Informationssikkerhed

Guide til dig som medarbejder

Herlev Kommune

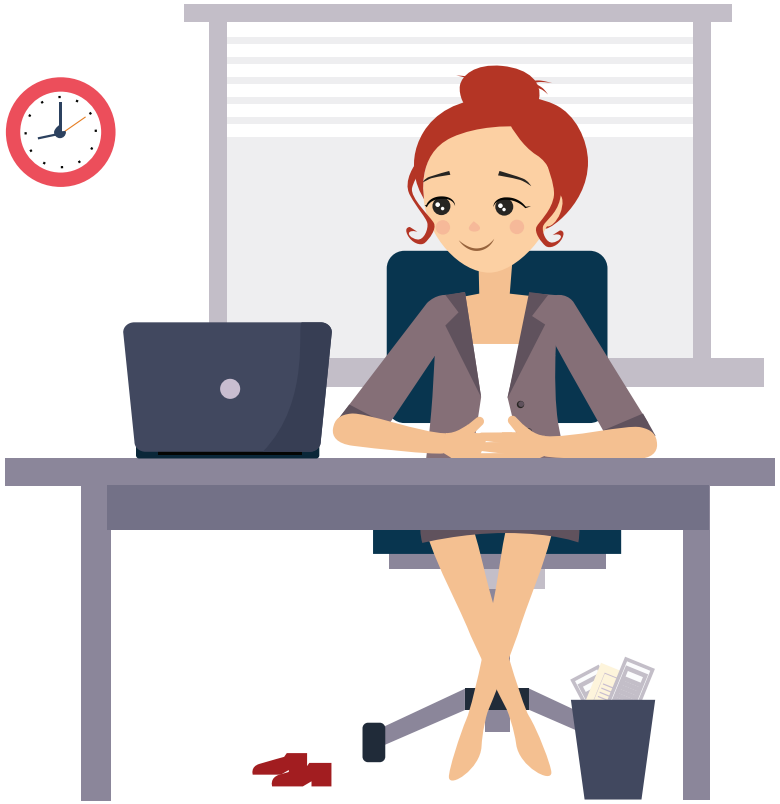
Vi passer på hinandens og borgernes data

marts 2022

Denne folder har til formål at sætte fokus på informationssikkerhed i Herlev Kommune.

Du skal betragte informationssikkerhed som noget grundlæggende, som du altid skal være bevidst om, når du bruger IT eller håndterer information.

Som IT-bruger i Herlev Kommune har du et ansvar for både at beskytte borgernes og organisationens data, så de ikke kommer i forkerte hænder, eller data går tabt.



Informationssikkerhed i hverdagen

Som IT-bruger har du selv ansvaret for din pc. Når du først er logget på, må du ikke overlade din pc til andre – hverken kolleger eller udefrakommende.

DU SKAL:

- Vide at Herlev Kommune logger alle brugerhandlinger, også søgning på internettet. Det gøres primært for at imødegå retslige og sikkerhedsmæssige aspekter. Herlev kommune respekterer din ret til privatliv, og vil nøje opveje dette hensyn med kommunens ret til at beskytte sine informationer.

- Låse din skærm når du forlader din plads, fordi andre ikke skal kunne tilgå din mail og dine sager. Hvis du ikke låser din skærm, har andre mulighed for at sende mails i dit navn eller søge efter oplysninger i fagsystemerne i dit navn.
  Lås derfor altid skærmen når du forlader din plads - for din egen sikkerheds skyld.

- Rydde dit skrivebord for fortrolige/følsomme dokumenter seneste ved arbejdsdagens afslutning.

- Huske, at du har ansvaret for dine gæster. Gæster skal altid følges rundt og følges til udgang.

DU MÅ IKKE:

- Give udtjent IT-udstyr til andre. Udtjent IT-udstyr skal altid afleveres til Team Service som sørger for at slette data og kassere udstyret.

- Ændre på udstyrets sikkerhedsindstillinger, opsætning eller antivirus-beredskab.

