digitaliserings ministeriet

Enhed
Administration og Økonomi

Sagsbehandler
Tobias Christoffer Thykjær

Koordineret med

Sagsnr.
2023 - 1432

Doknr.
15017

Dato
06-03-2026

Retningslinjer for informationssikkerhed for medarbejdere i Digitaliseringsministeriets departement

1. Indledning

Retningslinjerne følger departementets informationssikkerhedspolitik og beskriver den accepterede brug af departementets informationer og informationssystemer. Retningslinjerne har status som intern tjenesteinstruks til alle ansatte, hvilket betyder, at manglende overholdelse kan medføre disciplinære konsekvenser efter de regler, som gælder for dit ansættelsesforhold.

Retningslinjerne er fastsat på baggrund af departementets risikovurderinger og skal bidrage til at reducere identificerede risici for fortrolighed, integritet og tilgængelighed af informationer.

Alle medarbejdere, herunder konsulenter og andre eksterne med adgang til departementets informationer og systemer, skal overholde retningslinjerne i det omfang, det er relevant for deres opgaver.

Retningslinjerne revideres løbende og ajourføres ved væsentlige ændringer i trusselsbilledet, lovgivning, organiseringen eller departementets it-miljø. Efterlevelse følges gennem interne kontroller og audits med det formål at understøtte god praksis og kontinuerlig forbedring.

2. Organisering

Ansvaret for informationssikkerheden er placeret hos departementschefen, informationssikkerhedsgruppen og den enkelte medarbejder

- Departementschefen har det øverste ansvar for informationssikkerheden i departementet
- Informationssikkerhedsenheden i Administration og Økonomi udfører til daglig den praktiske styring, planlægning, implementering og overvågning mv. af informationssikkerheden.
- Den enkelte medarbejder har et individuelt ansvar for medvirken til at opretholde informationssikkerheden.

3. Adgangsforhold og lokaler

Departementets fysiske faciliteter på Stormgade 2-6 er sikret med adgangskontrol ved alle indgangsdøre. Du skal ved din adgang enten fremvise dit adgangskort til receptionen eller bruge de opsatte kortlæsere. Henvend dig i receptionen, hvis du har glemt dit adgangskort.

Man må kun lukke en person ind, som har et gyldigt ærinde til ministeriet, eller som kan fremvise gyldigt adgangskort. Leverandører og eksterne konsulenter skal bære synlig nøglesnor, der udleveres i receptionen. Øvrige gæster må aldrig gå alene rundt i bygningerne. Du skal følge dine gæster ind og ud af bygningerne, medmindre der foreligger en dispensation fra en kontorchef.

Enkelte lokaler i departementet er aflåst. Relevante medarbejdere får efter behov udleveret kode til nøgleboks eller tildelt de nødvendige rettigheder på deres adgangskort.4. Klassifikation og behandling af informationer

4.1 Kategorisering og klassifikation af informationer

Der skelnes i departementet mellem nedenstående typer af oplysninger. Et dokument kan godt tilhøre flere kategorier. Formålet er at sikre en tilstrækkelig beskyttelse af de enkelte informationer. Den medarbejder, der arbejder med en given information, har ansvaret for at vurdere, hvilken kategori informationen tilhører, og dermed omfanget af beskyttelse af informationen.:

1. Offentlige informationer

2. Informationer om personer (personoplysninger)
    a. Følsomme personoplysninger
    b. Almindelige personoplysninger
    c. Oplysninger om strafbare forhold
    d. Fortrolige personoplysninger
3. Interne informationer
4. Til tjenestebrug (NATO RESTRICTED)
5. Fortrolige informationer (NATO CONFIDENTIAL)
6. Hemmelige informationer (NATO SECRET)
7. Yderst hemmelige oplysninger (COSMIC TOP SECRET)

- 1. Offentlige informationer

Offentlige informationer er informationer, som alle kan få adgang til. Det kan for eksempel være informationer tilgængelige på ministeriets hjemmeside eller andre informationer, som under normale omstændigheder oplyses til alle, der retter henvendelse herom.

