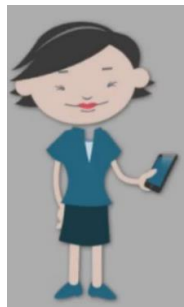




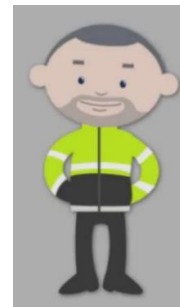
It-sikkerhed og databeskyttelse

Pjece 1



Pas på vores data!

I kommunen oplever vi et stigende antal angreb fra it-kriminelle. EU's Databeskyttelsesforordning stiller skærpede krav til beskyttelse af personoplysninger. Kommunen skal overholde kravene og kommunens it-sikkerhedsregler så borgere, medarbejdere og virksomheder kan være trygge ved, at vi behandler deres oplysninger sikkert, korrekt og efter loven. Derfor er det vigtigt at kende reglerne for it-sikkerhed og databeskyttelse.



ADGANGSKODER

Du må **ikke dele dit brugernavn og din adgangskode** med andre – heller ikke en kollega eller it-supporter. Alle adgangskoder til it-systemer er personlige og strengt fortrolige. *Hvis andre benytter sig af dit brugernavn og din adgangskode, kan du risikere at skulle stå til ansvar for noget, du ikke selv har gjort.*

Logger du ind i **flere it-systemer**, så skal du bruge **forskellige adgangskoder**.

Benyt altid adgangskoder der er svære at gætte for andre.

Skriv ikke dine adgangskoder ned og lad ikke PC'ens browser huske dem – **lær dem udenad**.

Hvis du har mistanke om, at andre har fået kendskab til din adgangskode, skal du straks skifte den.

Ved **mistanke** om, at **adgangskoden** er blevet **misbrugt**, så **ring straks til Koncernservice på tlf. 7080 8000**.

PROGRAMMER OG INTERNET

Alle de systemer og it-værktøjer vi bruger skal være godkendt af Koncern IT – dette for at undgå virus og ondsindet kode, der kan være gemt i systemkoden og for at sikre beskyttelse af de oplysninger vi opbevarer i systemerne.

Installer aldrig programmerne selv, men kontakt Koncernservice, der hjælper med at tjekke om et program er godkendt og med installationen.

Det er muligt at benytte visse godkendte netværkstjenester fx Facebook eller Dropbox, men vær opmærksom på, at du aldrig må udveksle personoplysninger eller kommunens værdioplysninger. Bruger du internettet – så tjek om der er lokale regler og retningslinjer i din forvaltning for, hvad du må bruge nettet til i din arbejdstid. Generelt må du ikke besøge anstødelige eller ulovlige sider på nettet, da

de sammen med spil-sider og konkurrencer udgør en særlig stor risiko for, at du kan blive ramt af virus, phishing og lignende.

HVEM ER ANSVARLIG FOR DATA

Københavns Kommune er ansvarlig for alle de oplysninger der gemmes i it-systemer og på medarbejdernes it-udstyr. Kommunen har ret til frit at anvende disse informationer inden for lovens rammer. Det gælder også alle de e-mail du sender og de oplysninger du gemmer på dit personlige drev.

Du kan markere private e-mail med 'privat' i emnefeltet eller gemme dem i en folder navngivet 'privat'. Private filer kan du gemme i mapper markeret 'privat' lokalt på din PC eller på dit personlige drev. Kommunen vil kun kunne anvende disse privat markerede e-mail og filer under særlige omstændigheder.

LÅS ALTID DIN PC NÅR DU FORLADER DEN

Husk at låse din PC når du forlader den, så din adgang ikke kan benytte af andre og eventuelt misbruges.

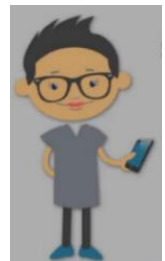
Tryk på  +  for at låse din pc

TAVSHEDSPLIGT

Som medarbejder i Københavns Kommune har du tavshedspligt. De følsomme og fortrolige oplysninger, du får kendskab til gennem dit arbejde, må ikke uberettiget videregives til andre eller komme til uvedkommendes kendskab. Det gælder både under og efter din ansættelse. *Tal fx ikke med din veninde om borgere eller forhold i kommunen.* Konsekvensen ved at overtræde tavshedspligten kan være alvorlig for dig som medarbejder.

MOBILE ENHEDER

Du har et ansvar for at beskytte de oplysninger, der ligger på dine mobile enheder.



