Region Hovedstaden

REGION

BESKYT VORES INFORMATIONER

Pssst...
Informationssikkerhed
fra hoved til hale

KÆRE MEDARBEJDER OG LEDER

Adgang til informationer i it-systemer og elektronisk kommunikation er for de fleste medarbejdere i Region Hovedstaden en selvfølgelig del af arbejdsdagen.

Hvis vi ikke har adgang til informationerne, vil mange opgaver ikke kunne løses eller blive meget vanskeligere at udføre. I nogle tilfælde kan det oven i købet true liv og helbred, hvis man f.eks. ikke kan få adgang til de rigtige oplysninger om en patient.

Derfor er det vigtigt, at alle ved, hvordan man i det daglige arbejde sikrer informationer, samt hvordan man beskytter sig mod virus, hackerangreb og andre sikkerhedstrusler mod vores it-systemer.

Som offentlig myndighed har vi desuden ansvaret for, at de personfølsomme og fortrolige oplysninger, vi opbevarer om borgere, virksomheder og andre samarbejdspartnere, bliver behandlet på en sådan måde, at de kan have tillid til, at kun de personer, der har brug for at se deres oplysninger, får adgang til dem.

I folderen finder du nogle enkle spilleregler, som fortæller dig, hvordan du kan bidrage til en sikker informationsanvendelse i regionen.

Hjalte Aaberg
Regionsdirektør

DAGLIG BRUG

Al dataanvendelse i Region Hovedstaden logges. Det betyder, at man kan spore, hvem der har set eller arbejdet med bestemte data. Loggen anvendes ikke til at kontrollere medarbejdernes brug af internet og e-mail, med mindre der er mistanke om kriminelle forhold, overtrædelse af sikkerhedsbestemmelserne eller i forbindelse med systemproblemer og fejlretning.

Computer er her i folderen betegnelse for alle typer af computere, samt mobilt udstyr som bl.a.: bærbare computere, tablets og mobiltelefoner.

PAUSESKÆRM

Du skal

- aktivere pauseskærmen , (⊞+L), så den er låst med password /pinkode, når du forlader din computer selv for en kortere periode.

Du må ikke

- deaktivere en pauseskærm med password /pinkode, som CIMT har installeret.

PASSWORD

Du skal

- have et personligt password med minimum otte tegn, bestående af store og små bogstaver og tal.
- udtænke et password, som er nemt at huske for dig, men ikke kan gættes af andre.
- skifte dit password, hvis du har mistanke om, at det er blevet kendt af andre.

Du må ikke

- anvende oplysninger, som vedrører dig selv, til dit password (f.eks. familiens navne, fødselsdatoer, bilnummer o.l.).
- bruge det samme password til systemer uden for regionen, f.eks. til din private mail eller på internettet.
- skrive dit password ned.
- videregive dit password til andre.

BRUG AF DREV

Du skal

- lagre dine arbejdsdokumenter og andre data på regionens fælles servere, hvor der er backup og andre sikkerhedsforanstaltninger. Persondata må kun gemmes i systemer, der er beregnet til det.

Persondata er alle informationer, der kan føres tilbage til en bestemt person via f.eks. person-nummer, ID-nr., navn, adresse, stemme eller et billede.

Du må

- opbevare persondata i tekstbehandlingssystem eller e-mailsystem i op til 30 dage uden særlige sikkerhedsforanstaltninger, hvis det indgår som led i behandlingen af en sag.

Du må ikke

- som fast arbejdsgang lagre arbejdsdata på dit C-drev, USB, nøgler e.l., hvor de kan blive slettet uforvarende eller måske komme til uvedkommendes kendskab. Lagring på dit C-drev, USB-nøgler e.l. skal være så kortvarig som mulig.

Arbejdsdata er informationer, der anvendes i en arbejdsmæssig sammenhæng og er relevante for opgaveløsningen på arbejdspladsen.