Der er ingen særlige krav til behandling eller opbevaring af offentlige informationer. Ligeledes skal der heller ikke tages nogen særlige hensyn ved destruktion af offentlige informationer.

- 2. Informationer om personer

Databeskyttelsesforordningen inddeler personoplysninger i to hovedkategorier: almindelige personoplysninger og følsomme personoplysninger. Herudover er oplysninger om strafbare forhold og om personnummeret særligt reguleret. Endelig anvendes i Danmark begrebet fortrolige personoplysninger.[1]

Kun medarbejdere med et arbejdsbetinget behov må tilgå følsomme og i øvrigt fortrolige personoplysninger. Informationerne skal opbevares sikkert, jf. afsnit 3, og kommunikeres således, at de ikke kan komme uvedkommende i hænde.

I departementets ESDH-system (F2) beskyttes visse sager med personoplysninger, eksempelvis personalesager, automatisk med indblik begrænset til enheden ved deres oprettelse. Andre sager belægges med indblik ved oprettelsen. Det gælder f.eks. ØU og KU-sager. Generel vejledning i, hvordan og hvilke sager der belægges med indblik findes bl.a. på intranettet. Evt. kontorspecifikke procedurer og instrukser udleveres af det enkelte kontor ved ansættelsens start.

Digital kommunikation af følsomme og i øvrigt fortrolige personoplysninger gennem usikre netværk, herunder internettet, skal altid ske i krypteret form. Vejledning om, hvordan man sender sikkert, findes på intranettet.

Digital kommunikation gennem interne netværk, f.eks. fra en arbejdsmail til en anden arbejdsmail inden for departementet eller mellem Statens It's kunder, anses for sikker e-post, idet informationsudveksling på interne netværk ikke skal krypteres.

Destruktion af følsomme og fortrolige personoplysninger og i øvrigt fortrolige oplysninger skal ske på sikker vis. Informationer i papirformat skal afleveres i de opstillede containere til sikkerhedsmakulering i kopi-rummene. Digitale medier, for eksempel USB-nøgler og harddiske, skal afleveres til departements afdeling for Økonomi og Administration, der sørger for korrekt destruktion.

[1]

Der henvises i øvrig til vejledningsmateriale på intranettet om persondatabeskyttelse.

- 3. Interne informationer
- Interne informationer er informationer, som indgår i den daglige drift. Det kan for eksempel være visse informationer på departements intranet. Alle medarbejdere må få adgang til interne informationer. Som udgangspunkt må interne informationer kun anvendes og kommunikeres internt i departementet. Informationerne skal behandles med omtanke, men det er ikke nødvendigt at tage særlige hensyn for at sikre informationerne. 4-7. Klassificerede informationer

Informationer, der er kategoriseret som "Til tjenestebrug" eller højere, er klassificerede og må kun tilgås af medarbejdere med sikkerhedsgodkendelse på mindst det relevante niveau. Der findes TTJ-versioner af både mail- og ESDH-løsningen.

Der findes særskilte retningslinjer for behandling af klassificerede oplysninger, som medarbejdere vil blive informeret om i forbindelse med adgang til de pågældende miljøer.4.2. Søgning og tilgang til informationer og sager

Søgning og tilgang til informationer og sager, herunder i ESDH-systemet, må alene ske som følge af et arbejdsbetinget behov og må aldrig ske i privat øjemed. Alle søgninger og opslag i ESDH-systemet logges, og loggen er løbende genstand for kontrol.

5. Anvendelse af departementets it-systemer

Du skal låse eller slukke pc-arbejdspladsen, når den forlades i længere tid.

Programmel, der kan hentes fra Statens It's softwarecenter, er forhåndsgodkendt til installation på departementets PC'er. Det er som udgangspunkt ikke tilladt at installere øvrige programmer. Der kan dog anvendes extensions og plug-ins til allerede godkendt programmel – f.eks. adblockers i browsere, der kan bidrage til at øge sikkerheden på internettet. Kontakt it i AMØK, hvis du har brug for et program, der endnu ikke er godkendt.

