Region Hovedstaden

Generelle retningslinjer for informationssikkerhed og databeskyttelse

Informationssikkerhed og databeskyttelse i Region Hovedstaden

I Region Hovedstaden løser vi samfundskritiske opgaver indenfor blandt andet hospitalsdrift, psykiatri samt handicap- og socialområdet. Alle områder, hvor borgerne er i centrum. Vi driver desuden vigtig forskning, der har betydning for samfundet generelt.

Når vi løfter opgaverne, gør vi det i større og større udstrækning gennem digitale løsninger. Forskningsdata og informationer om borgerne, deres helbred og behandling håndteres elektronisk, og hovedparten af det medicotekniske udstyr er afhængig af it og netværk. Digitaliseringen giver os en række uvurderlige muligheder i forhold til forskning og mødet med borgerne. Men med de digitale løsninger følger også trusler - blandt andet fra cyberangreb.

Region Hovedstaden gør brug af en række digitale og fysiske tiltag for at beskytte informationer og personoplysninger. Men informationssikkerhed og databeskyttelse er noget alle medarbejdere i regionen skal bidrage til. Ved at holde dig opdateret omkring regionens regler og retningslinjer, løfter du din del af ansvaret og er med til at beskytte borgerne, regionen og vores arbejdsplads.

Indholdsfortegnelse

Cybersikkerhed

Din adfærd på internettet kan sammenlignes med din adfærd i trafikken. Selv om vi har tekniske og fysiske foranstaltninger i form af lysreguleringer og fartbump, sker der stadig ulykker. Det samme er tilfældet med internettet. Region Hovedstaden har indført en række tekniske tiltag, der skal gøre det sikkert for dig at bruge internettet i forbindelse med dit arbejde. Men ligesom i trafikken, er de tekniske tiltag ikke altid nok. Det er derfor vigtigt, at du som medarbejder er opmærksom, klikker med omtanke og bruger din sunde og kritiske fornuft, når du er online.

ADGANG TIL INTERNETTET

De internetforbindelser, der stilles til rådighed af Region Hovedstaden, kan frit benyttes til arbejdsmæssige formål. Det er også tilladt at benytte forbindelsen til private formål. Der er dog nogle få ting, som du ikke må.

Du må fx ikke...

- Besøge hjemmesider, der indeholder ulovligt materiale.
- Downloade eller distribuere copyright beskyttet musik, film eller andet materiale uden tilladelse fra copyright indehaver.

Dine aktiviteter på internettet registreres af regionen. Det sker med henblik på fejlrettelser, ved mistanke om misbrug og opklaring af cyberangreb.

CYBERANGREB

Cyberangreb er blevet hverdag – også i Region Hovedstaden. De fleste udnytter sårbarheder i vores systemer og applikationer. Langt de fleste af denne type angreb afværges og håndteres af regionen gennem tekniske tiltag. Men mange cyberangreb går ikke efter tekniske sårbarheder. De forsøger i stedet at manipulere regionens medarbejdere til at overføre penge, afgive adgangskoder og andre fortrolige oplysninger. Men det kan også være et forsøg på at narre dig til at klikke på links, der installerer skadelig software, som inficerer din pc og regionens netværk. Der findes flere typer angreb, som målrettet forsøger at udnytte den menneskelige faktor.

PHISHING

Ved phishing udsendes en stor mængde enslydende mails til en bred personkreds. Formålet er at lokke fortrolige eller følsomme oplysninger ud af modtagerne eller manipulere dem til at åbne vedhæftede filer eller klikke på indlejrede links i de fremsendte mails.

De kriminelle gør de fremsendte mails troværdige med officielle navne og logoer på virksomheder og myndigheder, som er kendt i det offentlige rum. Ofte hævder afsenderen, at der er behov for akut handling. Simpelthen for at stresse modtageren til at handle hurtigt og uden om de formelle arbejdsgange.

Phishing sker typisk via e-mail, men kan også være igennem websider. Du kan stave en web-adresse forkert og ende på et phishing-site. Sitet ligner det rigtige site, men indeholder skadelige links eller formularer, der lokker oplysninger fra dig eller skader de systemer og udstyr du bruger. Husk, at også kendte hjemmesider, som du normalt har tillid til, kan blive inficeret med falske links.

SPEAR-PHISING

Et spear-Phishing angreb er målrettet enkeltpersoner i en organisation. Ligesom med phishing angreb er formålet at lokke fortrolige eller følsomme oplysninger ud af modtageren eller manipulere dem til at åbne vedhæftede filer eller klikke på indlejrede links i de fremsendte mails.

Et spear-phishing angreb adskiller sig ved, at den kriminelle på forhånd har indhentet en del viden om ofret – fx på sociale medier eller på virksomhedens egen hjemmeside. På den måde kan den kriminelle udforme sin mail, så den virker mere troværdig og tillidsvækkende.

Oplysningerne vil så – sammen med en mulig infektion af modtagerens computer, tablet eller mobiltelefon – kunne anvendes i forbindelse med et decideret cyberangreb mod organisationen.