COMPUTERE, NETVÆRK OG PROGRAMMER

VIRUS

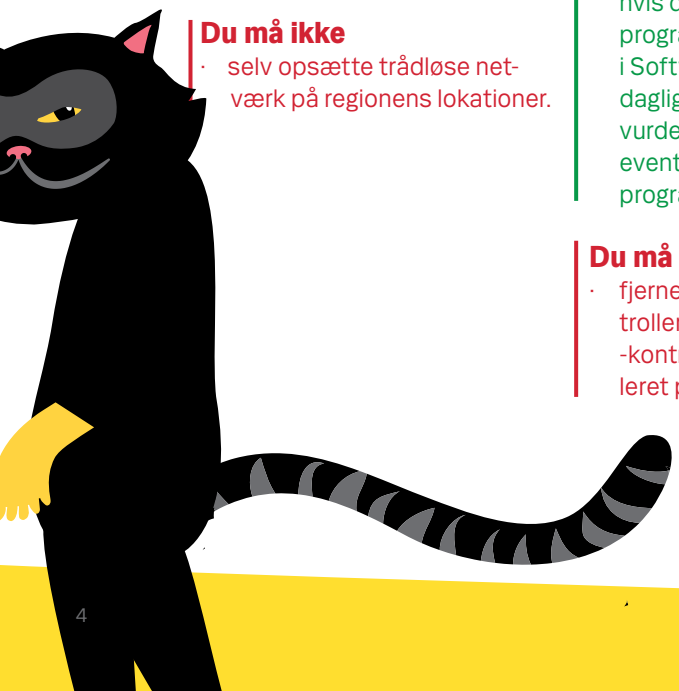
Du skal

- kontakte CIMT Service Desk, hvis du har mistanke om, at din computer har virus eller opfører sig mærkeligt.
- kontakte CIMT Service Desk, hvis du har mistanke om, at antivirusprogrammet ikke virker korrekt.

TRÅDLØSE NET

Du må ikke

- selv opsætte trådløse netværk på regionens lokationer.



PROGRAMMER

Du skal

- sikre, at licensforholdene er i orden for de programmer, der ikke er leveret af Region Hovedstaden.

Du må

- kun anvende programmer, som er godkendt til brug i Region Hovedstaden, og som kan hentes via Softwareshoppen. Kontakt CIMT Service Desk, hvis du har brug for et program, som ikke findes i Softwareshoppen. Din daglige leder og CIMT skal vurdere og godkende, en eventuel anvendelse af programmet.

Du må ikke

- fjerne de sikkerhedskontroller (antivirus, adgangs-kontrol o.l.), som er installeret på computeren.

BÆRBARE COMPUTERE OG FLYTBARE MEDIER

Du skal

- medbringe din computer, flytbare medier og andet mobilt udstyr som håndbagage, når du har udstyret med på rejse.

Du må ikke

- efterlade bærbare computere og andre flytbare medier, medmindre de er forsvarligt sikret i et aflåst skab eller rum.

Begrebet flytbare medier er her i folderen fællesbetegnelsen for bl.a. USB-enheder, der kan lagre data, eksterne harddiske, DVD og CD-rom.

Se endvidere retningslinjer for anvendelse af mobilt udstyr i folderen: "Sikker brug af mobilt udstyr – dit ansvar!" på intranettet under Informationssikkerhed.

E-MAIL

Du skal

- benytte sikker og krypteret e-mail, når du sender fortrolige eller følsomme personoplysninger til modtagere uden for Region Hovedstaden.

- sikre dig at modtagerne af fortrolige eller følsomme personoplysninger kan modtage dem sikkert og krypteret.

- behandle e-mails fra ukendte afsendere og/eller med ukendt eller manglende emne med varsomhed. De kan indeholde virus.

Du må

- sende og modtage e-mails med fortrolige og følsomme persondata internt i Region Hovedstaden, via regionh.dk-mailadresser.

- sende og modtage e-mails med fortrolige og følsomme persondata via "Send Digitalt" knap-løsningen i Outlook til/fra eksterne modtagere.

Du må ikke

- benytte din private mailkonto til at sende og/eller modtage regionens fortrolige og følsomme data.