Når du udskriver dokumenter, skal du opholde dig ved printeren, så uvedkommende ikke får adgang til følsomme eller fortrolige personoplysninger eller fortrolige udskrifter i øvrigt.

6. Rejser

På rejser er der trusler ud over dem, der er relevante til hverdag. Medarbejdere bør derfor udvise skærpet opmærksomhed omkring sikring af data og information, når de anvender departementets it-systemer eller udstyr under en rejse.

Det er ikke tilladt at anvende eller tilgå departementets it-systemer via et åbent netværk. Medarbejdere opfordres til at benytte internetdeling via. deres telefon. Medbragt IT-udstyr skal altid holdes under opsyn. Udstyret må aldrig udlånes til andre.

Bluetooth skal deaktiveres på alle enheder. Bluetooth kan forbinde enheden til et trådløst headset, overføre data eller sågar give adgang til enheden.

Ved arbejde i det offentlige rum skal der tages de nødvendige forholdsregler for at sikre, at følsomme og fortrolige personoplysninger og fortrolige informationer i øvrigt ikke kommer uvedkommende til kendskab. Et skærmfilter kan bestilles hos service. Man må ikke benytte offentligt tilgængelige computere – eksempelvis i en lufthavn eller på et hotel – til at få adgang til departementets systemer (inklusiv mailboks).

Vær opmærksom på tegn på brud på sikkerheden og meld mistænkelige hændelser via formularen på intranettet. Der er aktører, som forsøger at udnytte, at departementets medarbejdere er på tjenesterejse. Det er derfor vigtigt, at du som medarbejder rapporterer enhver mistanke om en sikkerhedshændelse. Det bør ske hurtigst muligt, så der kan reageres på situationen

Der henvises i øvrigt til bilaget *IT-sikkerhed på rejser.*

6.1 Rejser uden for EU

Der kan være yderligere risici forbundet med rejser uden for EU. Administration og Økonomi skal kontaktes forud for rejsen for gøre opmærksom på særlige forholdsregler og evt. udlevering af rejseudstyr i forbindelse rejsen til det pågældende land.

7. Passwords

Retningslinjer for passwords varierer for de enkelte systemer, du skal dog altid søge at vælge et password på mindst 12 karakterer med en kombination af store og små bogstaver, tal og specialtegn.

Passwords, som benyttes i arbejdsmæssig sammenhæng, bør ikke anvendes til private formål, og du skal sørge for, at de ikke kommer andre i hænde.

Ved din ansættelse udleveres der et midlertidigt password, som du skal ændre ved første log-on.

Genåbning ved spærret konto foretages via Statens It's Serviceportal eller Servicedesken.

8. Lokal- og fællesdrev

SIA-PC'en har et lokalt drev (C-drevet), der kan slettes uden varsel i forbindelse med system-opdateringer og installation af nye programmer mv. Undgå derfor at gemme materiale på drevet.

Personligt-drev (navnet afhænger af opsætningentypisk H-drevet) er et drev til lagring af dokumenter, som kun du har adgang til via dit Statens It-login. Drevet er ikke afhængigt af din lokale SIA-PC og kan også tilgås fra øvrige enheder.

Fællesdrevet (typisk K-drevet) og de tilhørende undermapper for de enkelte kontorer er mappe, der som udgangspunkt er bredt tilgængeligt for alle medarbejdere i departementet eller det enkelte kontor.

Der foretages daglig sikkerhedskopiering af kontordrev og dit personlige fildrev. Anvend derfor disse placeringer til de arbejdsrelaterede dokumenter. Der må kun i begrænset omfang lagres dokumenter uden arbejdsmæssig relevans på de to drev.

Alle filer og informationer, der befinder sig på udstyr udleveret af departementet, betragtes fortsat som statens ejendom. Departementet har således adgang til alle data – også på personligt-drev – hvis der er en saglig grund herfor.

Personoplysninger, der er sagsdannende, kan i en afgrænset periode gemmes på lokal- og netværksdrev, inden de overføres til journaliseringssystemet.