CEO FRAUD

CEO Fraud minder om Spear-phishing. Det kaldes CEO Fraud når svindlerne udgiver sig for at være en ledende person i en organisation, og enten på mail eller telefon beder en medarbejder om at overføre penge eller fortrolige oplysninger.

Ligesom med spear-phishing har den kriminelle på forhånd indhentet en del viden på fx sociale medier eller på virksomhedens egen hjemmeside, så denne mere overbevisende kan udgive sig for at være en ledende medarbejder i organisationen.

UNDGÅ PHISHING OG CEO FRAUD

- Forhold dig skeptisk til e-mails og websteder, der beder om personlige oplysninger. Ingen offentlige myndigheder, banker eller lignende vil bede om personlige oplysninger pr. mail.
- Ring eller skriv til afsenderen, hvis du er i tvivl om ægtheden af en mail eller webside. Men brug ikke svarfunktion eller telefonnummeret i den mail du har modtaget.
- Undgå at klikke på links i e-mails. Indtast i stedet selv web-adressen i en browser.
- Kontroller afsenderadressen i mailen. Står der fx ”navn.navn@region-h.dk” i stedet for ”navn.navn@regionh.dk”
- Man kan konstruere en mail, hvor den synlige afsender er forskellig fra den virkelige afsender. Kontroller derfor de skjulte oplysninger. I Outlook kan det gøres ved at flytte markøren over afsenderen, hvorved adressen på afsenderen vises.
- Vær opmærksom på falske links. Links i mailen kan pege på andre afsendere end dem, der er vist. I Outlook kan afsenderen fx kontrolleres ved at føre markøren over de enkelte links. Herved vises den bagvedliggende afsenderadresse.

Har du modtaget en mistænkelig mail eller har mistanke til en hjemmeside, skal du kontakte Center for IT, Medico og Telefoni via CIMT serviceportal eller ringe til Servicedesk på **38 64 80 80**

Det juridiske – Databeskyttelse

HVAD ER DATABESKYTTELSE?

Alle har ret til beskyttelse af sine personoplysninger. Og alle, der behandler personoplysninger om andre i "ikke-privat" sammenhæng, er forpligtet til at sikre disse rettigheder og til at beskytte personoplysningerne. Rettigheder og forpligtelser går samlet under betegnelsen **"databeskyttelse".**

Behandling af andres personoplysninger, skal ske i overensstemmelse med reglerne på databeskyttelsesområdet. Region Hovedstaden har indarbejdet de databeskyttelsesretlige krav i regionens politikker og retningslinjer, hvor det er relevant. Det er derfor vigtigt, at du kender og følger dem.

CENTRALE BEGREBER

Der knytter sig nogle centrale begreber til databeskyttelse. Kender du dem, bliver det lettere at forstå dit ansvar og opgaver.

Personoplysninger
Personoplysninger er enhver form for information, der kan henføres til en bestemt person. Det gælder også når personen kun kan identificeres, hvis oplysningen kombineres med andre oplysninger. Personoplysninger inddeles i almindelige, følsomme og strafferetlige oplysninger.

Almindelige personoplysninger
Navn, adresse, oplysninger om økonomi, skat, gæld eller oplysninger om sygedage, tjenstlige forhold, familie, ansættelsesforhold og lignende.

Følsomme personoplysninger
Race, etnisk oprindelse, politisk overbevisning, religiøs overbevisning, fagforeningsmæssige tilhørsforhold, helbredsoplysninger, seksuelle forhold eller orientering samt biometriske og genetiske data.

Cpr-numre og oplysninger om strafbare forhold er to kategorier af personoplysninger, som har særstatus i dansk lovgivning. I Region Hovedstaden behandles disse på lige fod med følsomme oplysninger.

Den registrerede
Personen, hvis oplysninger bliver behandlet, enten elektronisk eller fysisk.

Dataansvarlig
Den virksomhed, myndighed eller anden organisation, der behandler den registreredes oplysninger. Den dataansvarlige definerer, hvorfor, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.

Databehandler
Databehandleren er den virksomhed, myndighed eller anden organisation, der behandler personoplysninger på den dataansvarliges vegne. Fx leverandører eller samarbejdspartnere til regionen.

Behandling af personoplysninger
Behandling af personoplysninger dækker over en hver håndtering af personoplysninger. Det kan være indsamling, registrering, organisering, opslag, opbevaring, ændring, sletning eller videregivelse af informationer.

Når du arbejder med personoplysninger

Langt de fleste af os indsamler og behandler personoplysninger i det daglige. Det kan være som sundhedsperson i forbindelse med patientbehandling, som forsker ved et projekt eller som HR medarbejder i forbindelse med et ansættelsesforløb. Vi låner oplysningerne og såvel kolleger som borgere skal have tillid til, at vi passer godt på dem. Det gør vi ved at følge regionens interne retningslinjer og bruge vores sunde fornuft.

