

STYR PÅ INFORMATIONSSIKKERHEDEN

Som medarbejder, leder, chef, direktør eller politiker er du underlagt it-sikkerhedspolitikken. Her sætter vi spot på kerneområderne i den. Det er vel at mærke ikke en erstatning for politikken, så læs den – du vil med fordel kunne grave dybere – du er nemlig omfattet af det ansvar, der er beskrevet i den.

Din pc – dit ansvar

Du er ansvarlig for hvad der foregår på din pc fra du logger på, til du logger af; brug din sunde fornuft.

Hvis du mister din computer, iPad eller telefon, så tag straks kontakt til IT og anmeld det som et sikkerhedsbrud via Servicedesk.

Lås eller log af

Når du går fra din computer eller bærbare enhed, skal du altid sætte skærmlås/låsetilstand til, med mindre du logger helt af.

Beskyt dit password

Dit password er personligt og fortroligt. Du må ikke udlevere det eller vise det til andre. Hvis du får mistanke om at andre har kendskab til dit password, skal du ændre det med det samme.

Du skal ændre password med tre måneders mellemrum (minimum) – du får besked, når du logger på. Husk at du ikke må genbruge et password.

Vi arbejder med følsomme og fortrolige oplysninger

Som kommune arbejder vi med følsomme og fortrolige data. Vi har tavshedspligt og behandler alle henvendelser/oplysninger fortroligt. Vi skal leve op til databeskyttelsesforordningen og sikre at data ikke kommer i de forkerte hænder. Det er dit ansvar i det daglige arbejde.

Du må ikke opbevare fortrolige og følsomme oplysninger (fx dokumenter med cpr. numre) mere end 30 dage i mails eller på fællesdrev. Du skal slette filerne efter 30 dage, eller opbevare dem i SBSYS eller eventuelt i kombination med et dertil indrettet fagsystem, der kan håndtere de forskellige data sikkert (fx Nexus, DUBU eller Fasit).

Vi arbejder i SBSYS

SBSYS er vores ESDH-system (Elektronisk Sags og Dokument Håndtering). Alle filer, dokumenter osv. som du arbejder på i en konkret sag – emne- såvel som personsag – skal have base der og/eller journaliseres der. På den måde sikrer vi borgernes rettigheder og lever op til loven. Og samtidig lader vi ikke hinanden i stikken, fordi alt relevant materiale på en sag er samlet et sted som alle relevante medarbejdere kan tilgå.

Gem aldrig filer på dit C-drev, på skrivebordet og i mappen Dokumenter. Der bliver ikke taget backup af dem.

Gem aldrig dokumenter, der har sagskarakter på Ipad, USB-drev eller i cloudbaserede tjenester fx Dropbox.

Fysiske papirer

Fysiske papirer må ikke ligge, så uvedkommende kan få adgang til dem. Fysiske papirer skal låses inde, når du ikke arbejder med dem.

Når du sender og modtager mails

Åbn ikke mails og vedhæftede filer fra en afsender du ikke har tillid til – de kan indeholde virus. Er du i tvivl, kontakt IT og Digitalisering via Servicedesk.

Når du sender en mail, er det officiel post med Rebild Kommune som afsender – tænk over indhold, sprogbrug og målgruppe/modtager, når du skriver. Du skal ikke ændre i layout og signatur. Vedhæft kun pdf-filer, medmindre modtager skal kunne redigere i dokumentet.

Du skal behandle mails ligesom al anden post med hensyn til sagsbehandling, journalisering og besvarelse.

Brug for hjælp?

■ Skriv til Servicedesk.

■ Ring på telefon: 9090

(Udelukkende i tilfælde hvor du ikke har adgang til Servicedesk.)

Der ligger også diverse vejledninger i Servicedesk.

Brug digital post og send sikkert

Send eksternt e-post til borgere, virksomheder og andre myndigheder via den fællesoffentlige digitale postløsning – indholdet bliver krypteret under transmissionen og kan kun læses/sendes efter en tilstrækkelig sikker validering. Du skal bruge doc2mail eller et fagsystem med direkte integration til e-boks/digital post. Du finder vejledning på Skoven.