Personoplysninger, der ikke er sagsdannende, skal slettes, når der ikke længere er et sagligt grundlag for opbevaring af dem. Følsomme og fortrolige personoplysninger skal slettes inden for en måned.

Kontorerne skal periodisk foretage en gennemgang af lokal- og netværksdrevene med henblik på at rydde op i lagrede data. Krypteret data kan ligge ubegrænset på fildrevene uanset deres indhold.

9. Bærbare datamedier

Bærbare medier - bl.a. USB-drev, harddiske og bærbare PC'er - har en væsentlig risiko for at blive tabt, stjålet eller glemt. Beskyt derfor filer på USB-drev mv. med kryptering og hold kodeordet hemmeligt. Din SIA-PC fra Statens It er allerede krypteret.

Du må kun benytte USB-drev mv., der kommer fra en kilde, du har tillid til. USB-drev skal være beskyttet med kryptering (Bitlocker).

Alle medier, som ikke længere skal anvendes, skal afleveres til Administration og Økonomi med henblik på sikker destruktion.

10. Systemopdateringer

Statens It udsender løbende vigtige sikkerhedsopdateringer, og det er nødvendigt at genstarte pc'en for at fuldføre installationerne. Ved arbejdstidens ophør bør man derfor altid logge sig af samtlige systemer og lukke maskinen ned, så systemopdateringerne gennemføres.

11. Internet

Du skal udvise forsigtighed i forhold til, hvilke websites der besøges, og hvilke informationer du oplyser. Din anvendelse af internettet må ikke skade departementets omdømme.

Departementet tillader privat brug af internettet, forudsat at dette ikke leder til misbrug, sikkerhedskompromittering, påvirker departementets omdømme, er uforeneligt med arbejdet i departementet eller går ud over den enkeltes arbejdsindsats, samt i øvrigt ligger inden for de fastsatte retningslinjer.

Dokumenter eller andre filer, der hentes eller åbnes direkte fra internettet, skal behandles med stor forsigtighed – specielt hvis afsenderen er ukendt, eller indholdet er usædvanligt.

11.1 Anvendelse af generativ kunstig intelligens

Der eksisterer særskilte retningslinjer for anvendelse af generativ kunstig intelligens (AI) i departementet, som kan findes på intranettet.

Som udgangspunkt er det tilladt at anvende generative AI-værktøjer, såfremt retningslinjerne følges. Retningslinjerne omfatter blandt andet:

1. Du er ansvarlig for alt indhold produceret ved brug af generativ AI.
2. Personoplysninger eller fortrolige oplysninger må ikke deles med offentligt tilgængelige AI-værktøjer.
3. Vær kritisk over for output fra generativ AI og vurder korrekthed, relevans og sikkerhed.
4. Brug ikke generativ AI til at træffe automatiske afgørelser.
5. Vær åben om anvendelsen af AI i opgaveløsningen.

12. E-mail

E-mail-systemet er som udgangspunkt alene beregnet til arbejdsmæssig brug. Al indgående og udgående e-post tilhører derfor departementet. E-post dækker både E-mail, Digital Post mv.

Departementet tillader dog privat brug af e-mail-systemet, forudsat at dette ikke leder til misbrug, sikkerhedskompromittering, påvirker departementets omdømme, er uforeneligt med arbejdet i departementet eller går ud over den enkeltes arbejdsindsats, samt i øvrigt ligger inden for de fastsatte retningslinjer.

Det anbefales at mærke privat udgående e-post "privat" i emnefeltet, samt at oprette en mappe kaldet "privat" til opbevaring af modtaget privat e-post.

Generelt forudsættes det, at medarbejderne ved brug af e-post tager samme hensyn til professionel tone og sprogbrug, form og indhold, som ved anvendelse af departementets brevpapir.

Der må kun sendes e-post, som indeholder følsomme eller fortrolige personoplysninger eller fortrolige informationer i øvrigt til modtagere uden for ministeriet, hvis der benyttes kryptering.

