Mittuniversitetet
MID SWEDEN UNIVERSITY

# Riktlinjer för kryptering

**Publicerad:** 2020-11-04

**Beslutsfattare:** Helena Wallskog

**Handläggare:** Eva Rodin Svantesson

**Beslutsdatum:** 2020-11-04

**Giltighetstid:** Tillsvidare

**Ansvarig för förvaltning:** Riktlinjerna förvaltas av infrastrukturavdelningen.

**Målgrupp:** Infrastrukturavdelningen (INFRA)

**Sammanfattning:** Riktlinjerna sammanfattar hur kryptering ska användas inom universitetet. Riktlinjerna har anpassats utifrån Myndigheten för samhällsskydd och beredskaps föreskrifter MSBFS 2020:6-7.

# Innehållsförteckning

# 1. Riktlinjer för kryptering

Universitetet ska identifiera och hantera behovet av kryptering för att skydda information mot obehörig åtkomst och obehörig förändring vid överföring och lagring. Vid införande av principer för kryptering bör hänsyn tas till regelverk, nationella restriktioner som kan tillämpas på användningen av krypteringsteknik i olika delar av världen och frågor avseende gränsöverskridande flöde av krypterad information.

Säkerhetsåtgärder baserade på kryptering kan användas för att uppnå olika informationssäkerhetsmål t. ex:

a) konfidentialitet: användning av kryptering av information för att skydda känslig eller kritisk information som antingen lagras eller överförs;
b) riktighet/äkthet: användning av digitala signaturer eller "autentiseringskoder för meddelanden" för att verifiera äktheten eller riktigheten hos lagrad eller vidarebefordra känslig eller kritisk information;
c) oavvislighet: användning av kryptografiska tekniker för att ge belägg eller förekomst eller avsaknad av en händelse eller handling;
d) autentisering: användning av kryptografiska tekniker för att autentisera användare och andra systemenheter som begär åtkomst till eller verksamhetsförbindelser med systemets användare, enheter och resurser.

## 1.1 Regler för användning av kryptografiska säkerhetsåtgärder

Syfte: att säkerställa korrekt och verkningsfull användning av kryptering för att skydda informationens konfidentialitet och riktighet.

Kryptering ska användas vid Mittuniversitetet;

a) som säkerhetsåtgärd för att skydda information
b) för att skydda säkerhetsloggar mot obehörig åtkomst och obehörig förändring,
c) som autentiseringsuppgifter mot obehörig åtkomst och obehörig förändring, och
d) för information i behov av utökat skydd mot obehörig åtkomst och obehörig förändring vid överföring till myndighetens informationsssystem

## 1.2 Nyckelhantering

Syfte: för kryptografiska nycklars hela livscykel ska regler för användning, skydd och giltighetstid utvecklas och införas.

Mittuniversitetet ska ha interna regler för kryptering med krav på;

a) hantering av krypteringsnycklar, godkännande och förvaltning av krypteringslösningar, och hur krypteringsalgoritmer, krypteringsprotokoll och nyckellängder ska väljas.

## 1.3 DNSSEC

Mittuniversitetet ska använda Domain Name System Security Extensions (DNSSEC) avseende samtliga domännamn som myndigheten registrerat i domännamnssystemet (DNS).