



INDENRIGS- OG
SUNDHEDSMINISTERIET

Retningslinjer for brug af departementets it-udstyr på farten og på rejser

Indholdsfortegnelse

1. Sikkerhed på farten og på rejser	3
1.2 Målgruppe og omfang	3
1.3 Trusselsbilledet	3
2 Retningslinjer	4
2.1 Hjemmearbejdspladsen	4
2.2 På farten i Danmark	5
2.3 Tjenesterejser til udlandet	7
2.3.1 Indenfor EU/EØS eller NATO	7
2.3.2 Udenfor EU/EØS eller NATO	7
2.4 Ferierejser	8
3. Særligt vedr. sikkerhedshærdede mobile enheder	9
4. Afvigelser	9

1. Sikkerhed på farten og på rejser

Når du har behov for at medbringe og anvende departementets it-udstyr på andre lokationer end kontoret, skal du være særligt opmærksom på sikkerheden omkring departementets informationer og systemer.

Formålet med retningslinjerne er at beskytte departementets informationer og systemer mod uautoriseret adgang, misbrug, tab, ændring eller afsløring.

Det er vigtigt, at du som medarbejder gør de rette forberedelser og ved, hvordan du skal agere og bruge dit it-udstyr undervejs.

Retningslinjerne er bygget op på den måde, at du i afsnit 2.1 kan læse om, hvordan du skal forholde dig, når du arbejder hjemmefra. I afsnit 2.2 finder du de retningslinjer, som du **altid** skal følge, både når du er på farten i Danmark og på tjenesterejse i udlandet.

Hvis du er på tjenesterejse **uden for** EU/EØS eller NATO, skal du overholde en række yderligere skærpede retningslinjer. Det kan du læse mere om i afsnit 2.3.2, og du vil også blive informeret særskilt herom af ISDB-enheden i forbindelse med den konkrete rejse.

Retningslinjerne gælder også, hvis du efter aftale med din nærmeste leder, medbringer departementets it-udstyr på en ferierejse. Det kan du læse om i afsnit 2.4.

Du skal altid medbringe en **udprintet version** af denne vejledning, når du er på tjenesterejse, så du kan finde information om, hvordan du skal forholde dig, også selvom du har mistet dit it-udstyr og ikke længere kan tilgå retningslinjerne elektronisk.

Du kan læse mere om, hvad du skal gøre, hvis du mister dit it-udstyr på rejsen eller du har mistanke om, at dit it-udstyr er blevet kompromitteret på rejsen i afsnit 2.2, punkt 12: Mistet it-udstyr/mistanke om kompromittering.

1.2 Målgruppe og omfang

Retningslinjerne gælder alle medarbejdere i Indenrigs- og Sundhedsministeriets departement og for alt udstyr, der tilhører departementet, dvs. SIA-PC, mobiltelefon, iPads mv. Når der står it-udstyr i retningslinjerne omfatter det således din SIA-PC, mobiltelefon, iPads mv.

Retningslinjerne supplerer de generelle Retningslinjer vedr. informationssikkerhed for medarbejdere i Indenrigs og Sundhedsministeriets departement, som kan findes [her](#).

1.3 Trusselsbilledet

Cybertruslen er ifølge Politiets Efterretningstjeneste (PET) og Center for Cybersikkerhed (CFCS) tiltaget over de seneste år. CFCS vurderede i 2023, at truslen for cyberspionage er meget høj med bl.a. centrale embedsmænd som oplagte mål.

Stærke aktører med betydelige ressourcer er parate til at udnytte tekniske sårbarheder og eventuel fysisk adgang til vores it-udstyr. En kompromittering kan f.eks. finde sted i en lufthavn, hvor udstyret inspiceres uden dit opsyn.

Selvom du måske ikke har direkte adgang til følsomme og fortrolige oplysninger til daglig, så kan en angriber stadig kompromittere it-systemerne og informationssikkerheden ved at skaffe sig adgang til ministeriets netværk via dine enheder.

Derfor er det vigtigt, at du som medarbejder bidrager til at passe på departementets informationer, når du er på farten eller ude at rejse.