E-post, som indeholder følsomme eller fortrolige personoplysninger eller fortrolige informationer i øvrigt, skal desuden slettes fra e-post-systemet, når de ikke længere er nødvendige og senest efter en måned. Oplysninger, der er sagsdannende, skal forinden journaliseres i departementets sagsbehandlersystem. Dette gælder både for modtaget og afsendt e-post.

Links, dokumenter eller andre filer, der modtages med e-post, skal behandles med stor forsigtighed – specielt hvis afsenderen er ukendt, eller indholdet er usædvanligt.

13. Hjemmearbejde og fjernadgang

Adgang til departementets systemer og informationer uden for departementets fysiske rammer er også omfattet af alle dele af retningslinjerne for informationssikkerhed.

Når der arbejdes uden for arbejdspladsen, skal man i øvrigt sikre, at uvedkommende ikke kan få adgang til eventuelle papirudskrifter, og at udskifter mv. opbevares sikkert og makuleres på behørig vis – f.eks. ved at medbringe materialet til sikkerhedsmakulering i departementet.

Ved arbejde i det offentlige rum skal der tages de nødvendige forholdsregler for at sikre, at følsomme og fortrolige personoplysninger og fortrolige informationer i øvrigt ikke kommer uvedkommende til kendskab. Et skærmfilter kan bestilles hos service.

13.1. Fjernadgang til it-systemerne

Fjernadgang til departementets it-systemer kan og må kun ske på følgende måder:

- SIA-PC gennem VPN-opkobling (Cisco secure client)
- Statens It's Citrix miljø "VIA" (via.statens-it.dk).
- Adgang via mobil enhed gennem MDM-systemet (f.eks. Boxer, Workspace one web, F2 mobile).

Ved brug af fjernadgangene igennem VPN eller VIA er det vigtigt, at man husker at afbryde forbindelsen, når adgangen ikke længere skal benyttes.

Man må ikke benytte offentligt tilgængelige computere – eksempelvis i en lufthavn eller på et bibliotek – til at få adgang til departementets systemer. Der gøres desuden opmærksom på, at der som led i den generelle systemovervågning, jf. pkt.14, også ved fjernadgang foretages logning af aktiviteter i departementets systemer.

13.2. Anvendelse og genudlån af ministeriets pc'er

For pc'er, mobiler og andet udstyr, som ejes af ministeriet, gælder en række særlige forhold.

Udstyret er alene udlånt i tjenstligt øjemed. Det betyder, at det kun må benyttes af brugeren – udstyret må derfor ikke genudlånes til eksempelvis familiemedlemmer.

Det er brugerens ansvar at sikre, at uvedkommende ikke kan få adgang til data fra eller via pc'en. Udstyr bør derfor ikke efterlades uovervåget i det offentlige rum og skal så vidt muligt opbevares aflåst. Under rejser skal bærbare pc'er altid medbringes som håndbagage.

14. Anvendelse af mobile enheder

Departementet udleverer mobile enheder (mobiltelefoner og iPads) til medarbejderne. Disse registreres i Statens It's Mobile Device Management System (MDM) og er sat op til at synkronisere med arbejdsmail. Private enheder kan også anvendes, se afsnit 14.1.

MDM-systemet kan uden varsel låse og slette data på enheden, f.eks. hvis de tabes, stjæles eller bortkommer.

Departementet bærer intet ansvar for sletning af alle data på mobile enheder, arbejdsmæssige, såvel som private enheder. Data, herunder private data, vil ikke kunne genskabes efterfølgende.

Du skal sørge for, at telefon eller iPad er opdaterede ved altid at acceptere, når enhederne foreslår opdateringer. Større opdateringer kan kræve, at enheden er tilsluttet wi-fi forbindelse. Du skal derfor sørge for, at enheden med jævne mellemrum har adgang til dit eget eller departementets wi-fi netværk, så enheden kan modtage de nødvendige opdateringer.

Den mobile enhed skal være beskyttet af adgangskode eller fingeraftryk. Opstår der mistanke om, at uvedkommende har fået kendskab til koden, skal denne straks skiftes på alle relevante enheder.