Hvis du har mistanke om misbrug eller andre sikkerhedsbrud, skal du kontakte IT og din leder med det samme.

Brugernavn og adgangskode

Brugernavn og kode er personlige og må kun bruges af dig. Adgangskoder skal være svære at gætte for andre og nemme at huske for dig!

DU SKAL:

- Vælge en adgangskode som SKAL være mindst 8 tegn langt og bestå af en blanding af tal, store og små bogstaver (Der må ikke bruges æ, ø eller å).
- Undgå at bruge dit eget navn, initialer og nærmeste families navn, fødselsdag og lignende, da det er for nemt at gætte og dermed hacke.
- Skifte adgangskode, hvis du har mistanke om, at der blevet kendt af andre.

DU MÅ IKKE:

- Skrive din adgangskode ned og videregive adgangskoden til andre.
- Bruge samme adgangskoder på jobbet som derhjemme.

Hvis du har mistanke om, at nogen kender til dine adgangskoder, skal du ændre dem med det samme og dernæst kontakte IT.

E-mail og sikkerhed

Herlev Kommune registrerer din brug af e-mail. Ved mistanke om ulovlig brug af e-mail kan ledelsen i samarbejde med IT åbne og læse e-mails og eventuelle vedhæftede filer.

DU SKAL:

- Journalisere e-mails, der indgår som led i sagsbehandling, og ikke benytte Outlook som arkiv. Det også vigtigt, at dine kollegaer har adgang til alle sags-oplysninger, hvis de skal tage over for dig med kort varsel.
- Slette e-mails med fortrolige og følsomme persondata hurtigst muligt.
- Altid benytte din arbejdsmail, når du skal kommunikere internt.
- Benytte Sikker Mail, når du sender følsomme og fortrolige oplysninger med e-mail
- Behandle mails fra borgere med fornuft.
  Hvis en borger kontakter dig pr. mail er det vigtigt, skal du altid tage stilling til om mailen skal besvares sikkert. Du må kun svare via almindelig mail, hvis mailen kun indeholder almindelige oplysninger. Hvis mailen (både borgerens mail og dit svar) indeholder følsomme eller fortrolige oplysninger, skal du altid sende sikkert.

DU MÅ GERNE:

- Bruge kommunens mailsystem til privat brug i begrænset omfang. Husk at markere dine private e-mails som "privat" i emnefeltet eller gem dem i en folder i Outlook.

DU MÅ IKKE:

- Benytte din private mailkonto i arbejdssammenhæng. Du må ikke modtage/sende kommunes følsomme/fortrolige oplysninger på din private mailkonto.
- Bruge fast videresendelse af e-mail fra din herlev-mailadresse til en anden mailkonto.
- Åbne vedhæftede filer, eller klikke på links i e-mails fra ukendte eller mistænkelige afsendere

Hvis du ved en fejl kommer til at sende følsomt/fortroligt indhold som "usikker" mail, skal du tage kontakt til din leder hurtigst muligt. Hændelsen skal muligvis anmeldes til Datatilsynet.

Brug af internettet

DU SKAL:

- Anvende internettet med omtanke. Al datatrafik kan spores tilbage til Herlev Kommune.
- Være opmærksom når du opgiver din arbejds-emailadresse. Den kan blive brugt til spam.

DU MÅ GERNE:

- Downloade filer i begrænset arbejdsmæssig sammenhæng.
- Bruge internettet til privat brug med måde, og såfremt at det ikke er generende for dine arbejdsopgaver.

DU MÅ IKKE:

- Downloade, opbevare eller surfe på sider, der indeholder ulovligt materiale.
- Videregive adgangskoder og andre fortrolige oplysninger på internettet.
- Streame indhold fra internettet fx lyd/video med mindre det er fagligt relevant.
- Downloade/installere programmer fra internettet. Tal med din leder, hvis du mangler et program.

Hvis du for eksempel kommer ind på en mistænkelig side på internettet, kommer til at installere/afvikle et program eller kommer til at downloade ulovligt indhold, skal du straks tage kontakt til IT. Du skal vide, at det kan få ansættelsesretlige følger at udføre ulovlige handlinger.

