UiT
NORGES
ARKTISKE
UNIVERSITET

RETNINGSLINJE
for bruk av UiTs IT-utstyr og -tjenester ved reiser til risikoland

Fastsatt av:	Universitetsdirektør	Dato:	25.4.2018
Ansvarlig enhet:	Avdeling for IT	Id:	
Sist endret av:	Administrasjonsdirektør	Dato:	29.6.2023
Erstatter:		Arkivref.:	2023/472

Formål
Disse retningslinjene skal bidra til at informasjonssikkerheten ivaretas ved kortere reiser til land som Norge ikke har sikkerhetssamarbeid med og som representerer en forhøyet risiko for at delegater fra UiT kan bli utsatt for statlig etterretningsvirksomhet.

Retningslinjene skal motvirke en trusselaktørs evne og muligheter til å tilegne seg eller manipulere UiTs informasjon gjennom f.eks å stjele, aksessere, plante, modifisere eller slette data, som f.eks forskningsdata, viktige dokumenter, forhandlingsposisjoner, utredninger mv. De skal videre senke risikoen for at fremmede aktører får plantet uønsket innhold på UiT-eid, elektronisk utstyr, være seg programvare[1] eller maskinvare[2].

Virkeområde
Retningslinjen gjelder for alle ansatte, og omfatter reiser hvor UiT-eid utstyr og/eller informasjon (enten fysisk eller digitalt) medbringes til land som Norge ikke har sikkerhetssamarbeid med og som representerer en forhøyet risiko for UiTs informasjonssikkerhet.

Også land Norge har sikkerhetssamarbeid med, men hvor landets praksis rundt grensepasseringer medfører en forhøyet risiko for at fortrolig informasjon kommer på avveie, omfattes i den grad retningslinjen passer.

[1] Eksempelvis keyloggers eller programvare for å foreta opptak av lyd/bilde, sende ut kopier av filer etc.
[2] Dvs fysiske inngrep i maskinen, med tanke på å få tilgang til informasjon uten at det kan oppdages med enkle midler, eller motvirkes via reinstallering etc.

Ansvar, myndighet og oppgavefordeling

- *Administrasjonsdirektør* har myndighet til å endre gjennomførende del av ledelsessystemet for sikkerhet, beredskap og personvern, og fastsetter disse retningslinjene.
- *IT-direktør* delegeres ansvar og myndighet for revidering av disse retningslinjene, samt fastsettelse av tilhørende rutiner.
- Med *enhetsleder* menes enhetens øverste leder. Dersom reisen involverer enhetsleder selv legges eventuelle beslutninger til dennes nærmeste leder.
- *Avdeling for IT* v/digital arbeidshverdag har ansvaret for å koordinere iverksettelsen av retningslinjen med tilhørende rutiner, herunder presentere disse på nettsidene https://uit.no/sikkerhet og i serviceportalen.

Definisjoner

Med *risikoland* menes land hvor det er særlig risiko for aktivitet fra statlige etterretningsmyndigheter rettet mot UiT. Ifølge PSTs åpne trusselvurdering er det særlig Russland, Kina og Iran som utpeker seg med aktivitet mot norske interesser, og reiser til disse landene vil være omfattet av disse retningslinjene.

Med *privatreiser* menes reiser som ikke gjennomføres som del av rollen din som UiT-ansatt.

Krav og anbefalinger

For reiser som omfattes av denne retningslinjen plikter den aktuelle ansatte å orientere seg om og overholde følgende rutiner

For privatreiser:

- Det er *ikke* tillatt å ta med UiT-utstyr eller koble seg opp på UiT-tjenester på privatreiser, eksempelvis for å sjekke e-post på privatmobil e.l. Unntak fra dette kan gis dersom særlige grunner foreligger og det er i UiTs interesse at det gis.
    - Beslutning om unntak tas av enhetsleder i samråd med *Faggruppe for informasjonssikkerhet og personvern*
    - Dersom unntak innvilges skal den ansatte få låneutstyr fra UiT, og retningslinjene her gjelder fullt ut.

