INDENRIGS- OG
SUNDHEDSMINISTERIET

Informationssikkerhed

Retningslinjer for medarbejdere i
Indenrigs- og Sundhedsministeriets departement

Indenrigs- og Sundhedsministeriet
Januar 2026

Indholdsfortegnelse

1. Indledning

Retningslinjerne følger departementets informationssikkerhedspolitik og beskriver den accepterede brug af departementets informationer og informationssystemer.

2. Organisation og tilsyn

Ansvaret for informationssikkerheden er placeret hos departementschefen, Cyber-, Informationssikkerhed- og Databeskyttelsesudvalget og den enkelte medarbejder.

- Departementschefen har det øverste ansvar for informationssikkerheden i departementet.
- Cyber-, Informationssikkerhed- og Databeskyttelsesudvalget udfører til daglig den praktiske ledelse, planlægning, implementering og overvågning mv. af informationssikkerheden.
- Hver enkelt 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 vagten i receptionen eller bruge de opsatte kortlæsere. Henvend dig i receptionen, hvis du har glemt eller mistet 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 4.1.3), skal dette tillige låses, hvis det er praktisk muligt.

4. Behandling af informationer og klassifikation efter sikkerhedscirkulæret

Afsnit 4.1 og afsnit 4.2 definerer de forskellige informationskategorier som departementet og staten arbejder med og beskriver de specifikke sikkerhedsforanstaltninger og regler, der skal anvendes for hver kategori.

- Afsnit 4.1 omhandler informationer kategoriseret efter departementets interne retningslinjer.
- Afsnit 4.2 omhandler informationer klassificeret efter sikkerhedscirkulæret.

4.1. Behandling af informationer internt i departementet

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 – f.eks. at der påsættes adgangsbegrænsning i sagsbehandlingssystemerne, at du vurderer, om et dokument kan deles med andre, og når vi skal vurdere, om der kan gives aktindsigt i informationerne.

Den medarbejder, der arbejder med en given information kategoriseret efter afsnit 4.1.1 til 4.1.4, har ansvaret for at vurdere, hvilken kategori informationen tilhører og dermed omfanget af beskyttelse af informationen. Der er *ikke* krav om, at informationerne, kategoriseret efter afsnit 4.1.1 til 4.1.4, skal mærkes. Medarbejderen skal periodisk tage kategoriseringen op til revurdering.

4.1.1. 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.

4.1.2. 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.

4.1.3. Informationer om personer

Databeskyttelsesforordningen inddeler personoplysninger i to hovedkategorier: almindelige personoplysninger og følsomme personoplysninger. Herudover er oplysninger om strafbare forhold og om personnummer 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 automatisk med indblik begrænset til enheden ved deres oprettelse. Det gælder f.eks. personalesager i HR og (Koncern) DPO-sager, samt visse sager i Borgerbrevsenheden og CPR-administrationen. Andre sager belægges med adgangsbegrænsning (indblik) ved oprettelsen. Generel vejledning i, hvordan og hvilke sager, der belægges med indblik findes bl.a. på intranettet i "guidelines for god journaliseringspraksis". Der er desuden en vejledning i F2 om adgangsbegrænsning, der kan fremfindes ved søgning på "adgangsbegrænsning" i "F2 Hjælp". 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, behøver ikke at blive krypteret, idet informationsudveksling på interne netværk er vurderet som sikkert. Vær opmærksom på, at det ikke gælder for digital kommunikation med Lægemiddelstyrelsen, da de ikke er kunder hos Statens It.

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 personligt til en medarbejder i "Intern IT" i departementet, der sørger for korrekt destruktion.

[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.

4.2. Behandling af informationer klassificeret efter sikkerhedscirkulæret

Hvis du skal behandle informationer, der er klassificeret efter sikkerhedscirkulæret, er det et krav, at du sætter dig ind i cirkulæret og kender til, hvordan du håndterer klassificeret materiale. Der findes endvidere undervisning på CAMPUS i anvendelse af sikkerhedscirkulæret i praksis.

Man må kun arbejde med klassificeret information på godkendt udstyr og opbevare klassificeret information i godkendte skabe. Når information er klassificeret efter sikkerhedscirkulæret, er der en række minimumskrav til bl.a. opbevaring, transport, mærkning af dokumenter og håndtering af oplysningerne i de klassificerede dokumenter i øvrigt.

Du skal altid følge kravene til behandlingen af oplysningerne ud fra den angivne klassifikation (Til tjenestebrug, Fortroligt, Hemmeligt, Yderst Hemmeligt), når materiale er klassificeret i henhold til sikkerhedscirkulæret - alternativt tage kontakt til den, der har skabt informationen med henblik på at afdække om en evt. omklassificering er mulig.