Sociale medier og kommunikations- og samarbejdsværktøjer

DU SKAL:

- Være opmærksom på, at arbejdsdokumenter ikke må deles med kolleger eller samarbejdspartnere via ikke-godkendte medier.
- Være opmærksom på, at sociale medier ofte bruges til at skaffe informationer om virksomheder og deres ansatte, så overvej om informationer, som du deler, kan misbruges.

DU MÅ GERNE:

- Benytte sociale medier – fortrinsvis udenfor almindelig arbejdstid eller i pauser.
- Benytte sociale netværk fra kommunens IT systemer med mindre de er specifikt forbudte. Du kan altid spørge IT til råds!
- Connecte med samarbejdspartnere og borgere på sociale medier, forudsat at kommunens sikkerhedsregler i øvrigt overholdes.
- Benytte kommunikations- og samarbejdsværktøjer, som er godkendt af IT.
- Benytte godkendte kommunikations- og samarbejdsværktøjer som Microsoft Teams til dialog med borgere/ samarbejdspartnere, hvis det er dig, som inviterer.

DU MÅ IKKE:

- Dele dokumenter via sociale medier og kommunikationsværktøjer.
- Benytte kommunikations- og samarbejdsværktøjer, som kræver at der foretages en installation på din PC. med mindre det er godkendt af IT.

Behandling af persondata

DU SKAL:

- Opbevare følsomme og/eller fortrolige data i SBSYS eller i et fagsystem
- Udvise forsigtighed, når du fører arbejdsrelaterede samtaler i offentligheden – fx i telefon.
- Altid hente dit print med det samme eller bruge follow-me print.

DU MÅ IKKE:

- Skaffe dig oplysninger om personer, hvis du ikke skal bruge det i dit arbejder, herunder oplysninger om familie og venner.
- Gemme følsomme og fortrolige data lokalt på din pc – hverken din arbejds-PC/telefon eller din private computer.
- Opbevare fortrolige eller følsomme oplysninger på u-krypterede USB-nøgler og tilsvarende bærbare enheder.
- Gemme data længere end det er nødvendigt for at løse din opgave.
- Gemme persondata længere end det er nødvendigt for at løse din opgave, hverken i Outlook eller på et drev. Herefter skal de arkiveres i SBSYS eller relevant fagsystem og derefter slettes fra netværksdrevet/Outlook.
- Gemme følsomme personoplysninger og CPR-numre i Outlook kalenderaftaler. Du må heller ikke skrive borgeres navne i overskriften. Dette gælder også fælleskalendere samt fællespostkasser.

Når du arbejder hjemme

DU SKAL:

- Overholde kommunes sikkerhedsregler – også selv om du er derhjemme – det vil bl.a. sige låse skærm, beskytte papirer og PC og være påpasselig i telefonsamtaler.
- Beskytte papirer og PC under transport til- og fra arbejdspladsen.

DU MÅ IKKE:

- Tage sager eller dokumenter, der indeholder fortrolige eller følsomme personoplysninger med hjem – med mindre det er godkendt af din leder og at dokumenterne opbevares forsvarligt.
- Arbejde med personoplysninger udenfor Citrix med mindre andet er aftalt.
- Lade familiemedlemmer benytte pc´en, når denne er logget på Herlev Kommunes netværk (når VPN eller Citrix-forbindelsen er aktiveret).
- Smide dokumenter med personoplysninger i almindelig dagrenovation. Det skal makuleres på din arbejdsplads.

Hvis du mister dokumenter med personoplysninger/ fortroligt indhold eller dit IT-udstyr/mobil mv., skal du straks tage kontakt til din leder og IT.

Virus

Der er installeret antivirusprogrammer på alle kommunens pc'er.

DU SKAL:

- Kontakte IT, hvis du har mistanke om at din pc har fået virus, eller hvis den opfører sig mærkeligt.