2. Retningslinjer

Der gælder forskellige retningslinjer afhængig af, hvor du skal hen og i nogle tilfælde skal du kontakte IT og/eller ISDB-enheden forud for brug af it-udstyr uden for departementet for nærmere vejledning.

Retningslinjerne dækker fire kategorier for brug af it-udstyr uden for departementet:

- Hjemmearbejdspladsen (afsnit 2.1).
- På farten i Danmark (afsnit 2.2)
- Tjenesterejser i udlandet (afsnit 2.3)
 - Indenfor EU/EØS eller NATO (2.3.1)
 - Udenfor EU/EØS eller NATO (2.3.2)
- Ferierejser (2.4)

2.1 Hjemmearbejdspladsen

Det kræver en høj grad af opmærksomhed på sikkerheden at arbejde hjemmefra for at beskytte departementets informationer og systemer.

1. Benyt egen router

Når du arbejder hjemmefra eller i sommerhuset, må du gerne slutte din SIA-PC og dit it-udstyr til dit private, trådløse netværk, men sørg for, at det er udstyret med en stærk og unik WI-FI-adgangskode. Du skal vælge et password på mindst 15 tegn med en kombination af store og små bogstaver, tal og specialtegn. Du kan finde tips og hjælp til at lave stærke kodeord her: [Lav stærke adgangskoder](#).

2. Hold dit it-udstyr opdateret

It-udstyr kan være sårbart som følge af manglende opdatering af software. Husk derfor at installere de opdateringer, som it-udstyret giver besked om.

3. Anvend kun departementets strømforsyninger, opladere, USB-stik mv.

Tilslut kun USB-stik/opladere m.v. udleveret af departementet til dit it-udstyr. Tilslut aldrig private USB-stik eller strømopladere til dit it-udstyr. Vær opmærksom på, at du ikke må tilslutte dit private udstyr til din arbejdscomputer - heller ikke for at oplade din private mobiltelefon. Det skyldes, at USB-ladere/USB-udstyr får fysisk adgang til dit it-udstyr og derfor kan kompromittere det.

4. Vær opmærksom på dine omgivelser

Sørg for, at dit arbejdsområde er beskyttet mod uautoriseret adgang. Dette gælder også familie og venner. Lås altid din skærm, når du forlader din pc, selv for korte perioder.

Mange danskere har indrettet hjemmet med smart home-enheder, såsom intelligente stemmestyrede assistenter - f.eks. Amazone Alexa eller Google Home, smart fjernsyn, smart højtalere mv. Disse enheder bør slukkes ved hjemmearbejdspladsen, da denne type af enheder automatisk lytter med.

2.2 På farten i Danmark

Når du har departementets it-udstyr med på farten i Danmark, skal du følge nedenstående retningslinjer. Det er f.eks. i forbindelse med eksterne møder, ved konferencer og kurser samt ved transport til og fra arbejde.

1. **Vær opmærksom på, om udenforstående kan få adgang til fortrolige eller følsomme oplysninger, der hvor du sidder.**

Undlad så vidt muligt at arbejde med fortrolige og følsomme oplysninger på offentlige steder, såsom i en lufthavn eller på toget. Er det nødvendigt at arbejde på offentlige steder, så vær opmærksom på at placere dig, så udenforstående ikke kan se med på din skærm. Undlad at have mobile lagringsenheder som USB-stik fremme.

2. **Anskaf skærmfiltre til pc og telefon**

Hvis du jævnligt arbejder på farten, bør du overveje at anskaffe skærmfiltre, så det ikke er muligt for uvedkommende at følge med på dine skærme. Drøft behovet med din nærmeste leder. Skærmfiltre til din PC og din telefon kan bestilles via InternIT@sum.dk

3. **Tænk over omgivelserne og indholdet, når du taler**

Overvej altid om den information, du skal til at kommunikere, egner sig til at blive delt på den måde, du har tænkt dig. Det kan f.eks. være i taxaen, i lufthavnen, i flyet eller på toget, hvor uvedkommende kan lytte med.

4. **Brug din telefon som hotspot til internettet. Brug aldrig fremmede netværk eller åbent Wi-Fi på cafeer, hoteller, biblioteker, lufthavne mv.**

Du må altid bruge Wi-Fi-netværket "SITprod", hvis du bruger dit it-udstyr under et besøg hos andre statslige myndigheder.