14.1 Private enheders adgang til data

Hvis du vil synkronisere mails på en privat enhed, skal enheden registreres i Statens It's MDM-system, og du accepterer samtidig, at din enhed kan låses, eller data slettes, hvis enheden tabes, stjæles eller bortkommer mv. Du skal behandle de private enheder på lige fod med enheder udleveret af departementet.

De data, der synkroniseres til private enheder, er forretningsdata. Derfor må mobile enheder, hvortil der er etableret synkronisering til arbejdsmail mv., ikke anvendes af eller udlånes til andre, jf. afsnit 13.2.

Medarbejderen bærer selv eventuelle omkostninger til datatransmission på private enheder, herunder ved rejser til udlandet.

14.2 Tjenesterejser og private rejser med udstyr der synkroniserer med F2 og mail

Ved tjenesterejser uden for EU eller private rejser uden for EU skal Administration og Økonomi kontaktes med henblik på vejledning om IT-sikkerhedsmæssige forhold, hvis der medbringes og anvendes enheder, udleveret af arbejdspladsen, eller som tilgår eller synkroniserer med F2, mail mv.

15. Rapportering af hændelser

Hvis en medarbejder har mistanke om eller kan konstatere trusler mod eller brud på informationssikkerheden, skal dette straks rapporteres til departementets Informationssikkerhedskoordinator via formularen på intranettet eller til kontorchefen for Administration og Økonomi, som inddrager øvrige relevante parter, herunder Informationssikkerhedskoordinatoren, DPO og HR.

Derudover skal trusler mod eller brud på informationssikkerheden også rapporteres til Statens It's Servicedesk.

Ved rapportering af en hændelse er det vigtigt, at medarbejderen har noteret sig så mange detaljer som muligt. Det er samtidig vigtigt, at medarbejderen ikke selv forsøger at afhjælpe eller undersøge sagen, da problemet uforsætligt kan forværres, ligesom eventuelt bevismateriale kan mistes. Hvis hændelsen er opstået i forbindelse med brugen af en pc, skal medarbejderen sørge for, at skaderne mod netværket søges begrænset – f.eks. ved at slukke pc'en.

Truslerne rettet mod it-brugerne er under stadig forandring, og du kan finde information om de aktuelle trusler på intranettet.

16. Sikkerhedskopiering

Relevante data sikkerhedskopieres af Statens It for at kunne genskabe tabte data. Relevante data er eksempelvis e-mails, data på netværksdrev og data i F2.

17. Overvågning af it-systemer

Af hensyn til departementets driftsstabilitet og sikkerhed samt til kontrol af medarbejdernes anvendelse af ESDH-systemet foretages automatisk logning af alle brugernes handlinger - herunder netværkskommunikation og brug af ESDH, internet og e-post.

Som en del af drifts- og sikkerhedsarbejdet sker der løbende kontrol af logs. Der foretages også kontinuerlig generel overvågning af netværket og driftsmiljøet af både Statens It samt Center for Cybersikkerhed, m.fl. uden forudgående varsel.

I ekstraordinære tilfælde kan departementet få adgang til din e-post, hvis det er nødvendigt af hensyn til sikkerheden eller som led i efterforskning af lovbrud. Det kan f.eks. være ved konkret mistanke om igangværende misbrug, hackerangreb eller andre alvorlige sikkerhedstrusler, samt i forbindelse med efterforskning, reetablering efter sikkerhedshændelser eller genopretning efter nedbrud.Af hensyn til departementets drifts- og informationssikkerhed foretages løbende sikkerhedskopiering af log-filerne. Sikkerhedskopien opbevares i to år.

Der kan gælde særlige forhold vedrørende overvågning af de enkelte brugersystemer. Dette vil altid fremgå af sikkerhedsinstruksen for det enkelte system.

18. Systemspecifikke retningslinjer og vejledninger

For flere af departementets systemer, f.eks. F2 og Navision, gælder specifikke sikkerhedsinstrukser og vejledninger. Brugerne vil blive bekendtgjort med disse i forbindelse med oprettelse som bruger af systemet.

19. Ikrafttrædelse

Nærværende retningslinjer er gældende fra den 13. februar 2026