digitaliserings og ligestillingsministeriet

Enhed
Administration og Økonomi

Sagsbehandler
Tobias Christoffer Thykjær

Koordineret med

Sagsnr.
2023 - 1432

Doknr.
15017

Dato
03-05-2023

Retningslinjer for informationssikkerhed for medarbejdere i Digitaliserings- og Ligestillingsministeriets departement

Indholdsfortegnelse

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.

2. Organisation og tilsyn

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

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

3. Adgangsforhold og lokaler

Departementet 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. 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.

Visse af departementets lokaler er desuden sikrede gennem det interne låsesystem. Relevante medarbejdere får ved ansættelsen udleveret en nøgle gældende til kontorets lokaler. Opbevares der følsomme eller i øvrigt fortrolige personoplysninger i kontoret (se nærmere i afsnit 4.3), skal dette tillige låses, hvis det er praktisk muligt.

4. Klassifikation og behandling af informationer

I departementet inddeles dokumenter i fire kategorier: offentlig information, intern information, informationer om personer og fortrolig information. 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. Medarbejderen skal periodisk tage kategoriseringen op til revurdering.

4.1. 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.

4.2. 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.

4.3. 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.

4.4 Fortrolige informationer i øvrigt

I dette afsnit omtales håndteringen af fortrolige informationer, der ikke omhandler personer.[2]

Fortrolige informationer skal opbevares sikkert og kommunikeres således, at de ikke kan komme uvedkommende i hænde.

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

1

Almindelige personoplysninger – er alle oplysninger, der ikke er kategoriseret som følsomme. Det kan f.eks. være identifikationsoplysninger som navn og adresse, oplysninger om økonomiske forhold, familieforhold, CV, arbejdsområde, kundeforhold eller andre lignende ikke-følsomme oplysninger. Almindelige personoplysninger kan godt samtidig være fortrolige, jf. nedenfor.
Følsomme personoplysninger – er oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold, genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, fx fingeraftryk, helbredsoplysninger og oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.
Fortrolige personoplysninger i øvrigt – er oplysninger, der efter den almindelige opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab. Følsomme personoplysninger vil altid være fortrolige, men ikke alle fortrolige personoplysninger er følsomme. Personnummeret er et eksempel på en fortrolig oplysning, der er særskilt reguleret i databeskyttelsesloven. Herudover vil oplysninger om strafbare forhold, økonomiske, sociale eller andre private forhold efter en konkret vurdering kunne være fortrolige.

2

Fortrolige informationer defineres i forvaltningslovens afsnit vedr. tavshedspligt (§ 27 og 28, jf. lov nr. 571 af 19. dec. 1985), samt straffelovens § 152, stk. 3, jf. lovbekendtgørelse nr. 1034 af 29. oktober 2009. Dette inkluderer informationer, som er nødvendige at hemmeligholde af hensyn til det offentliges interesser, herunder udførelsen af det offentliges forretningsvirksomhed. I henhold til forvaltningsloven må den, der virker inden for den offentlige forvaltning, ikke i den forbindelse skaffe sig fortrolige oplysninger, som ikke er af betydning for udførelsen af den pågældendes opgaver. Der gælder desuden tavshedspligt for fortrolige informationer. Fortrolige informationer må således kun behandles af og kommunikeres til personer med et arbejdsmæssigt behov.

Som omtalt i afsnit 4.3 skal internt digital kommunikation – f.eks. mellem arbejdsmail hos Statens It's kunder - ikke krypteres.

Der gælder også samme regler som i afsnit 4.3 om destruktion af informationer i papirformat via sikkerhedsmakulering, og brugte digitale medier afleveres til Administration og Økonomi.

4.5. 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 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 Statens It, 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. Passwords

Retningslinjer for passwords varierer for de enkelte systemer, du skal dog altid søge at vælge et password på mindst 8 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.

7. 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.

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.

Kontor-drevet (navnet afhænger af kontoret) er et fællesdrev, hvor alle medarbejdere i kontoret og potentielt hele departementet har adgang til drevet og foldere.

Personligt-drev (navnet afhænger af opsætningen) er et drev til lagring af dokumenter, som kun du har adgang til.