Personer, der skal håndtere klassificeret information efter sikkerhedscirkulæret skal være sikkerhedsgodkendte og have godkendt adgang til "REGNEM" eller "TIL TJENESTEBRUG"- platformen, afhængigt af klassifikationsgraden af det materiale, der skal behandles.

Du kan finde sikkerhedscirkulæret på retsinformation.dk.

4.3. 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 og it-løsninger

Du skal sørge for at låse din skærm, hver gang du forlader din plads, så andre ikke kan få adgang. Du kan låse din skærm ved at trykke: "Windowsknap + L" eller "ctrl + alt + delete".

Programmel, der kan hentes fra Statens It's Software Center, er forhåndsgodkendt til installation på departementets PC'er. Det er ikke tilladt at installere øvrige programmer.

Du må også kun bruge de kommunikationstjenester, der stilles til rådighed af Statens It. Du må således ikke benytte andre online værktøjer til deling eller opbevaring af departementets informationer omfattet af pkt. 4.1.2 til 4.1.4,

Kontakt departementets Intern 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.

Når du holder online møder, skal du sikre dig, at uvedkommende ikke deltager i mødet.

6. Anvendelse af kunstig intelligens (AI)

Du må gerne benytte AI-værktøjer, hvis du overholder departementets retningslinjer for anvendelse af AI. Du kan læse om departementets retningslinjer i "Vejledning til medarbejdere om retningslinjer for brug af generativ kunstig intelligens" som du kan finde her.

7. Passwords

Retningslinjer for passwords varierer for de enkelte systemer, du skal dog altid søge at vælge et password på mindst 15 tegn med en kombination af store og små bogstaver, tal og specialtegn.

Vurderer Statens It, at det valgte password er for svagt, selvom det opfylder de generelle krav til passwords, vil du modtage en mail, hvori Statens It beder dig ændre dit password til et stærkere.

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 servicedesk.

Du kan hente statens passwordadministrationsværktøj "KeePass" i Statens-It Software Center, der kan hjælpe dig med at holde styr på dine passwords.

8. Lokal- og fællesdrev

SIA-PC'en har et lokalt drev (C-drevet), der kan slettes uden varsel i forbindelse med systemopdateringer 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.

Kontordrevet (navnet afhænger af kontoret eller enheden) er et fællesdrev, hvor alle medarbejdere i kontoret/enheden og potentielt alle medarbejdere i departementet har adgang til drevet og foldere.

Personligt-drev (H-drevet) 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. En saglig grund kan f.eks. være, hvis der er mistanke om, at der ligger virusinficeret materiale på et personligt drev.

Dokumenter med personoplysninger, der er sagsdannende, kan i en afgrænset periode gemmes på enten kontordrev eller personligt drev, inden de overføres til journaliseringssystemet.

Dokumenter med personoplysninger, der ikke er sagsdannende, skal slettes, når der ikke længere er et sagligt grundlag for at opbevare dem.

Dokumenter med fortrolige, herunder følsomme personoplysninger skal dog enten slettes eller – hvis de er sagsdannende - overføres til journaliseringssystemet og samtidig slettes fra drevet snarest muligt og senest inden for en måned.

Hvis du har et arbejdsmæssigt behov for at lagre filer (f.eks. Excel-ark), som indeholder fortrolige, herunder følsomme personoplysninger på kontordrevet eller personligt drev i længere tid end en måned, skal data krypteres og lagres under iagttagelse af databeskyttelsesretlige regler, herunder dataminimeringsprincippet og princippet om opbevaringsbegrænsning. Det betyder i praksis, at du f.eks. kan anvende 7-zip til krypteringen, samt at kodeordet skal opbevares forsvarligt, f.eks. i password manageren KeePass. Begge programmer findes i Software Centeret og er godkendt af departementet til dette formål.

Dokumenter med fortrolige, herunder følsomme personoplysninger skal, indtil de enten slettes eller journaliseres, opbevares enten på dit personlige drev eller på et kontordrev, som er underlagt adgangsbegrænsning, således at kun de medarbejdere, der har et sagligt, arbejdsmæssigt behov herfor, har adgang til dokumenterne. Adgangsbegrænsningen for drevene styres af Statens It via bestillinger fra departementets IT.

Kontorchefen skal løbende sikre, at kontorerne løbende foretager en gennemgang af lokal- og fællesdrevene med henblik på at rydde op i lagrede data. ISDB-enheden påminder en gang årligt kontorerne herom.

9. Bærbare datamedier

Bærbare medier – bl.a. USB-sticks, harddiske og bærbare PC'er – har en væsentlig risiko for at blive tabt, stjålet, glemt eller kompromitteret. Beskyt derfor filer på USB-stik mv. med kryptering – f.eks. Bitlocker, der er indbygget som standard i Windows - og hold kodeordet hemmeligt. Din SIA-PC fra Statens It er allerede krypteret.