HVORDAN MÅ DU BRUGE PERSONOPLYSNINGER

Når du behandler personoplysninger, skal du være opmærksom på, at loven skelner mellem

- almindelige personoplysninger
  og
- følsomme personoplysninger

I praksis betyder det, at du skal være opmærksom på, hvilken af de to typer oplysninger du har med at gøre, da der knytter sig forskellige regler for håndtering, opbevaring og deling af oplysninger i de to kategorier.

INDSAMLING OG BEHANDLING AF PERSONOPLYSNINGER

Når du indsamler personoplysninger, skal det være proportionelt med det formål oplysningerne indsamles til. Vi indsamler derfor kun oplysninger, der er nødvendige for at kunne varetage den opgave oplysningerne er indhentet til.

BEHANDLING AF PERSONOPLYSNINGER I FAGSYSTEMER

Fælles for regionens fagsystemer er, at de tager højde for de lovkrav og regler, der gør sig gældende for informationssikkerhed og databeskyttelse.

Du skal derfor altid bestræbe dig på at håndtere personoplysninger i de relevante fagsystemer.

Når du indsamler og behandler personoplysninger i regionens fagsystemer, skal du være særligt opmærksom på, at du...

- kun må lave opslag i regionens systemer, hvis det er nødvendigt for at du kan løse dine arbejdsopgaver i regionen.

- ikke må lave opslag på familie og venner af nysgerrighed eller privat interesse.

- ikke må lave opslag på dig selv i fx Sundhedsplatformen. Brug i stedet de muligheder du har som privat borger. Det kan være "Min Sundhedsplatform" eller sundhed.dk.

For at opfylde regionens juridiske forpligtelser i forhold til databeskyttelse, bliver alle opslag og aktiviteter i regionens systemer registeret og logget.

Nogle registreringer gennemgås automatisk, mens andre udtages ved stikprøver eller hvis der opstår mistanke om bevidst overtrædelse af regionens regler og retningslinjer.

På intranettet kan du læse mere om reglerne for opslag i fx Sundhedsplatformen.

BEHANDLING AF PERSONOPLYSNINGER UDENFOR FAGSYSTEMERNE

Når du opbevarer filer med personoplysninger udenfor fagsystemerne, øges risikoen for, at regionen ikke kan imødekomme de persondataretlige regler. Af samme årsag er der eksplicitte regler for, hvor og hvor længe du må opbevare personoplysninger uden for fagsystemerne.

Uagtet hvilken type personoplysninger du arbejder med, gælder at du ikke må opbevare dem lokalt på din pc, tablet eller anden device.

DIGITALE PLATFORME

Du skal altid bestræbe dig på, ikke at håndtere personoplysninger uden for regionens fagsystemer. Hvis behovet alligevel opstår, skal du anvende en af regionens digitale platforme eller regionens drevstruktur.

Der er i Region Hovedstaden to primære digitale platforme, der understøtter medarbejdernes håndtering af filer med personoplysninger udenfor fagsystemerne. De to platforme er:

- Workzone

Administrativt system, der benyttes til journalisering og længerevarende opbevaring af fx filer med personoplysninger.

- REDCap

Overvejende for medarbejdere, der arbejder med forskningsdata.

NETVÆRKSDREV

Du kan opbevare personoplysninger i mapper på

- V-drevet
- P-drevet
- R-drevet
- H-drevet

Her må du opbevare personoplysningerne i op til 30 dage. Husk at tage stilling til adgangsbegrænsningen på det drev og den mappe, filerne placeres i. Bestil eventuelt en særskilt lukket mappe, hvis du har behov for det.

Efter 30 dage skal oplysningerne flyttes til et relevant og af regionen godkendt fagsystem eller til en af de to digitale platforme - Workzone eller REDCap.

Har du undtagelsesvis behov for at opbevare personoplysninger uden for et godkendt fagsystem eller en digital platform længere end 30 dage, skal de flyttes til en lukket mappe på L-drevet. Oprettelse af lukkede mapper på L-drevet, skal ske efter aftale og godkendelse af din personaleansvarlige leder.

Arbejder du med forskningsdata skal du være opmærksom på, at forskningsdata, der indeholder personoplysninger skal opbevares i lukkede mapper på L-drevet. Personoplysningerne skal pseudonymiseres og omsætningsnøglen skal opbevares i en lukket mappe på enten V-, P- eller R-drevet.

Lukkede mapper skal bestilles på CIMT Serviceportal.

OFFICE 365 ONLINE

De fleste medarbejdere i Region Hovedstaden har mulighed for at benytte Office 365 online. Det giver mulighed for at opbevare data i Cloudløsningen OneDrive. Du skal dog være opmærksom på, at du ikke må benytte OneDrive til opbevaring af personoplysninger.

PERSONOPLYSNINGER I OUTLOOK

Outlook adskiller sig fra de øvrige opbevaringsmuligheder, idet der her skelnes mellem almindelige og følsomme personoplysninger.

