

Retningslinje for Kryptografiske kontroller

Type dokument	Retningslinje
Forvaltes av	CISO, Seksjon for Digital sikkerhet
Godkjent av	Direktør for Organisasjon og infrastruktur
Gjelder fra	01.10.2025
Neste revisjon innen	01.10.2027
Unntatt offentlighet	Nei
Referanse ISO	ISO 27002:2022; 8.11, 8.24
Referanse NSMs veiledninger	NSM Cryptographic Recommendations NSMs Grunnprinsipper for informasjonssikkerhet: 2.2.1,2.4.2,2.7.1-2.7.4
Referanse Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning	Pkt 10
Referanse LOV/Regel	eForvaltningsforskriften
Referanse interne dokumenter	IKT-reglementet og Politikk for informasjonssikkerhet, Styringsdokument for sikkerhet og beredskap

1. Formål

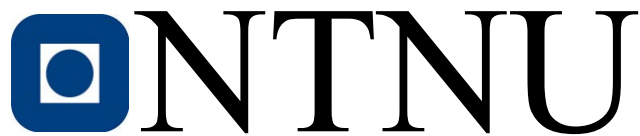
Formålet med «Retningslinje for kryptografiske kontroller» er å sikre at NTNU bruker kryptografiske metoder for å beskytte data og informasjon under overføring og lagring, i tråd med beste praksis og myndighetskrav.

2. Gjelder for

«Retningslinje for kryptografiske kontroller» gjelder for alle ansatte ved NTNU, samt studenter som behandler skjermingsverdig eller gradert informasjon iht. retningslinje for informasjonsklassifisering.

3. Ansvar og roller

Arbeidet med informasjonssikkerhet berører virksomheten på alle nivå. Ansvar og myndighet for informasjonssikkerhet følger det ordinære linjeansvaret. Alle roller tilhørende styringssystemet er definert i politikk for informasjonssikkerhet.



Leder av IT-avdelingen, leder av Seksjon for IT Infrastruktur og leder for Seksjon for digital sikkerhet har sentrale roller i oppfølging av retningslinje for kryptografiske kontrollere.

4. Overordnede prinsipper

- a. NTNU skal følge «NSM Cryptographic recommendation»[<https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/kryptografiske-anbefalinger-en-veileder-fra-nsm>]
- b. NTNU skal alltid bruke den sterkeste tilgjengelige kryptografiske mekanismen der det er hensiktsmessig. Hvis mulig, bør kvantesikre algoritmer benyttes når informasjon sendes over internett
- c. NTNU skal kryptere lokal lagring for alt sluttbrukerutstyr (arbeidsstasjon, laptop, nettbrett og mobiltelefon) for å forhindre informasjon på avveie ved tap av utstyr
- d. Behov for kryptering for utstyr på laboratorier skal vurderes basert på krav til konfidensialitet, integritet og hensiktsmessighet
- e. Alle kablede og trådløse forbindelser skal krypteres

5. Digitale sertifikater

Digitale sertifikater er unike datafiler som kan brukes som digital legitimasjon. Det kan utstedes til nettsted, program, organisasjon (virksomhets sertifikat) og person (personsertifikat) og skal sikre integriteten ved digital kommunikasjon.

5.1. TLS-sertifikater

- a. Alle domener eid av NTNU skal benytte TLS-sertifikater utgitt av en autorisert og godkjent CA
- b. NTNU skal ha en DNS CAA oppføring for å begrense utstedning av sertifikater til godkjente og autoriserte «Certificate Authorities».
- c. Domener eid av NTNU skal kun støtte tilkoblinger på TLS 1.2 eller nyere.
- d. Domener eid av NTNU skal valideres med OV(Organization Validation)-sertifikat.

5.2. Virksomhets sertifikat

- a. Virksomhets sertifikater brukes til å:
 - i. Signere – virksomhets sertifikat er NTNUs juridiske og digitale signatur og kan brukes overalt hvor rektor eller økonomidirektør måtte ha signert.
 - ii. Autentisere – innlogging i Altinn og andre offentlige tjenester.
 - iii. Kryptere - sikre kommunikasjon.
- b. Virksomhets sertifikatene forvaltes av Seksjon for Digital sikkerhet og driftes av Seksjon for IT-infrastruktur.
- c. NTNU skal skille på forskning og forvaltning ved bruk av virksomhets sertifikat.
- d. Behov for virksomhets sertifikat skal godkjennes av Seksjon for Digital sikkerhet.
- e. Seksjon for Digital sikkerhet kan trekke tilbake virksomhets sertifikat ved misbruk.

5.3. Personlige sertifikater

Personlige sertifikater kan brukes for å signere dokumenter (digital signatur) og epost for å verifisere avsender.



- a. Alle ledere ved NTNU bør ha et personlig sertifikat for å signere epost.
- b. Alle som jobber med sikkerhet og beredskap innenfor NTNU skal ha personlig sertifikat.
- c. Personlig sertifikat skal ikke brukes til andre formål enn tjenesteformål jf. §19 eForvaltningsforskriften.

6. Kryptering

- a. Kryptert harddisk skal benytte AES-XTR med 128 (FORTROLIG) eller 256 bits (STRENGT FORTROLIG/BEGRENSET). Lagring av BEGRENSET krever egen autorisasjon og godkjenning utover kryptert harddisk.
- b. For generell kryptering skal AES-GCM benyttes opptil FORTROLIG, og AES-GCM 256 benyttes ved STRENGT FORTROLIG/BEGRENSET.
- c. Nøkkelen skal oppbevares forsvarlig.
- d. Krav til passord ved kryptering av filer:
 - i. Fortrolig informasjon: Minimum 20 tegn med høy kompleksitet, dvs store og små bokstaver, tall og spesialtegn.
 - ii. Strengt Fortrolig informasjon: Minimum 30 tegn med høy kompleksitet

Gradering	Generell kryptering	Kryptering av lagringsmedier/harddisk
BEGRENSET*	AES-GCM (AES-256)	XTS-AES (AES-256)
STRENGT FORTROLIG		
FORTROLIG	AES-GCM (AES-128)	XTS-AES (AES-128)
INTERN	AES-GCM (AES-128) eller sterkeste hensiktsmessig	XTS-AES (AES-128) eller sterkeste hensiktsmessig
ÅPEN	Ingen krav, men anbefalt sterkeste hensiktsmessig	Ingen krav, men anbefalt sterkeste hensiktsmessig

*BEGRENSET krever autorisasjon og godkjenning av systemer uavhengig av kryptering.

6.1. Kryptografisk sletting

Ved kryptografisk sletting slettes nøkkelen til den krypterte enheten slik at det er svært vanskelig å gjenopprette dataene igjen.

- a. Kryptografisk sletting skal gjøres på en kontrollert måte for å kunne verifisere at nøkkel ikke kan gjenopprettes.