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.

8. 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. Du kan få hjælp af Administration og Økonomi til at kryptere bærbare medier.

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

9. Windows opdateringer og antivirus mv.

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

10. 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. 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.

12. Hjemmearbejdspladser

Departementet stiller hjemmearbejdspladser til rådighed for medarbejderne. Disse løsninger og anvendelsen heraf 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.

12.1. Fjernadgang til it-systemerne

Det er muligt at få fjernadgang til departementets it-systemer gennem en VPN-opkobling af din SIA PC. Der er ligeledes adgang til Citrix-baserede løsninger. Adgangene styres med to-faktor autentifikation – f.eks. koder modtaget via SMS eller apps – og udstyr til understøttelse af disse elementer af løsningerne er personlige og må ikke videregives eller udlånes.

Citrix-løsningen har af sikkerhedshensyn begrænsninger på overførsel af filer. Medarbejdere, der har fået adgang til departementets netværk fra egen private pc, bør desuden sikre sig, at pc'en er sikkerhedsmæssig tilstrækkelig konfigureret, at styresystemet er fuldt opdateret og ikke lade andre bruge pc'en, mens den er forbundet til departementets netværk. Der må på intet tidspunkt opbevares arbejdsrelaterede følsomme eller fortrolige personoplysninger eller fortrolige informationer i øvrigt på private pc'er.

Ved brug af fjernadgangene er det vigtigt, at man husker at logge af netværket, 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 hjemmearbejde foretages registrering af den enkeltes log on, log off og tidsforbrug mv.

12.2. Anvendelse og genudlån af ministeriets pc'er

For pc'er 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. Bærbare pc'er 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.

13. Anvendelse af mobile enheder

Departementet udleverer mobile enheder (mobiltelefoner og iPads) til medarbejderne. Disse er på forhånd registreret i departementets Mobile Device Management System (MDM) og er sat op til at synkronisere med arbejdsmail. Private enheder kan også anvendes, se afsnit 13.1.

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 kræver, 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.

13.1 Private enheders adgang til data

Hvis du vil synkronisere mails på en privat enhed, skal enheden registreres i departementets 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 12.2.

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

Der ydes fra ministeriets side ikke support til private enheder - herunder opsætning af synkronisering mv.

13.2 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.

14. 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.[3]

3

Sikkerhedsbrud, fejl eller sårbarheder inkluderer, men er ikke begrænset til følgende:
- Tab af it-udstyr, mobiltelefon, fysiske dokumenter mv.
- Hvis der er adgang til informationer, som ikke burde være tilgængelige.
- Hvis adgang til informationer, som burde være tilgængelige, er mistet.
- Hvis informationer kan være kommet de forkerte personer i hænde.
- Hvis retningslinjer eller procedurer ikke følges.
- Fejl i systemer eller udstyr.
- Angreb fra virus, skadelige programmer eller lignende i it-systemerne.

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.

15. Sikkerhedskopiering

Relevante data sikkerhedskopieres af IT for at kunne genskabe tabte data. Relevante data er eksempelvis e-mails, data på netværksdrev og data i F2. Genskabelse af den seneste version af et dokument, der er taget backup af, kan ske ved henvendelse til Statens It.

16. 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.

Departementet kan få adgang til din e-post øjeblikkeligt ved mistanke om igangværende misbrug, hacker-angreb, sikkerhedstrusler, efterforskning, reetablering efter sikkerhedshændelser eller genopretning efter nedbrud.

Derudover kan din nærmeste chef eller formanden for informationssikkerhedsgruppen beslutte, at der skal gives adgang til din e-post. Det kan f.eks. være, hvis du er utilgængelig i en længere periode, eller din ansættelse er ophørt. Privat e-post i mail-systemet, som ikke har nogen relation til departementet, læses som udgangspunkt ikke af andre.

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.

17. 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.

18. Ikrafttrædelse

Nærværende retningslinjer træder i kraft den 15. maj 2023

- Enhver anden hændelse, der vedrører fortroligheden, integriteten eller tilgængeligheden af departementets informationer.