MAILS MED FØLSOMME PERSONOPLYSNINGER

Når du har modtaget e-mails med følsomme personoplysninger, kan du gemme dem i din mailboks i op til 30 dage. Herefter skal de slettes eller overføres til et af regionens fagsystemer, en digital platform eller en lukket mappe på L-drevet.

MAILS MED ALMINDELIGE PERSONOPLYSNINGER

Du må gerne gemme mails i Outlook, der indeholder almindelige personoplysninger i form af fx navne på medarbejdere, der nævnes i kraft af deres faglige rolle i en sag eller projekt.

VIDERESENDELSE AF MAILS

Vær altid ekstra opmærksom, når du videresender mails, der indeholder personoplysninger. Husk at fjerne vedhæftninger, der ikke er relevante og orienter dig grundigt i mailtråden, så personoplysninger, der ikke er relevante for din modtager, bliver fjernet inden du videresender.

Du må aldrig sætte din arbejdsmail til, automatisk at videresende mails til en privat mailadresse.

SLETNING OG BERIGTIGELSE

Personoplysninger på medarbejdere og borgere skal altid være ajourførte og korrekte. Særligt når det handler om personoplysninger i forbindelse med patientbehandling og forskning.

Som medarbejder i en offentlig myndighed har du pligt til at dokumentere behandlingen af sager, hvor der indgår oplysninger om borgerne. Det kan have betydning for den videre sagsbehandling, at oplysningerne ikke har været korrekte. Du må derfor ikke slette personoplysninger, der indgår i en sagsbehandling. Hvis der i sagen optræder forkerte oplysninger om borgeren, skal du berigtige oplysningerne. Det vil sige notere, at oplysningerne er forkerte og henvise til de rigtige oplysninger.

Hvis du behandler patientoplysninger, skal du være særligt opmærksom på din journalføring. Heller ikke her må du slette oplysninger, men i stedet berigtige og henvise til de rigtige oplysninger.

DELING INTERNT I REGION HOVEDSTADEN

Du må gerne dele indsamlede personoplysninger med dine kolleger, hvis de har et arbejdsbetinget formål med at modtage og anvende oplysningerne. Deling af personoplysninger forudsætter altså, at det er nødvendigt for, at du og dine kolleger kan varetage jeres opgaver.

Deling af personoplysninger skal ske med de værktøjer Region Hovedstaden har godkendt og stiller til rådighed. Du må fx gerne sende personoplysninger pr. mail, såfremt de sendes fra en Region Hovedstaden mailadresse til en tilsvarende Region Hovedstaden mailadresse. Her er forbindelsen krypteret og du vil kunne sende på helt normalt vis. Du skal dog være opmærksom på reglerne for opbevaring af personoplysninger i Outlook.

Deling af personoplysninger kan også ske via mapper på netværksdrevene.

DELING MED MODTAGERE UDEN FOR REGION HOVEDSTADEN

Du må aldrig benytte uautoriserede fildelingstjenester og internet services som Dropbox til filer med personoplysninger.

Hvis du har behov for at sende følsomme og/eller fortrolige personoplysninger til eksterne modtagere – det vil sige modtagere, der ikke har en mailadresse, som ender på regionh.dk - skal du bruge en sikker kommunikationsform. Det betyder, at sender du personoplysninger til en borger, virksomhed eller anden offentlig myndighed, skal du sende via "Send Digitalt" funktionen i mail-systemet Outlook.

Som alternativ til "Send Digitalt" funktionen i Outlook, kan du benytte en af nedenstående løsninger. Det kan være ved deling af store filer, der indeholder billeder, video og lyd.

- SFTP serverløsning
- Tunnelkryptering

Herud over har du mulighed for at benytte eksterne tjenester som Filkassen.dk eller deic.dk

Har du brug for en af ovenstående muligheder, skal du eller din leder tage kontakt til CIMT Servicedesk for at få afdækket den rigtige løsning. Du skal have en ledelsesgodkendelse, hvis løsningen påfører regionen ekstra omkostninger.

VIDEOKONFERENCER OG TELEFONI

Når du deltager i møder, der foregår over enten video eller telefon, skal brugen af personoplysninger begrænses til det allermest nødvendige. Du må kun udveksle personoplysninger, hvis det er arbejdsmæssigt relevant for alle parter på mødet.

Brug altid de løsninger regionen har godkendt og stiller til rådighed.

PRÆSENTATIONER

Undgå så vidt muligt at dele materiale med personoplysninger til møder, seminarer eller konferencer. Hvis du har behov for at vise materiale, der indeholder personoplysninger – fx Pdf-filer, skærmdumps eller udtræk fra it-systemer, og ikke har mulighed for at slette personoplysningerne, skal de i stedet anonymiseres – fx ved simpel overstregning. Du kan også benytte dig af klippeværktøjet SnagIT, der kan hentes i Softwareshoppen.

PERSONOPLYSNINGER I FYSISK FORM

Personoplysninger optræder også i fysisk form. Det kan være i form af print, biologisk materiale, blanketter eller etiketter til pilleglas og doseringsæsker.