- Din mobil eller tablet er personlig og du må ikke dele den med andre.
- Mobilen skal altid sikres med en pinkode til både sim-kortet og til skærmlåsen og koderne skal være forskellige - del dem ikke med andre - skriv dem ikke ned - men lær dem udenad.
- Du skal huske at låse enheden, når du går fra den og hav den altid under opsyn når du er i det offentlige rum. Undgå at andre læser med når du fx tjekker mails i bussen på vej hjem.
- Du skal løbende rydde op på enheden, så der ikke ligger noter, billeder eller filer med fortrolige oplysninger gemt lokalt.

Skal du have adgang til din kalender, læse mails, intranet m.v. på enheden, så er det et krav, at du har installeret kommunens sikkerhedsløsning til mobile enheder.

Sikkerhedsløsningen sikrer bl.a. at Koncern IT kan slette alle data på enheden, hvis den bliver stjålet, så data ikke kan misbruges.

Vær opmærksom på at du aldrig må opbevare personoplysninger eller kommunens værdioplysninger lokalt på enheden – de skal opbevares sikkert i et journalsystem eller fagsystem.

Bliver din mobile enhed stjålet så ring straks til Koncernservice på 70 80 80 00.

PHISHING, RANSOMWARE OG SUSPEKTE HJEMMESIDER

Koncern IT gør alt hvad de kan for at beskytte kommunens it-udstyr mod virus, phishing, ransomware m.v. Men det sker, at noget alligevel slipper igennem. Det er her **din fornuftige adfærd spiller en vigtig rolle.**

Phishing er it-kriminelle der typisk via mail eller sms forsøger at få fat i dine personlige oplysninger fx kontonummer, cpr-nummer eller adgangskode.

Ransomware er en slags virus der krypterer og låser dine og kommunens filer og de it-kriminelle kræver løsepenge for at låse dem op igen.

Typisk udgiver de it-kriminelle sig ofte for at være nogen du kender eller stoler på.

- Lad dig ikke narre af tilbud og konkurrencer eller en umiddelbar troværdig anmodning om at indtaste oplysninger.
- Modtager du en mistænkelig mail eller sms, så slet den – svar ikke på den – åbn aldrig de vedhæftede filer – klik ikke på links.
- Besøg heller ikke suspekte hjemmesider, pas på pop up vinduer og download af filer.

Vær kritisk, opmærksom og brug altid din sunde fornuft.

Hvis du bliver ramt af phishing eller ransomware eller er du i tvivl, så kontakt straks Koncernservice på tlf. nr. 7080 8000.



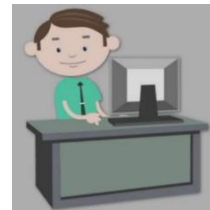
FYSISK SIKKERHED

Fysisk sikkerhed på arbejdspladsen er et vigtigt element, når vi skal beskytte personoplysninger og andre fortrolige data.

Den lokale ledelse har ansvaret for, at din arbejdsplads er sikret på tilstrækkelig vis, så uvedkommende ikke kan få adgang til udstyr eller data, men du spiller også en vigtig rolle.

Hvis der ikke er offentlig adgang på din arbejdsplads, så skal indgangsdøre normalt være låst fx med kode eller lås. *Luk aldrig fremmede med ind på arbejdspladsen, hvis du ikke er overbevist om, at de må være der. Ser du personer på din arbejdsplads, som du ikke kender, er det ok at spørge hvem de er, så det sikres, at de har et lovligt ærinde.*

Arbejder du med person- eller værdioplysninger er der en række ting, du skal være opmærksom på:



- Når du udskriver dokumenter, skal du sørge at benytte en printer der er placeret et sted hvor uvedkommende ikke har adgang eller brug en printer der først udskriver, når du er fysisk til stede.
- Printudskrifter skal også opbevares sikkert, fx i et aflåst skab. Smid dem aldrig i papirkurven. De skal makuleres.

Arbejder du et sted med offentlig adgang, så sørg for at uvedkommende ikke kan se med på din skærm og lad ikke papirer ligge frit fremme så andre kan læse med.

Når du forlader dit kontor, så skal du sikre, at uvedkommende ikke har adgang til udstyr og fortrolige dokumenter. Du kan fx låse kontoret når du går.

Benyt kun USB-stik, som du ved hvor kommer fra. Brug aldrig et USB-stik på din arbejdsplads, som du har fundet på gaden eller på en café (*det kan indeholde virus, ondsindet kode og lignende*).

Få mere viden

Du finder mere information om uddannelse, forvaltningernes kontaktpersoner og supplerende materiale på KKintra:

[Pas på vores data](#)

Med venlig hilsen
Vejledende Sikkerhed
Koncern IT - Økonomiforvaltningen

Pjecen knytter sig til uddannelse / e-læringsforløb om it-sikkerhed og databeskyttelse
Udarbejdet af Koncern IT til Københavns Kommunes medarbejdere maj 2018