For jobbreiser:

1. Man skal ikke ta med den bærbare PC man har fått utstedt av UiT til daglig bruk, men bruke en lånePC spesifikt for dette formålet. Disse utstedes ved å ta kontakt med IT-brukerstøtte før avreise, og må leveres igjen ved hjemkomst.
2. Det anbefales ikke å ta med privat mobiltelefon, og UiT kan låne ut mobiltelefoner til bruk på reisen.
3. Det må så tidlig som mulig meldes fra til IT-brukerstøtte om at man har behov for låneutstyr, og senest en måned før avreise.
4. Det er ikke tillatt å koble seg til UiTs tjenester via privat utstyr (f.eks datamaskin, mobiltelefon, nettbrett) på noe tidspunkt under reisen og oppholdet.

5. Multifaktor/tofaktor til pålogging til UiTs tjenester skal skje ved hjelp av app på mobiltelefonen eller «sikkerhetsnøkkel». Sistnevnte utleveres av Avdeling for IT. SMS skal aldri benyttes, og skal deaktiveres som mulighet for brukerkontoen.
6. Kun arbeidsdokumenter/informasjon som er nødvendig i løpet av reisen skal medbringes, dette gjelder uavhengig av om informasjonen er lagret digitalt eller fysisk
7. Elektroniske gaver som man mottar i løpet av reisen, skal ikke brukes verken under eller etter reisen[3]. Dette kan være minnepinner, nødladere mv. Tilsvarende gjelder for elektroniske enheter som man finner underveis[4]
8. Bruk av offentlige/hotellets ladestasjoner til mobiltelefoner mv. bør unngås. Hvis disse ***må*** brukes skal enheten være låst eller slått av.
9. Bruker skal ikke være pålogget UiTs tjenester ved grensepasseringer (f.eks Microsoft 365), dette inkluderer tjenester som synkroniserer filer til datamaskin og/eller mobiltelefon.
10. Fortrolig eller strengt fortrolig[5] informasjon skal ikke medbringes[6] ved grensepasseringer. Slik info skal hentes ned fra UiTs skytjenester når man er fremme[7].
11. Utstyr (datamaskin, mobiltelefon, ladekabler) skal være under oppsyn til enhver tid. Hotellsafer er *ikke* sikker oppbevaring.
12. Ved bruk av internett på hotell, konferanselokaler, flyplass, universiteter mv, skal man alltid koble til UiTs VPN-klient *før* man kobler seg til de aktuelle UiT-tjenestene (som Sharepoint, e-post mv). Adressen man da skal benytte i UiTs VPN-klient er vpn.uit.no/alltrafikk. Dersom reisen er til land som sperrer VPN-tilkoblingen må den ansatte ta opp den problemstillingen med Avdeling for IT slik at aktuelle løsninger kan vurderes.
13. Innsynsfilter[8] på datamaskin (enten innebygget eller eksternt) skal benyttes når andre er tilstede.
14. UiTs mekanismer for informasjonsbeskyttelse[9] skal benyttes så langt det er mulig.
15. Medbrakte lagringsmedier som eksterne harddisker og/eller minnepinner skal være krypterte, men se også punktet nedenfor.
16. Den ansatte er selv ansvarlig for å sette seg inn i det aktuelle reisemåls lover, regler og normer, og ikke medbringe utstyr og/eller informasjon som det er forbudt å innføre. Eksempelvis kan det i enkelte land være forbudt å medbringe krypterte filer og/eller krypteringsprogramvare, og overtredelse kan i ytterste konsekvens være straffbart. I slike tilfeller må man ta kontakt med *Faggruppe for informasjonssikkerhet og personvern* i god tid før avreise, for å få avklart hvordan informasjonen kan sikres. Faggruppa kan ikke gi oversikt eller råd om forståelse av lokale lover og regler i landet man skal reise til, se også punkt nedenfor om generelle reiseråd.
17. Når man kommer tilbake fra en slik reise, skal passord på UiT-konto byttes. Dette gjøres på nettsiden https://passord.uit.no.
18. Hendelser og mistanke om sikkerhetsavvik skal meldes raskt til *Faggruppe for informasjonssikkerhet og personvern* (se uit.no/sikkerhet).