Også her skal du begrænse uvedkommendes adgang til oplysningerne. Vær opmærksom på, hvor det fysiske materiale opbevares og overvej, hvordan du kan begrænse uvedkommendes adgang, når du ikke har det under opsyn.

Når du printer skal du være opmærksom på, om printet indeholder personoplysninger. Hvis det er tilfældet, skal du hente printet hurtigst muligt og altid med det samme, hvis du har printet til en printer, der står placeret, hvor uvedkommende har adgang.

Adgangskoder

KRAV TIL ADGANGSKODER

Adgang til regionens netværk og systemer kræver en personlig adgangskode. Din adgangskode skal være nem at huske for dig, men svær at gætte for andre. Din adgangskode skal

- Bestå af mindst 8 karakterer
- Indeholde både store og små bogstaver
- Indeholde mindst ét tal (0 til 9)

Adgangskoden skal skiftes hver tredje måned. Men hvis du har mistanke om, at andre har fået kendskab til din kode, skal du skifte den med det samme. Du må ikke skrive adgangskoden ned - hverken på din telefon, tablet, papir eller lignende ligesom du heller ikke må tage billeder af den. Din adgangskode er personlig og må ikke deles med andre.

De adgangskoder du anvender i forbindelse med dit arbejde i Region Hovedstaden, må ikke anvendes til private formål som fx sociale medier, netbank eller andet.

Har du svært ved at huske dine adgangskoder, kan du hente Password Manageren "Keepass" i Software shoppen.

DIGITAL SIGNATUR

Nogle medarbejdere kan have behov for at anvende digital medarbejdersignatur (NemID) i forbindelse med deres funktion og opgaver for Region Hovedstaden. Hvis du benytter digital medarbejdersignatur, skal du beskytte den på samme måde, som du skal beskytte dine personlige adgangskoder. Du må ikke bruge din medarbejdersignatur til private formål, ligesom du ikke må bruge din private signatur i forbindelse med dit arbejde.

KODEFRASER ER BEDRE END KODEORD

En lang kode er god kode. Derfor vil en hel kodefrase være bedre end blot et kodeord.
En kodefrase er en frase af umiddelbart tilfældige ord, tal og tegn. Følge 3 simple regler:

- Frasen skal være lang.
- Bland tal, store og små bogstaver i kodefrasen.
- Brug hellere personlige og unikke minder end kendte citater og fraser.

Eksempel: cirKusmedbornene17
(Refererer til en tur i cirkus med børnene i 2017)

cirKusmedbornene17

Applikationer og systemer

Du har i forbindelse med dit arbejde adgang til en række forskellige applikationer og systemer. Nogle er almindelige og bruges til administrative opgaver, mens fx klinikere og forskere kan have brug for mere specialiseret software. Fælles for dem alle er, at der er regler for, hvilke applikationer og systemer du må anvende, hvordan og til hvad.

Region Hovedstaden er dataansvarlig. Det betyder grundlæggende, at regionen ejer alle de data, du anvender, producerer og gemmer på drevene og i regionens systemer – inklusiv dine mails m.m. i Outlook. Privat korrespondance er dog undtaget, hvorfor den type korrespondance bør markeres som private mails.

Region Hovedstaden har pligt til at følge op på om regionens it anvendes i overensstemmelse med reglerne for informationssikkerhed og databeskyttelse.

Det betyder, at din anvendelse af netværk, applikationer, systemer, drev og data registreres.

Registreringerne kan anvendes ved fejl eller hvis der opstår mistanke om bevidst overtrædelse af reglerne for informationssikkerhed og databeskyttelse.

HVAD MÅ DU BRUGE

Du må kun anvende applikationer og systemer, der er godkendt til brug i Region Hovedstaden. De mest almindelige får du adgang til, når du tiltræder din stilling. Det samme gør sig gældende for de applikationer og systemer, som din nærmeste leder har vurderet nødvendige for, at du kan udføre dine opgaver.

Generelt er adgangen til Regionens applikationer og systemer betinget af, at du har et arbejdsbetinget behov. Det er din nærmeste leder, der vurderer behovet og godkender adgangen. Har du brug for flere applikationer og systemer, finder du dem i Softwareshoppen.

Du må ikke fjerne de applikationer og systemer, der styrer sikkerheden på din pc. Det gælder fx antivirusapplikationer, adgangskontrol m.m.

OPDATERING

De fleste cyberangreb udnytter kendte sårbarheder i styresystemer og gængse applikationer på din pc og devices. Det er derfor vigtigt, at din pc, smartphone, tablet og lignende holdes opdateret.

Hovedparten af det udstyr du får udleveret af Region Hovedstaden, opdateres automatisk. Det er dog ikke alle applikationer og systemer, der understøtter automatisk opdatering.

Der kan være situationer, hvor du har fået mulighed for selv at installere software på dit udstyr – fx hvis du er systemadministrator. I de tilfælde er det vigtigt, at du undersøger om du selv skal opdatere eller om det sker automatisk.