- sætte en fast videresendelse af mails op fra din regionh.dk-mailadresse til en privat mailkonto.

- åbne vedhæftede filer/klikke på links i e-mails fra ukendte eller mistænkelige afsendere.

"Send Digitalt" og "sikker e-mail" er krypterede og signerede e-mails, som sendes med et virksomhedscertifikat. Hvis du har brug for at anvende en sikker e-mail, kan du kontakte CIMT Service Desk. Send Digitalt knap-løsningen installeres via Softwareshoppen.

Husk, at e-mails og sikker e-mails med fortrolige og følsomme persondata skal slettes fra postkassen inden 30 dage.

INTERNET

Du skal

- være varsom med at opgive e-mailadresser på internettet. De kan blive brugt til spam.
- anvende internettet med omtanke og uden at være til gene for eller virke stødende på dine kolleger eller andre.

Du må

- bruge internettet i privat øjemed med måde.
- kun downloade programmer og opdateringer fra internettet, som er godkendt. Kontakt CIMT Service Desk, hvis du har brug for et program.

Du må ikke

- downloade, opbevare eller surfe på sider, som indeholder ulovligt materiale.
- ulovligt downloade og distribuere materiale med copyright på.

BEHANDLING AF PERSONDATA

Du skal

- være omhyggelig med at sikre, at uvedkommende ikke får adgang til personfølsomme eller fortrolige data.

Du må

- udveksle fortrolige oplysninger eller personoplysninger internt med dine kolleger, hvis det er nødvendigt og lovligt i forhold til de arbejdsopgaver, du udfører.

Du må ikke

- skaffe dig oplysninger om personer, hvis du ikke skal bruge det i dit arbejde, herunder oplysninger om familie og venner.
- tage sager eller dokumenter, der indeholder fortrolige eller personfølsomme oplysninger med hjem, med mindre det er godkendt af din leder, og dokumenterne opbevares forsvarligt.
- opbevare eller behandle fortrolige eller personfølsomme data på din private computer.
- benytte services på internettet til at opbevare og arbejde med fortrolige og personfølsomme data.
- indsamle, registrere eller opbevare oplysninger, der kan henføres til en faktisk person, medmindre der foreligger en godkendt anmeldelse af databehandling.

DIGITAL SIGNATUR

Du skal

- beskytte din digitale medarbejdersignatur på samme måde som dit password.
- kontakte CIMT Service Desk, hvis du har mistanke om, at din signatur bliver misbrugt.