Det er ligeledes tilladt at bruge private Wi-Fi-routere med stærk kode på mindst 15 karakterer f.eks. i eget eller lejet sommerhus eller på private besøg

Alle andre netværk end ovennævnte betragtes som fremmede netværk, som du ikke må bruge. Du skal i stedet bruge din arbejdstelefon som hotspot, [se vejledning](#)

Skulle du have anvendt et usikkert netværk, skal du sætte dit it-udstyr til at glemme netværket, så det ikke automatisk kobler på, når netværket er inden for rækkevidde. Det gør du ved at skrive Wi-Fi i søgefeltet nederst til venstre på din PC, vælg Wi-Fi-indstillinger og vælg derefter "Administrer kendte netværk", som er skrevet med blåt. Slet derefter det trådløse netværk.

5. **Anvend kun departementets strømforsyninger, opladere, USB-stik mv.**

Tilslut aldrig fremmede USB-enheder eller strømoladere til dit it-udstyr. USB-ladere/USB-udstyr får fysisk adgang til dit it-udstyr og kan derfor compromittere det.

Undgå i videst mulig omfang brug af USB-stik eller andre eksterne lagerenheder. Brug F2 eller mailen, hvis du skal dele eller tilgå filer på farten. Hvis du f.eks. skal holde et foredrag eller afvikle en konference, skal alle præsentationer sendes på mail.

Evt. dokumenter som for en sikkerhedsskyld opbevares på en lagerenhed skal beskyttes med kode. Du kodeordsbeskytter en USB-lagerenhed ved at sætte den i din PC, hvorefter du skriver bitlocker i søgefeltet i nederste venstre hjørne på skrivebordet på

din PC. I det kontrolpanel, der åbner, kan du sætte kode ved at vælge "Flytbare datadrev" og vælge din USB-enhed. Der må kun benyttes USB-enheder, der er udleveret af InternIT@sum.dk

Vær opmærksom på, at du ikke må tilslutte dit private it-udstyr til din arbejdscomputer, heller ikke til f.eks. at oplade din iPhone.

6. Slå Bluetooth og Wi-Fi fra på dine enheder, når du er udenfor din arbejdsplads

Bluetooth har en lang rækkevidde og søger ofte efter andre enheder. Ved at deaktivere bluetooth sikrer du, at funktionen ikke kan anvendes til sporing eller kompromittering. Brug et headset med ledning, hvis du har brug for at have hænderne fri fra mobilen på farten.

Wi-Fi-netværk, herunder særligt de åbne, kan benyttes til at opsnappe information, men risikoen elimineres effektivt ved at slå Wi-Fi fra på mobile enheder (mobiltelefon og iPad). Tænd kun for det trådløse netværk, når du skal opdatere din mobiltelefon på kontoret.

7. Pas på dit it-udstyr. Hav det altid i nærheden af dig – f.eks. i håndbagagen

Vær særligt opmærksom på steder med mange mennesker, som f.eks. i lufthavne og på banegårde.

8. Medbring kun det nødvendige

Du bør altid nøje overveje, hvad du har brug for at medbringe. Lad f.eks. din pc blive på kontoret, hvis du ikke har behov for at tilgå den ved mødet eller på rejsen. Undgå at medbringe printversioner af arbejdsdokumenter af sensitiv karakter, hvis dette ikke er nødvendigt.

Inden rejsen bør du desuden overveje, om der er e-mails eller andet indhold, som skal slettes på dit it-udstyr.

9. Lån ikke it-udstyret til andre

Du må ikke videregive eller lade andre benytte departementets it-udstyr.

10. Husk at holde dit it-udstyr opdateret, selvom du er på farten

It-udstyr kan være sårbart som følge af manglende opdatering af software. Husk derfor at installere de opdateringer, som it-udstyret giver besked om.

11. Adgang til it-support på rejsen

Du kan få it-support hos Servicedesk i Statens IT (SIT), på tlf. nr. 72 31 00 01 (døgndåben).