ADGANG TIL MAILBOKSE OG DREV

Region Hovedstaden kan skaffe sig adgang til alle regionens mailbokse og drev. Det kan være nødvendigt af driftsmæssige hensyn eller ved et tvingende behov for at skaffe sig adgang til en mail, der er blevet sendt til en fraværende medarbejder.

Hvis regionen er nødt til at skaffe sig adgang, sker det altid efter aftale med den pågældende medarbejder selv. Hvis dette ikke er muligt, sker det efter aftale, med vedkommendes nærmeste leder, hvorefter medarbejderen orienteres hurtigst muligt.

I tilfælde af, at en medarbejder rejser eller bliver afskediget, har Region Hovedstaden ret til at tilgå den pågældende medarbejders mailboks. Det sker med henblik på at få adgang til korrespondance, der er relevant for Region Hovedstadens virke.

Når en medarbejder fratræder, lukkes vedkommendes brugerkonto. Det betyder også at data i mailsystemer slettes efter 6 måneder.

PC og andet udstyr

I Region Hovedstaden er vi som så mange andre steder, afhængige af forskelligt it-udstyr. Det kan være pc'er, tablets eller smartphones. Fælles for udstyret er, at der knytter sig nogle regler til brugen og den fysiske håndtering af det.

Pc, tablet, smartphone og andre devices stillet til rådighed af regionen er personlige. Det betyder i praksis, at andre – inklusiv din familie – ikke må anvende udstyret. Det skyldes, at der kan ligge personoplysninger og fortroligt materiale på udstyret, ligesom uvedkommende ikke må få adgang til regionens netværk.

Det er dig, der har ansvaret for, hvordan dit udstyr anvendes. Lås derfor altid din pc, når du forlader den. Det gøres let ved at trykke på "Windows "-tasten og "L" på samme tid. Dette gælder også selvom det kun er for en kort periode. Hvis andre får adgang til din pc, når du har forladt den, risikerer du at blive holdt ansvarlig for patientopslag eller andre handlinger, der er foretaget på den, mens du var væk.

Hvis du og dine kolleger anvender en dele-pc, skal du være opmærksom på, at du har ansvaret for de handlinger, der foretages med dit login. Det er derfor vigtigt, at du enten logger af pc'en eller låser den når du forlader den.

PRIVAT BRUG

Du må anvende din arbejds-pc til privat brug i moderat omfang og med omtanke. Du må eksempelvis gerne bruge udstyret til at tilgå internettet, så længe det sker i overensstemmelse med reglerne for internetadgang.

Du må også gerne gemme private data på din arbejds-pc og regionens drev. Du skal dog være opmærksom på, at regionen har grænser for, hvor meget og hvilken type materiale du må gemme. Det betyder, at du kan blive bedt om at fjerne private filer fra regionens drev. Gemmer du private data på din arbejds-pc og regionens drev, skal du placere det i en mappe mærket "Privat".

INDKØB

IT-udstyr som pc'er, tablets, telefoner, printere og lignende skal altid købes gennem serviceshoppen i CIMT. Det samme gør sig gældende for klinisk udstyr i form af PDA'er og scannere til medicinrum. Medicoteknisk udstyr købes gennem Medusa.

ELEKTRONISKE OVERSIGTSSKÆRME

I Region Hovedstaden anvender vi ofte forskellige typer af oversigtsskærme. Det kan være for at give flere medarbejdere visuelt overblik over data.

Der er ofte personoplysninger på oversigtsskærmene. Det betyder i praksis, at du skal være opmærksom på reglerne for håndtering af personoplysninger.

Personoplysningerne må kun være tilgængelige for medarbejdere, der har et arbejdsbetinget behov for at kunne tilgå dem. Af samme årsag skal oversigtsskærme og lignende så vidt muligt placeres så uvedkommende ikke kan læse med på skærmene – fx gennem en døråbning eller rude.

MOBILE DEVICES

Mobile devices som fx tablets og smartphones, fungerer som adgang til Region Hovedstadens netværk, ligesom de kan indeholde personoplysninger og fortrolige informationer. Af samme årsag, skal din telefon og tablet altid være udstyret med Mobile Iron til beskyttelse af både device og regionens informationer.

Du kan finde vejledning til opsætning af Mobile Iron på regionens intranet.

Du må gerne gemme private og personlige informationer på smartphones og tablets udleveret af Region Hovedstaden. Men det kan være en god idé at holde privatliv og arbejdsliv adskilt, da regionen af sikkerhedsmæssige årsager kan blive nødt til at slette data fra din telefon eller anden device. Det kan hvis den bortkommer eller hvis der er mistanke om, at personoplysninger eller fortrolige informationer er kommet i de forkerte hænder. Du skal altså være parat til at miste dine private fotos og informationer.

Du må også gerne installere egne applikationer på regionens mobile devices, men regionen har tilladelse til at fjerne uønskede og skadelige applikationer.

Husk, at dine devices er personlige og ikke må benyttes af andre personer, som fx familiemedlemmer og venner.

