Retningslinje for Kryptografiske kontroller

Type dokument	Retningslinje
Forvaltes av	Leder av IT-avdelingen
Godkjent av	Direktør for Organisasjon og infrastruktur
Gjelder fra	12.06.2023
Neste revisjon innen	12.06.2025
Unntatt offentlighet	Nei
Referanse ISO	ISO 27002:2022; 811, 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 LOV/Regel	eForvaltningsforskriften
Referanse interne dokumenter	IKT-reglementet og Politikk for informasjonssikkerhet

1. Formål

Formålet med «Retningslinje for kryptografiske kontroller» er å sørge for at kryptografiske nøkler anskaffes, administreres, distribueres og avvikles på en korrekt måte.

2. Gjelder for

«Retningslinje for kryptografiske kontroller» gjelder for alle ansatte ved NTNU, samt studenter som behandler gradert informasjon.

3. Overordnede prinsipper

a. Styrken til krypto skal gjenspeile klassifiseringen til informasjonen og systemet.
b. Administrerte enheter skal ha kryptert harddisk.
c. Alle kablede og trådløse forbindelser bør krypteres.
d. Kryptering skal benyttes når informasjon klassifisert høyere enn Intern overføres, eller når tilliten til informasjonskanalen er lav.

4. Digitale sertifikater

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

4.1. SSL-sertifikater

a. Alle tjenester under domene ntnu.no og ntnu.edu skal benytte TLS-sertifikater utgitt av NTNU IT

4.2. Virksomhetssertifikat

a. Virksomhetssertifikater brukes til å:
    i. Signere – virksomhetssertifikat 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. Virksomhetssertifikatene forvaltes av Seksjon for Digital sikkerhet og driftes av Seksjon for IT drift.
c. NTNU skal skille på forskning og administrasjon ved bruk av virksomhetssertifikat.
d. Behov for virksomhetssertifikat skal godkjennes av seksjon for Digital sikkerhet.
e. Seksjon for Digital sikkerhet kan trekke tilbake virksomhetssertifikat ved misbruk.

4.3. 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.

5. Kryptering

a. Administrerte klienter skal ha kryptert harddisk for å kunne lagre Fortrolig informasjon.
b. Nøkkel til kryptert harddisk for behandling av Fortrolig informasjon skal ha AES eller tilsvarende algoritme med minimum 256 bits lengde.
c. Lagringsmedier som skal oppbevare Strengt Fortrolig skal krypteres med AES eller tilsvarende algoritme med minimum 256 bits lengde.
d. Nøkkelen skal oppbevares forsvarlig.
e. 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

5.1. 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.

6. Roller og ansvar

6.1. Leder av IT-avdelingen

6.2. Leder av Seksjon for Digital sikkerhet

a. er ansvarlig for å anskaffe virksomhetssertifikat
b. er ansvarlig for å behandle søknader om tilgang til virksomhetssertifikat
c. er ansvarlig for kontraktinngåelse ved distribusjon av virksomhetssertifikat
d. er ansvarlig for å avvikle virksomhetssertifikat

6.3. Leder av Seksjon for IT-drift

a. er ansvarlig for å distribuere virksomhetssertifikat
b. er ansvarlig for at virksomhetssertifikat oppbevares på et trygt område