12. Mistet it-udstyr/mistanke om kompromittering

Hvis du får mistanke om, at dit it-udstyr (PC, iPad eller mobiltelefon) er blevet kompromitteret, eller hvis du har mistet dit udstyr, skal du straks kontakte Servicedesk hos Statens IT (SIT) på tlf. +45 72 31 00 01 (døgndåben). SIT kan lukke for adgang til din PC og din mobiltelefon. Du modtager en skriftlig kvittering fra SIT på din telefoniske anmeldelse. Når du har teknisk mulighed for det, dvs. når du igen har adgang til dit udstyr, skal du sende denne kvittering fra SIT til isdb@sum.dk.

Du skal informere din nærmeste leder om sikkerhedshændelsen.

*Du må **ikke** bruge dit udstyr, hvis du har mistanke om kompromittering.*

2.3 Tjenesterejser til udlandet

Når du rejser ud af landet, er det ekstra vigtigt at være opmærksom på sikkerheden omkring departementets informationer og systemer.

2.3.1 Indenfor EU/EØS eller NATO

Som udgangspunkt gælder samme retningslinjer, som når du er på farten i Danmark. Det kan du læse om i afsnit 2.2. Det betyder bl.a., at du kan medbringe din bærbare SIA-pc og benytte din arbejdstelefon til internetdeling.

2.3.2 Udenfor EU/EØS eller NATO

Du skal kontakte ISDB-enheden på isdb@sum.dk i god tid og senest 3 uger forud for en rejse til lande udenfor EU/EØS eller NATO, så ISDB-enheden kan foretage en konkret vurdering af informationssikkerheden ifm. rejsen og så det rette rejseudstyr kan nå at blive bestilt hos Statens IT. Departementets IT hjælper dig med at bestille udstyr.

I nogle tilfælde vil ISDB-enheden vejlede om forhold, du skal være ekstra opmærksom på, men som udgangspunkt gælder ovenstående retningslinjer med nedenstående indskærpelser:

1. Du må kun medbringe særligt rejseklargjort it-udstyr på tjenesterejser til lande udenfor EU/EØS eller NATO

Hvis du har brug for at medbringe PC, skal du bestille en "Rejsecomputer" samt "Rejsetelefon" på Statens-IT serviceportal. Kontakt ISDB-enheden før du bestiller udstyret.

Rejsecomputeren kan tilgå nettet via indbygget SIM-kort, alternativt ved at benytte rejsetelefonen som hotspot, så du kan tilgå din virtuelle arbejdsplads (VIA), dvs. de applikationer (f.eks. mail, kalender og F2), som normalt er tilgængelige på din computer. Bestil dit it-udstyr i god tid, så du har mulighed for at teste det (min. 3 uger).

Udstyret skal returneres til departementets IT efter endt rejse.

2. Anvend i videst mulige omfang kun it-udstyret til opgaver, der ikke involverer adgang til følsomme personoplysninger eller på anden vis har sensitiv karakter
Du bør altid nøje overveje, hvad du har brug for at tilgå og arbejde med på din rejse.

3. Hvis du har blandet arbejds- og privattelefon
Enkelte medarbejdere benytter samme telefon i arbejdssammenhæng og privat. Hvis du er en af dem, skal du kontakte ISDB-enheden hurtigst muligt.

4. Undlad at skrive SMS'er, men brug beskedtjenesten Signal App
Almindelig SMS er ikke sikker kommunikation på rejsen. Den krypterede tjeneste "Signal", som findes i Apples app-store, kan installeres på rejsetelefonen og benyttes til evt. skriftlig kommunikation. Du skal hos [SIT bestille en såkaldt ikke-personhenførbart mailadresse](#) og benytte dette ved registrering af Apple-ID. Departementets IT kan bistå med installation og vejledning.

5. Medbring dit it-udstyr som håndbagage og sluk udstyret
Sluk din pc og mobiltelefon helt undervejs på rejsen. En PC, der kun er på vågeblus (f.eks. ved at lukke låget) kan nemmere kompromitteres, hvis den bliver stjålet eller der opnås fysisk adgang til den f.eks. under sikkerhedskontrol i en lufthavn. Det er derfor vigtigt, at din PC er helt lukket ned og din mobil er slukket, når du er undervejs på rejsen.

