# Policy for Cryptographic Controls

| | |
|---|---|
| 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 | Open |
| Reference ISO | ISO 27002:2022; 811, 8.24 |
| Reference NSMs principles for ICT-security | NSM Cryptographic Recommendations<br>NSM's General Principles for Information Security: 2.2.1,2.4.2,2.7.1-2.7.4 |
| Reference Law/Rule | eGovernment regulations (eForvaltningsforskriften) |
| Reference internal documents | ICT Regulation and superior Policy for Information Security |

## 1. Purpose

The purpose of this policy is to assure that cryptographic keys are correctly procured, administrated, distributed, and dissolved.

## 2. Applies to

Policy for Cryptographic Controls applies to all employees at NTNU, and students who process classified information.

## 3. General Principles

a. The strength of the crypto must reflect the classification of the information and the system.
b. Administrated devices must have encrypted hard disks.
c. All wired and wireless connections must be encrypted.
d. Encryption must be used when information classifies as higher than internally transmitted or when the reliance on the information channel is low.

## 4. Digital Certificate

Digital certificates are unique data files that can be used as digital credentials. They can be issued to websites, programs, organizations (business certificates), and individuals (personal certificates) and are intended to ensure the integrity of digital communication.

### 4.1. SSL Certificates

a. All services under the domains ntnu.no and ntnu.edu must use TLS certificates issued by NTNU IT.

### 4.2. Business Certificates

a. Business certificates are used for:

   i. Signing – a business certificate is NTNU's legal and digital signature and can be used wherever the rector or chief financial officer would need to sign.
   ii. Authenticating – logging into Altinn and other public services.
   iii. Encrypting – securing communication.

b. Business certificates are managed by the Digital Security Section and operated by the IT Infrastructure Section.
c. NTNU should differentiate between research and administration when using business certificates.
d. The need for a business certificate should be approved by the Digital Security Section.
e. The Digital Security Section can revoke a business certificate in case of misuse.

### 4.3. Personal Certificates

Personal certificates can be used to sign documents (digital signature) and verify the sender in emails.

a. All managers at NTNU should have a personal certificate to sign emails.
b. Anyone working with security and emergency preparedness at NTNU must have a personal certificate.
c. Personal certificates must not be used for purposes other than official duties, as specified in §19 eForvaltningsforskriften.

## 5. Encryption

a. Managed clients must have encrypted hard drives to store Confidential information.
b. The key to the encrypted hard drive for processing Confidential information must use AES or an equivalent algorithm with a minimum length of 256 bits.
c. Storage media that will store Highly Confidential information must be encrypted using AES or an equivalent algorithm with a minimum length of 256 bits.
d. The key must be stored securely.
e. Password requirements for file encryption:
   i. Confidential information: Minimum 20 characters with high complexity, including uppercase and lowercase letters, numbers, and special characters.
   ii. Highly Confidential information: Minimum 30 characters with high complexity.

### 5.1. Cryptographic Deletion

During cryptographic deletion, the key to the encrypted device is erased to make it extremely difficult to recover the data.

a. Cryptographic deletion must be performed in a controlled manner to verify that the key cannot be recovered.

## 6. Roles and Responsibilities

### 6.1. Head of IT Division

### 6.2. Head of Digital Security Section

a. Responsible for acquiring the enterprise certificate.
b. Responsible for processing requests for access to the enterprise certificate.
c. Responsible for contract negotiation during the distribution of the enterprise certificate.
d. Responsible for terminating the enterprise certificate.

### 6.3. Head of IT Infrastructure Section

a. Responsible for distributing the enterprise certificate.
b. Responsible for securely storing the enterprise certificate in a safe location.