Du må kun benytte USB-stick mv., der er udleveret af departementet til dit it-udstyr. Du må ikke tilslutte "fremmede" USB-sticks til dit it-udstyr eller tilslutte dit USB-stick til en "fremmed" pc. Det betyder f.eks., at oplægsholdere skal sende deres præsentationer på mail.

Alle medier, som ikke længere skal anvendes, skal afleveres til departementets Interne IT med henblik på sikker nulstilling eller destruktion. Det gælder også i forbindelse med fratrædelse.

Hvis du mister et bærbart medie, der indeholder arbejdsrelaterede oplysninger, refereres der til afsnit 15 – Indberetning af sikkerhedshændelser.

10. 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 pc'en ned, så systemopdateringerne gennemføres.

11. Internet

Du skal udvise forsigtighed i forhold til, hvilke websites der besøges, og hvilke informationer du oplyser.

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.

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.

Der må kun sendes e-post, som indeholder følsomme eller fortrolige personoplysninger eller fortrolige informationer gennem usikre netværk, hvis der benyttes kryptering.

En vejledning i at sende e-post sikkert med brug af kryptering ligger 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, behøver ikke blive krypteret, idet informationsudveksling på interne netværk er vurderet som sikkert. Vær opmærksom på, at det ikke gælder for digital kommunikation med Lægemiddelstyrelsen, da de ikke er kunder hos Statens It.

E-mails, som indeholder følsomme eller fortrolige personoplysninger eller fortrolige informationer i øvrigt, og som er sagsdannende, skal journaliseres i departementets sagsbehandlersystem snarest muligt efter modtagelsen eller afsendelsen. Når e-mailen er journaliseret, skal den slettes fra e-mailsystemet snarest muligt og senest efter en måned.

E-mails, der indeholder følsomme eller fortrolige personoplysninger eller fortrolige informationer i øvrigt, som ikke er sagsdannende, og dermed ikke er omfattet af journaliseringspligten (som f.eks. interne e-mails vedrørende overvejelser om en sag), bør derimod slettes løbende, når det ikke længere er nødvendigt at opbevare dem og senest efter en måned.

Ovenstående gælder både for modtagne og afsendte e-mails.

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. Anvendelse af it-systemer uden for arbejdspladsen, herunder hjemmearbejdspladser m.v.

Departementet stiller hjemmearbejdspladser til rådighed for medarbejderne. Disse løsninger og anvendelsen heraf er også omfattet af alle dele af retningslinjerne for informationssikkerhed.

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 kaldet VIA. Adgangene styres med to-faktor autentifikation – koder modtaget via apps– og udstyret til understøttelse af disse elementer af løsningerne er personlige og må ikke videregives eller udlånes.

Der gælder særlige retningslinjer, som du skal overholde, når du arbejder hjemme eller på rejser. Du bedes læse om, hvordan du skal forholde dig i "Retningslinjer for brug af departementets it-udstyr på farten og på rejser", som du kan finde her.

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. Der må på intet tidspunkt opbevares arbejdsrelaterede følsomme eller fortrolige personoplysninger eller fortrolige informationer i øvrigt på private pc'er.

Der gøres desuden opmærksom på, at der som led i den generelle systemovervågning, jf. pkt.17, også ved hjemmearbejde foretages registrering af den enkeltes log on, log off og tidsforbrug mv.

13.1. Anvendelse og genudlån af ministeriets pc'er

For pc'er og andet udstyr, som ejes af Statens It og lejes 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.

Bærbare pc'er må ikke efterlades uden opsyn 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, herunder regler om sletning af SMS-beskeder m.v.

14.1. Anvendelse af mobile enheder udleveret af departementet

Departementet udleverer mobile enheder (mobiltelefoner og i visse tilfælde iPads) til medarbejderne, som på forhånd er registreret hos Statens It og installeret med Statens It's mobile it-arbejdsplads (MIA), som giver sikker adgang til bl.a. mails og F2.

Departementet kan uden varsel låse og slette alle data på enheden, hvis den f.eks. tabes, stjæles eller bortkommer, eller sikkerhedskopiere telefonens indhold, hvis den f.eks. skal indgå i en kommissionsundersøgelse.

Medarbejderen skal sørge for, at enheden altid er sikkerhedsopdateret til seneste version.

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.

Medarbejdere i departement må som udgangspunkt kun sende arbejdsrelaterede SMS-beskeder mv. på udstyr, der er udleveret af departementet.

Nogle beskedtjenester har redigerings- og slettefunktioner, der betyder, at afsenderen kan redigere og slette i beskeder, som slår igennem på modtagerens telefon, og den oprindelige besked derved slettes eller ændres på både afsenderens og modtagerens telefon. Der må ikke anvendes sådanne redigerings- og slettefunktioner.

