

Beskyt vores informationer

Daglig brug

Computere, netværk og programmer

E-mail

Internet

Behandling af persondata

Digital signatur

Reparation og bortskaffelse af udstyr

Sikkerhedsbrud

Kære medarbejder og leder

Adgang til informationer i it-systemer og elektronisk kommunikation er for de fleste medarbejdere i Region Hovedstaden blevet 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 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.

Det er den lokale ledelse, som har ansvaret for at spillereglerne drøftes på arbejdspladsen, og at de overholdes.

Hvis der er arbejdssituationer, hvor det ikke er muligt at overholde reglerne, så er det ledelsens ansvar at sørge for at bringe forholdene i orden eller at søge dispensation.

Venlig hilsen

Helle Ulrichsen
Regionsdirektør

Daglig brug

Password

- Du skal**
- have et personligt password med mindst 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 det bliver kendt af andre (f.eks. supportmedarbejdere, der har hjulpet dig).
- Du må ikke**
- anvende oplysninger, som vedrører dig selv, til dit password (f.eks. familiens navne, fødselsdatoer, bilnummer o.l.).
 - bruge dine passwords til systemer uden for regionen, f.eks. til din private post eller på internettet.
 - skrive dit password ned.
 - videregive dit password til andre.

Pauseskærm

- Du skal**
- aktivere pauseskærmen, når du forlader din arbejdsplads, selv for en kortere periode, hvis ikke andet er aftalt med din ledelse.
- Du må ikke**
- deaktivere en pauseskærm med password, som it-afdelingen har installeret.

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 fx personnummer, navn, adresse eller et billede.

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

Du må ikke ● lagre arbejdsdata permanent på dit C-drev, USB-nøgler e.l., hvor de kan blive slettet uforvarende eller måske komme til uvedkommendes kendskab.

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

Virus

Du skal ● kontakte din supportfunktion, hvis din computer har virus eller opfører sig mærkeligt.

Ordet supportfunktion er her i folderen fællesbetegnelsen for Help Desk, Service Desk og Brugerservicecenter (BSC).

- kontakte din supportfunktion, hvis du har mistanke om, at antivirusprogrammet ikke virker korrekt.
- virusscane disketter, cd-rom eller USB-nøgler, inden du åbner filerne. Du kan evt. kontakte supportfunktionen, hvis du har brug for hjælp.

Computere, netværk og programmer

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. Kontakt supportfunktionen, hvis du har brug for et program. Din daglige leder skal godkende, at du bruger programmet.

- Du må ikke** ● fjerne de sikkerhedskontroller (antivirus, adgangskontrol o.l.), som er installeret på computeren.

Trådløse net

- Du må** ● kun anvende din computer på trådløse net uden for regionen, hvis computeren er installeret og godkendt af en it-afdeling i regionen.

- Du må ikke** ● Selv opsætte trådløse netværk på regionens lokationer.

Bærbare computere

- Du skal** ● medbringe din computer og andet udstyr som håndbagage, når du har udstyret med på rejse.

- Du må ikke** ● efterlade bærbare computere, medmindre de er forsvarligt sikret i et aflåst skab eller rum.

E-mail

- Du skal** ● benytte sikker e-mail, når du sender fortrolige eller følsomme personoplysninger til modtagere uden for Region Hovedstaden.
- behandle e-mails fra ukendte afsendere og/eller med ukendt eller manglende emne med varsomhed. De kan indeholde virus.

- Du må** ● sende fortrolige og personfølsomme e-mails internt i Region Hovedstaden, men husk, at de skal slettes fra postkassen inden 30 dage.

Sikker e-mail er krypteret og signeret e-mail, som sendes med et virksomhedscertifikat. Hvis du har brug for at anvende sikker e-mail, kan du kontakte supportfunktionen.

Internet

- Du skal**
- være varsom med at opgive e-mail-adresser 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 supportfunktionen, 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.

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

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.

- tage sager eller dokumenter, der indeholder fortrolige eller personfølsomme oplysninger med hjem, medmindre det er godkendt af din leder, og dokumenterne opbevares forsvarligt.
- opbevare eller behandle fortrolige eller personfølsomme data på din private computer.

Digital signatur

- Du skal**
- beskytte din digitale medarbejdersignatur på samme måde som password.
 - kontakte din supportfunktion, hvis du har mistanke om, at din signatur bliver misbrugt.
- Du må ikke**
- bruge din medarbejdersignatur til private formål.
 - bruge din private signatur i forbindelse med dit arbejde.

Reparation og bortskaffelse af udstyr

- Du skal**
- aflevere computerudstyr, som skal repareres eller kasseres, til din supportfunktion.
- Du må ikke**
- tage kasseret udstyr med hjem.

Sikkerhedsbrud

- Du skal**
- fortælle din sikkerhedsansvarlige leder, hvis du opdager eller har mistanke om et sikkerhedsbrud.
 - være klar over, at brud på sikkerheden kan medføre disciplinære forholdsregler i overensstemmelse med regionens personalepolitik.
 - være klar over, at lovovertrædelser meldes til politiet.



**Region
Hovedstaden**

For yderligere oplysninger kontakt
Enheden for informationssikkerhed

Pia Jespersen
Tlf.: 45 11 00 29
Mobil: 20 44 20 11

Jørn Knudsen
Tlf.: 45 11 00 30
Mobil: 26 16 38 57

Finn Verner Nielsen
Tlf.: 45 11 00 31

E-mail: informationssikkerhed@regionh.dk

Enheden for informationssikkerhed
Koncern IT
Region Hovedstaden
Borgervænget 7
2100 Kbh Ø