Lagermedier som USB Sticks og eksterne harddiske skal altid være krypteret med stærk kryptering, når de bliver anvendt til opbevaring af fortrolige data eller følsomme personoplysninger. Du kan selv kryptere eksterne lagermedier. Skriv Bitlocker i søgefeltet nederst på din skærm og følg anvisningerne.

Informationssikkerhed på farten

Når du er på farten og medbringer pc, tablet, smartphone eller andre mobile devices, kan du bekvemt tilgå regionens data og arbejde hvorfra du vil. Men med det privilegie følger også en øget risiko. Uagtet om du arbejder hjemmefra, på café, i toget eller ved en konference i udlandet, er der øget risiko for, at dit udstyr bliver væk, stjålet eller hacket. Konsekvensen kan være, at uvedkommende får adgang til regionens netværk, personoplysninger og fortrolige informationer.

SHOULDER SURFING

Når du bruger din pc, tablet eller smartphone et offentligt sted, er der altid risiko for, at nogen kigger dig over skulderen. Når du bruger dine kreditkort og taster pinkoden, sikrer du dig, at ingen aflurer koden. På samme måde skal du være opmærksom på, hvem der kigger med, når du indtaster brugernavn, pin- og adgangskoder på dit udstyr. Hvis du arbejder med personoplysninger eller fortrolige informationer, skal du være ekstra opmærksom på, at uvedkommende ikke læser med over skulderen.

OFFENTLIGT NETVÆRK

Uanset om du befinder dig i ind- eller udland, vil der de fleste steder være mulighed for at komme på nettet via offentlige netværk på caféer, hoteller, lufthavne og lignende. Men der er en bagside.

De trådløse netværk er ofte usikre og giver andre mulighed for at opsnappe de informationer du sender over nettet. De trådløse netværk du kan fremsøge via din pc, tablet og smartphone, kan virke harmløse. Men de kan være sat op af cyberkriminelle, med henblik på at overvåge og opnå adgang til alt datatrafik fra de personer, der logger på.

Hvis du tilgår regionens netværk og systemer via et offentligt netværk, skal det ske via en sikker vpn-forbindelse. Benytter du dig af en pc udleveret af Region Hovedstaden logger du automatisk på med Global Protect, der giver sikker adgang.

Hvis du vil tilgå regionens data med en smartphone eller tablet skal du have installeret regionens sikkerhedsløsning Mobile Iron på din device. Det gælder både devices udleveret af Region Hovedstaden og i de tilfælde, hvor du vil benytte dig af egne devices.

Mobile Iron giver dig en sikker forbindelse til regionens data og ændrer sikkerhedsindstillingerne på din device, så de er i overensstemmelse med regionens retningslinjer og gældende lovgivning.

NÅR DU REJSER

Hvis du skal have din pc eller andet udstyr med til udlandet, skal det medbringes som håndbagage, og udstyret må ikke efterlades uden opsyn, medmindre det er låst inde i et forsvarligt sikret skab eller rum.

Flere lufthavne, hoteller og caféer stiller USB-ladestik til rådighed. Men du kan ikke være sikker på, at tilslutningen ikke er kompromitteret og at du kun får strøm gennem kablet. Hvis ladestikket er kompromitteret, kan du også få malware i form af virus eller anden skadelige software, der kan opsnappe brugernavne, adgangskoder, pinkoder eller andre fortrolige og personlige oplysninger.

Undgå derfor så vidt muligt USB-ladestik og benyt dig i stedet af et almindeligt ladekabel, der modsat USB kablet, ikke kan overføre data.

Fysisk sikkerhed

ADGANGSKORT OG PINKODER

Adgang til Region Hovedstadens bygninger er ofte styret ved hjælp af elektronisk adgangskontrol. Det samme kan være tilfældet på fx hospitaler, der ellers fremstår åbne for offentligheden. Her kan det være særlige områder i bygningen, der er adgangskontrolleret.

Hvis du har et arbejdsbetinget behov for adgang til en adgangsbegrænset bygning eller område, får du udleveret adgangskort og pinkode. Adgangskortet skal altid bæres synligt.

Der gælder de samme regler for adgangskort og pinkoder som for adgangskoder i øvrigt.

Det betyder at kode og kort er personligt og ikke må udleveres til andre. Hvis du mister dit adgangskort, skal du hurtigst muligt tage kontakt til kortudsteder med henblik på at få det lukket.

Når du har gæster i huset, skal du altid følge de lokale adgangsregler.

NÅR UDSTYR SKAL BORTSKAFFES

Fysisk materiale skal bortskaffes på en måde, der også yder beskyttelse af fx personoplysninger når udstyret ikke længere skal anvendes. Det kan være ved makulering af dokumenter, brug af aflåste affaldsspande, beholdere og containere.

IT-udstyr og devices, du ikke længere skal bruge, skal afleveres til CIMT. Det gælder også det udstyr, der skal repareres eller kasseres. Du må ikke tage kasseret udstyr med hjem.