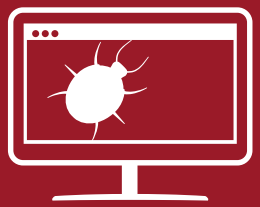
Videresend IKKE virus-advarsler. Lad IT vurdere om det er en reel trussel!

DU MÅ IKKE:

- Åbne vedhæftede filer/klikke på links i e-mails fra ukendte eller mistænkelige afsendere. Pas især på filer med underlige eller lokkende navne. Også hvis e-mailen kommer fra nogen, du kender.

Hvis du får mistanke om, at din pc har fået virus, så hiv netværksstikket ud, så du ikke spreder virus og kontakt IT med det samme!

Hellere kontakt IT en gang for meget end en gang for lidt, hvis dit IT udstyr/dine programmer opfører sig anderledes end normalt.



Sikkerhed på mobile enheder

Som f.eks. bærbar PC, mobiltelefoner og tablets.

DU SKAL:

- Sikre din mobile enhed med en skærmlås, kode og/eller fingeraftryk, så den ikke kan misbruges, hvis den kommer i de forkerte hænder.
- Låse din mobile enhed, når du forlader den.
- Straks kontakte IT, hvis du mister din mobile bærbare PC, tablet eller mobiltelefon.

DU MÅ GERNE.

- Forbinde din mobile enhed til netværk udenfor kommunen, hvis det er sikret med kode.

DU MÅ IKKE:

- Dele din mobile enhed med andre, med mindre det er aftalt med din leder.
- Efterlade din bærbare pc, tablet eller smartphone uden opsyn på offentlige steder.
- Benytte din arbejds-mobil i udlandet, med mindre du har lavet en aftale med din leder.
- Anvende privat mobiltelefon til at downloade eller bruge arbejdsrelaterede apps eller til arbejdsrelateret brug af sms, foto, arbejdsmail og/eller opbevaring af andet arbejdsrelateret materiale på telefonen.

Hvis du mister din arbejds-mobil, din bærbare PC, en tablet eller en USB-nøgle, skal du straks tage kontakt til din leder og IT.

Opbevaring af data

For at efterleve Offentlighedsloven, skal relevante dokumenter, e-mail mm. være journaliseret indenfor 7 dage efter modtagelse.

DU SKAL:

- Journalisere e-mails, der indgår som led i sagsbehandling, og ikke benytte Outlook eller drev som arkiv.
- Opbevare følsomme og/eller fortrolige data i SBSYS eller i et fagsystem.
- Undgå at gemme på lokale drev som fx C-drevet. Hvis du gemmer informationer og data lokalt på f.eks. den bærbare computer og denne mistes, kan værdifulde informationer og data være tabt for altid. Samtidigt risikeres det at informationerne på den bærbare computer kan komme i forkerte hænder.
- Makulere fysiske dokumenter med personoplysninger, når dokumenterne ikke længere skal bruges.

DU MÅ IKKE:

- Gemme data længere end det er nødvendigt for at løse din opgave, hverken i Outlook eller på et drev.

Sikkerhedsbrud og brud på persondatasikkerheden

DU SKAL:

- Stoppe sikkerhedsbruddet hvis muligt.
- Fortælle din leder eller IT, hvis du opdager eller har mistanke om et sikkerhedsbrud.
- Kontakte GDPR-enheden, så bruddet kan blive anmeldt til Datatilsynet inden 72 timer, hvis det omhandler personoplysninger.
- Være klar over, at lovovertrædelser vil blive anmeldt til politiet.
- Være klar over at sikkerhedsbrud kan medføre disciplinære forholdsregler i overensstemmelse med kommunens retningslinjer.

Har du spørgsmål?

Hvis du har spørgsmål til indholdet i denne folder eller til informationssikkerhed generelt, så skriv til it@herlev.dk

Kontakt GDPR-enheden
Email: sikkerhedsbrud@herlev.dk

Kontakt IT
Tlf. 44 52 70 30
E-mail: 2.level@herlev.dk