

## Før reise

- Se reiseinformasjon fra Utenriksdepartementet (UD). Avklar sikkerhetssituasjon til destinasjonslandet og følg UDs reiseråd.
- Meld «forflytning av arbeidssted for ansatte» på Innsida, når du skal utføre arbeid et annet sted i mer enn tre dager.
- Reisende er ansvarlig for egen reiseforsikring som ikke dekkes av statens reiseregulativ.
- Registrer kontaktopplysninger om din reise hos UD: [reiseregistrering.no](https://reiseregistrering.no).
- Lagre telefonnummer til nødetater til det landet du skal til.
- Tenk igjennom behovet for å ta med informasjon (fysisk og digital) ut av Norge og minimer mengden. Lokale myndigheter kan forlange å få tilgang til kryptert informasjon.
- Unngå å legge i fra deg informasjonsheter (mobiltelefon, nettbrett og PC) på steder hvor du ikke har direkte oppsyn med dem.
- Vær oppmerksom på at eksportkontrollregelverket kommer til anvendelse ved forskningssamarbeid, deling av informasjon og forskningsresultater med utenlandske institusjoner. Dette gjelder også ved annen tilgjengeliggjøring av slik informasjon og ved deltakelse eller gjennomføring av kurs og konferanser.

## Under reise

- Gjør deg kjent med nødutganger på ulike transportmidler og ditt hotell/oppholdssted.
- Lagre adressen på ditt hotell/oppholdssted slik at du kan komme deg dit/eller har behov for hjelp.
- Vurder sikkerheten i områder du beveger deg i. Ikke gå alene gjennom områder med høy kriminalitet.
- Blir du utsatt for ran – ikke gjør motstand. Materielle verdier kan erstattes.
- Skulle du komme i en ulykke, følg instruksene fra nødetatene på stedet. Dersom du selv/reisefølget er involvert må du varsle instituttet ved nærmeste leder.
- Skru av WiFi og Bluetooth når dette ikke benyttes.
- Bruk et sikkert nett. Hvem som helst kan sette opp trådløse nettverk og kalle det opp etter en flyplass eller et hotell. Å åpne fremmede nettverk innebærer derfor risiko. Bruk ditt eget mobilnett om mulig.
- Hvis du blir tilbudt å benytte en USB-lagringsenhet slik som f.eks. en minnepinne fra noen, sier du nei. Unngå også å låne bort dine egne minnepinner eller andre USB-enheter med minne. Dette gjelder også pekeenheter og mus.
- Benytter du internett, skal du koble opp med [NTNUs VPN](#).
- Bruk egen lader for mobiltelefon.
- Tenk over hvem du deler kunnskapsinformasjon med. Ikke gi bort sensitiv informasjon.

Mistenker du at informasjon har kommet på avveie eller ved andre IT-sikkerhetshendelser, ta kontakt med [soc@ntnu.no](mailto:soc@ntnu.no) (+47 906 64 350)

## Etter hjemkomst

- Lever tilbake lånt IKT- utstyr. Ikke koble dette opp mot NTNU- nett eller hjemmenett.
- Vær oppmerksom på mistenksomme henvendelser i ulike kanaler. Dette kan være e-post, tekstmeldinger o.l.
- Etter du kommer hjem kan det være lurt å skifte passord på kontoene du har brukt på reisen. Gjør det fra en annen maskin enn den du har brukt på reisen.

## Informasjonssikkerhet

### Ved reiser til land av bekymring

- Det anbefales sterkt at det benyttes PC du ikke benytter til vanlig. Instituttet bør legge til rette for informasjonsheter som er «clean». ID-tag på PC som benyttes, må meldes inn til [sikkerhet@ntnu.no](mailto:sikkerhet@ntnu.no) og instituttleder.
- Bruk 6-sifret PIN eller passord på mobiltelefon og nettbrett. Deaktiver fingeravtrykk og ansiktsgjenkjenning på telefonen, samt aktiver tottrinnsverifisering der det er mulig.
- Ta i bruk verktøy som muliggjør fjernsletting av enhetene dersom den kommer på avveie.

**NTNU**  
**BEREDSKAPSTELEFON**  
+47 800 80 388

**NTNU DIGITAL**  
**SIKKERHET: SOC**  
+47 906 64 350

**UDs OPERATIVE**  
**SENTER**  
+47 239 50 000

**SJØMANSKIRKEN**  
+47 951 19 181

**NØDNUMMER**  
Last ned Sjømannskirken  
sin nødnummerapp for  
lokale nødnummer