Kontakt CIMT Servicedesk, hvis du skal af med defekt eller gammelt it-udstyr, devices og lignende.

CIMT Servicedesk sørger for, at gamle data slettes og ikke kan genskabes, ligesom de sørger for, at udstyret kasseres med respekt for miljøet.

Sociale medier

Internettet og de sociale medier er gode kanaler når du vil kommunikere hurtigt og bredt. Men informationssikkerhed og særligt de databeskyttelsesretlige regler har indflydelse på hvad du må dele og ikke må dele.

Informationer, der tilhører Region Hovedstaden må kun deles på sociale medier, hvis de oprindeligt er tiltænkt offentligheden.

Vær forsigtig med at blande arbejdsliv og privatliv på de sociale medier. Fagligt materiale som du får adgang til i kraft af dit arbejde, kan være omfattet af din tavshedspligt, ligesom du skal være opmærksom på licensrettigheder og ophavsret tilknyttet materialet.

Personoplysninger må aldrig deles på de sociale medier - heller ikke selv om du har fået samtykke.

Du må ikke oprette facebooksider på vegne af regionen uden forudgående godkendelse hos Center for Kommunikation. Det gælder også for facebooksider, som optræder i en form og med et indhold, der kan tolkes som sider oprettet af regionen.

Du må ikke kommunikere med patienter på de sociale medier. Brug i stedet et relevant fagsystem – fx Sundhedsplatformen

TAVSHEDSPLIGT

Du har naturligvis ytringsfrihed, men du må ikke udtale dig på vegne af din arbejdsgiver og det må ikke fremstå som om at du gør, medmindre, at du er bemyndiget til det.

Som offentligt ansat har du desuden tavshedspligt om fortrolige oplysninger, som du får kendskab til gennem dit arbejde. Hvis du er i tvivl om, hvorvidt en oplysning er fortrolig, kan du drøfte det med din nærmeste leder.

Din tavshedspligt gælder også efter, at din ansættelse hos Region Hovedstaden ophører.

Håndtering af hændelser

Du kan i forbindelse med dit arbejde for Region hovedstaden, opleve hændelser, der har betydning for regionens informationssikkerhed og databeskyttelse. Det kan være hændelser eller egentlige brud på persondatasikkerheden. Når det sker, er det vigtigt, at du reagerer. Dels for at forhindre, at en hændelse udvikler sig, dels for at begrænse muligheden for, at en lignende hændelse opstår igen. Kontakt altid din nærmeste leder, hvis du er i tvivl om, hvad du skal gøre i en konkret situation.

SIKKERHEDSHÆNDELSE

Når du opdager en sikkerhedshændelse, skal du hurtigst muligt tage kontakt til

CIMT Servicedesk på
telefon **38 64 80 80** eller
gennem CIMT Serviceportal.

Det kan være når

- Du modtager en mail med krav om betaling uden for regionens normale betalingsprocesser (CEO-Fraud)
- Du modtager mails, der forsøger at få dig til at opgive adgangskoder, betalingsoplysninger eller lignende (Phishing mails)
- Personer uretmæssigt får fat i adgangskoder og udstyr
- Du har formodning om, at dit udstyr er inficeret med virus eller lignende.

BRUD PÅ PERSONDATASIKKERHEDEN

Der er tale om et brud på persondatasikkerheden, hvis en eller flere borgeres personoplysninger er blevet tilgængelige for uvedkommende.

Der er dog først tale om et brud på persondatasikkerheden, når bruddet er bekræftet. Det vil sige, at en mistanke som udgangspunkt ikke i sig selv er et brud på persondatasikkerheden. Du skal dog reagere på din mistanke ved at undersøge sagen nærmere. Kan du bekræfte, at uvedkommende har haft adgang til personoplysninger, skal du indmelde det.

Hvis du opdager et brud på persondatasikkerheden, skal du reagere hurtigt. Du skal med det samme indmelde bruddet til CIMT. Det er også en god idé at orientere din nærmeste leder. Indebærer bruddet en risiko for de personer oplysningerne handler om, har regionen pligt til at anmelde bruddet til Datatilsynet inden for 72 timer.

Du indmelder bruddet gennem CIMT Serviceportal. Her klikker du på "Meld fejl", og finder skabelonen til indberetning af brud på persondatasikkerheden under kategorien "Andet".

Du må aldrig selv anmelde brud på persondatasikkerheden til Datatilsynet. Når du har indmeldt bruddet til Serviceportalen, vil CIMT håndtere sagen og foretage en konkret vurdering i forhold til underretning af Datatilsynet og de berørte personer.

HVIS DU MISTER DIT UDSTYR

Hvis du mister din Pc, tablet, telefon eller lignende udstyr, skal du hurtigst muligt kontakte

CIMT SERVICEDESK
38 64 80 80

Her oplyser du, hvilket udstyr du har mistet. CIMT Servicedesk vil så fortælle, hvordan du skal forholde dig i den konkrete situation og hjælpe med spærring af adgangsrettigheder m.m.