Retningslinje for Sikring av personlig IKT-utstyr

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
Klassifisering	Åpen
Referanse ISO	ISO27002:2022 5.10, 5.11, 7.9, 7.10, 7.14, 8.1
Referanse LOV/Regel	
Referanse interne dokumenter	Denne retningslinjen er underlagt Politikk for informasjonssikkerhet ved NTNU

1. Formål

Formålet med retningslinjen er å sikre kontroll av personlig IKT-utstyr som benyttes til å aksessere, transportere og/eller lagre informasjonsverdiene ved NTNU. Personlig IKT-utstyr omfatter, men er ikke begrenset til, datamaskiner, nettbrett, mobiltelefoner, smartklokker, samt bærbare lagringsmedium.

2. Gjelder for

"Retningslinje for sikring av personlig IKT-utstyr gjelder for alle ansatte og studenter ved NTNU, samt alle som har tilgang til, eller bearbeider og forvalter informasjon gjennom NTNUs IKT-infrastruktur.

3. Overordnede prinsipper

a. All bruk av personlig IKT-utstyr skal til enhver tid følge reglene i NTNUs IKT- reglement.
b. Alt personlig IKT-utstyr som aksesserer, transporterer, behandler og/eller lagrer NTNUs informasjonsverdier skal tilgangsstyres i henhold til krav i «Retningslinje for tilgangskontroll».
c. Personlig IKT-utstyr skal ikke brukes av andre enn de som er autorisert for å bruke utstyret.
d. Informasjon som er klassifisert som Fortrolig eller Strengt Fortrolig skal ikke kunne sees av andre enn de som informasjonen er ment for. Dette betyr eksempelvis at en ikke skal vise Fortrolig eller Strengt Fortrolig informasjon om uvedkommende kan se skjermbildet eller lignende.
e. Informasjon klassifisert som Strengt Fortrolig skal ikke lagres på bærbare maskiner, eller mobiltelefoner..
f. Personlig IKT-utstyr og datamedier som inneholder informasjon klassifisert som Intern, Fortrolig eller Strengt fortrolig skal ikke være ubevoktet på offentlige steder. Ved reiser skal utstyr som inneholder informasjon klassifisert som fortrolig håndteres som håndbagasje.

g. Ved reiser utenlands må en være oppmerksom på at enkelte land vil kunne kreve at utstyr som er kryptert skal dekrypteres for å kunne utføre kontroll. I slike tilfeller skal ikke kryptert materiale tas med til land som kan kreve å kunne kontrollere innhold.
h. Ved reise til andre land skal informasjonsverdier omfattet av eksportkontrolloven ikke medbringes.
i. Ved reise til land definert som risikoland av PST, skal det gjøres en ekstra vurdering før IKT-utstyr brukt i jobbsammenheng medbringes. Vurderingen gjøres i henhold til gjeldende reiserutine.
j. Ved avhending av personlig IKT-utstyr skal «Rutine for avhending av lagringsmedium» følges.
k. Når personlig IKT-utstyr benyttes for å få tilgang til NTNUs informasjon gjennom offentlige eller private datanett skal kommunikasjonen skje på en sikker måte, definert i «Retningslinje for nettverk og informasjonsoverføring» og «Retningslinje for bruk av kryptografiske kontroller».

4. Roller og ansvar

4.1 Leder av IT-avdelingen

a. er ansvarlig for at kravene i «Retningslinje for sikring av personlig IKT-utstyr» blir implementert i virksomheten
b. skal konsulteres ved endringer i retningslinjen

4.2 Leder av HR- og HMS-avdelingen

a. er ansvarlig for at ledere er kjent med, og har tilstrekkelig kompetanse, til å ivareta sitt ansvar i henhold til denne retningslinjen

4.3 Leder av Seksjon for digital sikkerhet

a. skal konsulteres ved endringer i retningslinjen

4.4 Linjeleder

a. er ansvarlig for at medarbeidere har tilstrekkelig kompetanse til å behandle personlig IKT-utstyr som benyttes til å aksessere, transportere og/eller lagre informasjonsverdiene ved NTNU
b. skal påse at avdelingen har rutiner som sikrer at bruk av personlig IKT-utstyr som blir brukt til å behandle, bearbeide og lagre informasjon er i henhold til denne rutinen

4.5 Systemeier

a. skal angi hvilke klassifiseringer av informasjon IKT-systemet er godkjent for å benytte, transportere og/eller lagre