An alarm system for the door is required. The room must be adequately labelled. An annual risk and vulnerability assessment (ROS analysis) must be conducted to identify security measures for the area. During the review, the following must be revised: • Access during events such as fire, terrorism, etc. • Access revision.
YELLOW Areas where information classified as internally can be accessed. Offices, meeting rooms, print rooms etc. Where there is access control 24/7.	Lock and personal access card + PIN code. External individuals must only be granted access after a specific agreement and signing a confidentiality statement. For print rooms located in the green zone, the print room may be classified as a yellow zone when printing confidential information. In such cases, secure printing functionality is required for the printer/printing system.
GREEN Publicly accessible areas: lounges, foyers, corridors, cafeteria, etc. In principle, every area that is "open areas".	Perimeter security for buildings outside of opening hours and any additional security measures deemed necessary, such as video surveillance, etc. Security measures are based on a risk assessment (ROS analysis) and assets located within the premises

5. Roles and Responsibility

5.1. Director of Organization and Infrastructure

a. Consultation is required for changes to the access control policy.

5.2. Head of Division for Governance and Management Systems

a. Is responsible for ensuring that the work on access control is subject to internal/external auditing to ensure that the desired effect is achieved with the proper use of resources (efficiency).

5.3. Head of IT Division

a. Must be consulted in case of changes to the access control policy.

b. Is responsible for ensuring that the principles and requirements defined in the access control policy are followed in the IT Division.

5.4. Head of HR and HSE Division

a. Must be consulted in case of changes to the access control policy.

b. Is responsible for ensuring that line managers are aware of and have sufficient competence to fulfil their responsibilities according to the access control policy.

c. Must ensure good procedures for the management of roles and identities, and that these are incorporated into relevant processes.

5.5. Head of Digital Security Section

a. Is responsible for ensuring that the access control policy complies with the necessary requirements to secure access to NTNU's ICT infrastructure.

b. Is responsible for temporarily overriding assigned access rights in situations where it is necessary to safeguard the security of NTNU's ICT infrastructure.

c. Is responsible for reporting on the effectiveness and efficiency of measures implemented to protect against unauthorized access, attacks, and/or threats to NTNU's ICT infrastructure.

5.6. Line Manager

a. Must ensure correct registration and management of roles and identities within their area of responsibility.

b. Must ensure corrections and removal of access in accordance with the principles and requirements set forth in this access control policy within their area of responsibility.

c. Must ensure that access to sensitive information is managed in accordance with the principles and requirements set forth in this access control policy within their area of responsibility.

5.7. System Owner

a. Must be consulted for changes to the access control policy.

b. Is responsible for ensuring that the principles and requirements defined in the access control policy are followed and implemented on systems for which they are responsible.

c. Is responsible for defining the roles that should have access to the system they own.