Det gælder særligt e-post der indeholder fortrolige personoplysninger (fx personnummer og økonomiske forhold) eller følsomme oplysninger (fx om helbred, strafbare forhold, fagforeningsmæssigt tilhørsforhold, seksuel, religiøs, filosofisk eller politisk overbevisning, racemæssig eller etnisk baggrund) – de skal altid sendes via digital post. De modtagere der endnu ikke har oprettet en digital postkasse modtager automatisk et almindeligt brev, når du sender via digital post.

Når du ikke er til stede

Sørg for, at din kalender altid er opdateret og at din mail og telefon bliver besvaret...også når du ikke er til stede.

Brug 'Træffes-ikke-assistenten' når du er fraværende mere end en arbejdsdag – sæt en henvisning på til en kollega eller chef. Det er afgørende for, at vi alle kan levere en god service til borgerne.

Vær opmærksom på, at du ikke må sætte din mail op til at videresende automatisk til eksterne mailsystemer.

Brug din sunde fornuft når du bruger internettet

Vær opmærksom på risikoen for virusangreb og spam. Lad være med at downloade og installere programmer – det må du faktisk ikke.

Du skal have tillid til de eventuelle eksterne netværk, du kobler din bærbare, din tablet eller din smartphone op til – kør en virusscanning, hvis du ikke har været på kommunens netværk i over en uge og i mellemtiden har brugt eksterne netværk eller søgt information på internettet.

It-sikkerhedsorganisationen

Øverste it-sikkerhedsansvarlig:

- Christian Hesthaven, Kommunaldirektør

Daglig it-sikkerhedsansvarlig:

- Charles Lydersen, Funktionsleder for It og Digitalisering

SÆRLIGT TIL LEDERE OG CHEFER - sund viden for alle andre

Som leder/chef i Rebild Kommune, er du ansvarlig for at medarbejderne kender it-sikkerhedspolitikken og følger den.

Årlig sikkerhedskontrol

Vi tjekker dit center en gang om året sammen med dig. Vi ser blandt andet på:

- henvendelser omkring sikkerhed
- behandling og opbevaring af personfølsomme/fortrolige data
- download af programmer
- kendskab til it-sikkerhedspolitikken



Hvad siger loven?

Der sker løbende ændringer i forhold til informationssikkerhed i loven fx inden for serviceloven, databeskyttelsesloven, styrelsesloven, folkeskoleloven osv. Det har blandt andet betydning for hvordan vi håndterer data i kommunen. It og Digitalisering sørger for at holde it-sikkerhedspolitikken opdateret, men det er dit ansvar at følge med løbende.

Ejer du noget data? Har du ansvar for et it-system?

Vi har mange forskellige it-systemer i kommunen og de har alle en centerchef som "ejerman". Hvis du er dataejer eller systemansvarlig, har du ansvaret for at vi, via systemet håndterer data hensigtsmæssigt og lever op til kravene i it-sikkerhedspolitikken.

Har du styr på de programmer dine medarbejdere bruger?

Bruger de dem rent faktisk? Vi skal ikke have licenser og autorisationer til programmer, vi ikke har behov for. Det er dit ansvar at informere It og Digitalisering om programmer, I ikke længere har behov for. Vi trækker med jævne mellemrum rapporter som viser om der er overensstemmelse mellem indgåede licensaftaler og programanvendelse.

Afmeld medarbejdere der stopper, flytter osv.

Når en medarbejder fratræder skal vedkommendes adgang til vores it-systemer lukkes ned – brug Servicedesk.

Af med gammelt it-udstyr?

Vi genanvender udtjent it-udstyr, mobiltelefoner osv. Kontakt it og Digitalisering – vi sørger for miljømæssig forsvarlig og sikker skrotning, eller videresalg til medarbejdere eller eksterne.

Mistanke om virus?

Stop arbejdet og kontakt It og Digitalisering.



Rebild
KOMMUNE