SMS-beskeder og beskeder på andre beskedtjenester må ikke slettes på mobile enheder udleveret af departementet, medmindre:

- beskederne er private
- beskederne er modtaget ved en åbenlys fejl
- der er tale om beskeder, der udelukkende har et personalerelateret indhold, eksempelvis en SMS-besked om, at man holder fri, beskeder til og fra en tillidsrepræsentant (i kraft af dennes funktion) eller beskeder mellem medarbejder og chef om rent personlige forhold, f.eks. en sygemelding
- beskeden er journaliseret (men kun fra det tidspunkt, hvor beskeden er journaliseret).

Arbejdsrelaterede SMS-beskeder og beskeder på andre beskedtjenester opbevares i øvrigt af departementet i overensstemmelse med Justitsministeriets retningslinjer herom.

14.2. Private enheders adgang til data

En privat mobil enhed (telefon eller iPad) må ikke anvendes til at tilgå departementet systemer, herunder e-mails og F2.

14.3. Tjenesterejser og private rejser med udstyr, der synkroniserer med F2 og mail

Hvis du skal på tjenesterejse uden for EU/EØS eller NATO, skal du kontakte ISDB på isdb@sum.dk i god tid og senest 3 uger forud for en rejse, så ISDB 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. Du kan læse mere i "Retningslinjer for brug af departementets it-udstyr på farten og på rejser", som du kan finde her.

15. Indberetning af sikkerhedshændelser

Hvis en medarbejder har mistanke om eller kan konstatere trusler mod eller brud på informationssikkerheden[2], skal dette straks rapporteres til Statens It ved at oprette en fejlmelding i Serviceportalen hos Statens It.

Så snart du har modtaget kvitteringsmailen fra Statens It ("Emne: Vi har registreret din sag…"), skal du videresende den til ISDB-enheden på ISDB@sum.dk.

Ved den videre behandling af hændelsen inddrages andre relevante parter – f.eks. Intern IT, departementets DPO og andre – afhængigt af hændelsestypen.

Vær opmærksom på, at der kan være særlige procedurer for indberetning af hændelser på fagsystemer. Du vil i givet fald blive informeret herom af nærmeste leder.

Der henvises endvidere til proceduren for "Indberetning af sikkerhedshændelser", der kan findes på Intranettet. Her kan du også finde hjælp til at indberette en hændelse.

[2] **Sikkerhedsbrud, fejl eller sårbarheder inkluderer bl.a.:**
-Mistet it-udstyr, f.eks. bærbar computer, mobiltelefon, IPad, usb-nøgle og lignende
-Fysiske dokumenter med fortrolige oplysninger, der har ligget tilgængelige for uvedkommende
-Virus og anden malware på din computer
-Indtastning eller upload af personoplysninger eller andre sensitive oplysninger i en generativ AI-tjeneste (ChatGPT, Bard eller lign.)
-Utilsigtet deling eller sletning af oplysninger
-Afsendelse af mail/brev til forkert modtager eller med oplysninger om en forkert person
-Tildeling af forkerte adgangsrettigheder, således at medarbejdere får indblik i oplysninger, som de ikke skulle have haft

16. Sikkerhedskopiering

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

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.

Departementet kan få adgang til din e-post, hvis det er nødvendigt for, at arbejdsgiveren kan forfølge berettiget interesser, og hensynet til den ansatte ikke overstiger disse interesser. Det kan f.eks. være af hensyn til drift, sikkerhed, genetablering og dokumentation samt hensynet til kontrol af medarbejderes brug.

Derudover kan din nærmeste chef eller formanden for Cyber-, Informationssikkerhed- og Databeskyttelsesudvalget 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 ikke af andre.

Af hensyn til departementets drifts- og informationssikkerhed foretages løbende sikkerhedskopiering af logfilerne. 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, CPR og Navision, gælder specifikke sikkerhedsinstrukser og vejledninger. Brugerne vil blive bekendtgjort med disse i forbindelse med oprettelse som bruger af systemet.

19. Versioner

Version	Godkendt af	Gyldig fra dato	Status	Bemærkninger/ændringer
1.0	CID-udvalget den 23. maj 2024	1. juli 2024	Endelig	Behandlet på chefmøde den 12. juni 2024 og på Samarbejdsudvalgsmøde den 25. juni 2024
1.1	CID-udvalget 16. september 2025			Opdateret i forbindelse med årlig gennemgang, herunder konsekvensrettet som følge af "Retningslinjer for brug af departementets it-udstyr på farten og på rejser"
1.2	CID-udvalget 11. december 2025	1. januar 2026	Endelig	Opdateret ifm. ændring i krypteringskrav ifm. mailkorrespondance med Lægemiddelstyrelsen.

Indenrigs- og Sundhedsministeriet
Slotsholmsgade 10-12
1216 København K

www.ism.dk