---

[3] Disse skal avhendes, enten av den ansatte selv eller via UiTs ordning for destruksjon av IT-utstyr.

[4] F.eks på gaten, på hotellet etc.

[5] Se retningslinje for klassifisering av informasjon

[6] Dvs være lagret lokalt på datamaskin eller mobiltelefon, inkludert synkronisert ned fra en skytjeneste.

[7] Merk: Ikke bruk private skytjenester (som Dropbox, Google Drive etc) eller e-post (selv UiTs e-post) til denne typen dokumenter.

[8] Et innsynsfilter gjør at det blir vanskeligere å se på skjermen fra siden av, og bidrar derfor til å hindre at andre personer kan lese hva som står på skjermen. Merk at det ikke forhindrer alt av innsyn, f.eks kan de som sitter på rader bak deg på et fly eller i et auditorium lese hva som står på skjermen.

[9] Her menes klassifiseringen av dokumenter og filer som kan gjøres gjennom Microsoft 365.

Ansatte bes være oppmerksom på følgende:

- vurder hvilke elektroniske hjelpemidler det er nødvendig å ta med, f.eks mobiltelefon, nettbrett, PC m.m. (dette gjelder også privat utstyr, ikke bare UiT-eid)
- vær oppmerksom på at enkelte land har grensekontroller med utvidet sjekk av dokumenter og bagasje, herunder beslag av digitalt utstyr. Planting av ondsinnet programvare og/eller avlyttingsutstyr kan forekomme.
- Hotellsafen kan ikke regnes som trygg
- Enkelte land har iverksatt tekniske sperrer for bruk av VPN-klienter. Dette kan medføre at man ikke får tilgang til de filene/tjenestene ved UiT som man behøver.
- Denne retningslinjen erstatter ikke behovet for å sette seg inn i Utenriksdepartementets reiseråd, og hvilke lover, regler og normer som gjelder i det aktuelle landet.

Virketid

Denne retningslinjen tar sikte på å følge PSTs årlige trusselvurdering som utkommer i januar/februar, og vil derfor bli revidert årlig dersom nye trusselvurderingene har relevante endringer.

Dette er imidlertid et område hvor forutsetningene for de vurderinger som er gjort kan endre seg raskt. Det kan derfor i visse tilfeller være aktuelt med endringer på kort varsel. Sjekk derfor alltid nettsiden https://uit.no/sikkerhet for å være sikker på at du har den gjeldende versjonen.

Referanser

- Denne retningslinjen er underlagt *Ledelsessystemet sikkerhet, beredskap og personvern ved UiT*, kapittel 11.
- Retningslinjen er basert på interne risikovurderinger og
    - PSTs sikkerhetsråd for delegasjoner og medreisende på reiser til utlandet[10]
    - PSTs Nasjonale trusselvurdering 2023[11]
    - NSMs tiltak for IKT-sikkerhet på reise[12]

Versjonslogg

Versjonsnummer	Dato	Kommentar
1	25.4.2018	
2	<vedtaksdato>	Viktigste endring er at alle ansatte omfattes, og retningslinjen gjelder alt av UiTs IT-utstyr og -tjenester. Noen nye tiltak er innført, og krav til oppsett av utstyr (håndteres av ITA) er skilt ut i egen rutine.

[10] Linken sist hentet 28.6.2023.
[11] Linken sist hentet 28.6.2023.
[12] Linken sist hentet 28.6.2023.