6. Brug sikkerhedsposer –bestilles via departementets IT.

Vær også opmærksom på, at pengeskabe på hoteller ikke er et sikkert sted at opbevare dit it-udstyr. Selvom pengeskabet er sikret med nøgle eller kode, har personalet ofte en ekstranøgle eller en masterkode. Der er derfor risiko for, at it-udstyret kan blive kompromitteret.

Hvis du er nødt til at efterlade dit it-udstyr på hotellet, skal du anbringe det medbragte it-udstyret i forseglede sikkerhedsposer (og dernæst i pengeskab), så der er muligt at se, om der har været uvedkommende, som har forsøgt at få adgang til indholdet.

Vær opmærksom på at udfylde felterne på sikkerhedsposen omhyggeligt, da det øger synligheden af evt. kompromittering. Skriv til Departementets IT (internIT@sum.dk) og bestil et antal sikkerhedsposer, der passer til rejsens varighed og aktiviteter.

7. Efter rejsen: Skift adgangskode når du kommer hjem

8. Efter rejsen: Evaluer rejsen med dine rejsefæller og del erfaringer med ISDB-enheden

Hvis du har oplevet noget mistænkeligt på din rejse, så meld det til ISDB-enheden.

Afhængig af hvor du har været, vil ISDB-enheden invitere til et kort evalueringsmøde.

Du opfordres til altid at orientere dig i Udenrigsministeriets Rejsevejledninger før enhver udlandsrejse. Rejsevejledningerne er tilgængelige på www.um.dk.

2.4 Ferierejser

Der er som udgangspunkt ikke behov for at medbringe departementets it-udstyr på private ferierejser.

Hvis du og din nærmeste leder ifm. en konkret ferierejse vurderer, at der er et arbejdsmæssigt behov for, at du medbringer dit it-udstyr, gælder følgende:

- I Danmark og indenfor EU/EØS eller NATO kan it-udstyret medbringes, idet retningslinjerne i afsnit 2.2 følges.
- Udenfor EU/EØS eller NATO er det nødvendigt at bestille rejseudstyr, og retningslinjerne under afsnit 2.2 og 2.3 skal følges.

For ledelsesgruppen er det en egenvurdering, hvorvidt der er et arbejdsmæssigt behov, men ovenstående retningslinjer er stadig gældende. Ved behov for at medbringe it-udstyr på en privat rejse udenfor EU/EØS eller NATO, skal du - på samme måde, som hvis det var en tjenesterejse - kontakte ISDB-enheden på isdb@sum.dk i god tid og senest 3 uger forud for en rejse til lande udenfor EU/EØS eller NATO, så ISDB-enheden kan foretage en konkret vurdering af informationssikkerheden ifm. rejsen, og så det rette rejseudstyr kan nå at blive bestilt hos Statens IT. Departementets IT (internIT@sum.dk) hjælper dig med at bestille udstyr.

3. Særligt vedr. sikkerhedshærdede mobile enheder

En mindre gruppe medarbejdere har sikkerhedshærdede mobile enheder (mobiltelefoner og iPads). Hærdede mobile enheder må medbringes på rejser indenfor EU/EØS eller NATO.

Hærdede mobile enheder må som udgangspunkt ikke medbringes udenfor EU/EØS eller NATO.

Kontakt ISDB-enheden for vejledning vedr. den konkrete rejse, da en række forskellige forhold kan gøre sig gældende ift. sikkerheden.

4. Afvigelser

Eventuelle afvigelser fra retningslinjerne vil indebære en risiko for informationssikkerheden i departementet og kan kun under særlige omstændigheder godkendes. Afvigelser skal godkendes af Formanden for departementets Cyber-, Informationssikkerheds og Databeskyttelsesudvalg.

Version	Udarbejdet af	Bemærkninger	Dato
1.0.	ISDB	Godkendt af CID-udvalg	13-12-2024
1.1	ISDB	Indføjet supplerende vejledende tekst Godkendt af CID-udvalg Godkendt af Direktion Behandlet i Samarbejdsudvalg	5-02-2025 21-02-2025 18-03-2025