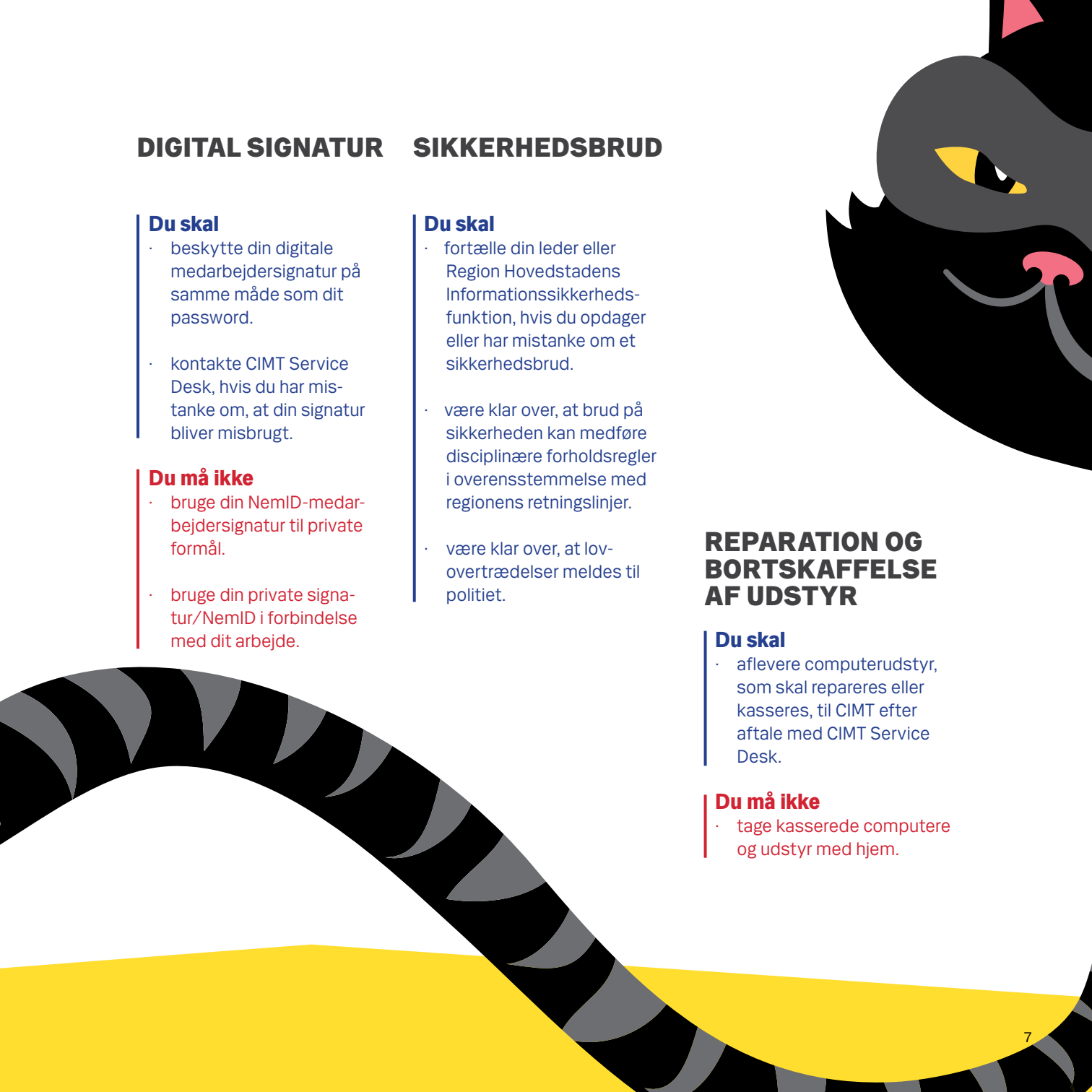
Du må ikke

- bruge din NemID-medarbejdersignatur til private formål.
- bruge din private signatur/NemID i forbindelse med dit arbejde.

SIKKERHEDSBRUD

Du skal

- fortælle din leder eller Region Hovedstadens Informationssikkerheds-funktion, hvis du opdager eller har mistanke om et sikkerhedsbrud.
- være klar over, at brud på sikkerheden kan medføre disciplinære forholdsregler i overensstemmelse med regionens retningslinjer.
- være klar over, at lovovertrædelser meldes til politiet.



REPARATION OG BORTSKAFFELSE AF UDSTYR

Du skal

- aflevere computerudstyr, som skal repareres eller kasseres, til CIMT efter aftale med CIMT Service Desk.

Du må ikke

- tage kasserede computere og udstyr med hjem.

Alle brugere af regionens informationer skal følge rammen for informationssikkerhed og de vejledninger og instrukser, som regionen har fastsat.

Medarbejdere må kun anvende informationer, som regionen har ansvaret for, i overensstemmelse med de arbejdsopgaver, de udfører. Informationerne skal beskyttes i overensstemmelse med deres følsomhed og væsentlighed.

LÆS MERE PÅ INTRANETTET UNDER:
It\informationssikkerhed

Bevidstheden om sikker anvendelse af regionens informationer gælder også alle andre brugere som forskere, konsulenter, regionsrådsmedlemmer, elever, studerende og andre, der får adgang til regionens informationer.

Fra Region Hovedstadens
Ramme for informationssikkerhed

CIMT - Informationssikkerhedsteamet

Telefon.: 38649090
E-mail: informationssikkerhed@regionh.dk

Center for It, Medico og Telefoni

Region Hovedstaden
Borgervænget 7
2100 København Ø

REGION Region Hovedstaden