Informationssikkerhedsregler for medarbejdere og ledere

Som ansat i Aabenraa Kommune er der en række retningslinjer inden for informations-sikkerhed. Dem kan du læse mere om på denne side.

Informationssikkerhedsregler ajourføres efter behov og senest hvert 2. år. Nærværende version af informationssikkerhedsreglerne er udarbejdet i 2024.

Adgangskoder

Din adgangskode i Aabenraa Kommune skal være mindst 15 tegn og overholde tre af de fire regler.

1. Minimum et lille bogstav
2. Minimum et stort bogstav
3. Minimum et specialtegn
4. Minimum et tal

Udlever aldrig din adgangskode til andre - heller ikke til IT-Helpdesk.

Genbrug aldrig dine adgangskoder. Bruger du samme kode flere steder, vil hackere få adgang til alle de steder, når de først har knækket din kode. Skriv aldrig din adgangskode ned på en lap papir og have liggende ved computeren - husk den udenad.

Efter overgangen til M365 har du mulighed for at oprette en 6-cifret pinkode på din egen computer (Windows Hello). Pinkoden gælder kun til den pågældende enhed og erstatter ikke din adgangskode. Hvis du glemmer din pinkode, kan du logge på med din adgangskode. Hvis du glemmer din adgangskode, kan du nulstille den med MitID på https://kode.aabenraa.dk

Husk du er som udgangspunkt ansvarlig for, hvad der sker på dit login, så lås altid din skærm, når du forlader din computer.

Trådløse netværk

Du må ikke koble dig på ukrypterede, åbne trådløse netværk (f.eks. i lufthavnen eller på hotellet), hvor der ikke er nogen form for sikkerhed. Et åbent netværk er usikkert, og selvom Aabenraa Kommune benytter Always-on VPN, udgør åbne netværk en trussel mod sikkerheden.

Tilgår du et trådløst netværk ved at logge på med en adgangskode, som du fx har fået udleveret af et hotel, så er netværket lukket og sikkert.

Har du brug for netværksforbindelse, når du er ude, kan du bestille mobilt bredbånd til din bærbar eller dele netværk fra din arbejdsmobil.

Mails

Mails, der skal sendes til eksterne, og som indeholder fortrolige eller følsomme personoplysninger eller andre fortrolige oplysninger, skal altid sendes krypteret. Det betyder, at du i disse tilfælde altid skal sende digital post til borgere og virksomheder.

Borgere, der er fritaget for digital post, modtager forsendelsen som almindeligt brev. Et almindeligt brev er også betragtet som en sikker forsendelse.

Sociale medier

Du skal være meget opmærksom på, hvilke arbejdsrelaterede informationer du deler på sociale medier. Du er som ansat underlagt tavshedspligt om de oplysninger, du kommer i besiddelse af i forbindelse med dit arbejde. Ovenstående betyder ikke, at du ikke har ytringsfrihed. Læs mere om Aabenraa Kommunes vejledning til medarbejderes brug af ytringsfrihed i Aabenraa Kommune her.

Se nedenstående rammer fra Aabenraa Kommunes vejledning om medarbejderes brug af ytringsfrihed i Aabenraa Kommune.

- Man skal gøre det klart, at man udtaler sig på egne vegne og ikke på myndighedens vegne.
- Man må ikke bryde sin tavshedspligt
- Man må ikke udtale sig på en freds- og ærekrænkende måde, f.eks. ved at fremsætte injurier.
- Man må ikke udtrykke sig i urimelig grov form eller fremsætte åbenbart urigtige oplysninger om væsentlige forhold inden for ens eget arbejdsområde.

Mobile enheder og IT-udstyr

Gem ikke fortrolige og følsomme personoplysninger eller andre fortrolige oplysninger på dine mobile enheder (telefoner og tablets).

Du skal altid sørge for, at dine enheder er beskyttet med pinkode.

Du må ikke efterlade dine mobile enheder eller IT-udstyr synligt, når du tager dem med dig fra din arbejdsplads.

Lån ikke dine mobile enheder eller IT-udstyr ud til andre. Dette gælder ikke i afdelinger, hvor man har fælles udstyr.

Hvis dine enheder bliver stjålet, skal du hurtigst muligt kontakte IT-Helpdesk på tlf.: 7376 7827.

Opbevaring af oplysninger

Personoplysninger og andre fortrolige oplysninger skal altid opbevares sikkert også i fysiske udgaver. Dokumenter med disse oplysninger må ikke ligge fremme på skrivebordet, når du forlader dit kontor, og de skal opbevares aflåst, når du ikke er på din arbejdsplads.

Printere, der bruges til at udskrive denne type oplysninger, skal være placeret i områder, hvor uautoriserede personer ikke har adgang, og du bør så vidt det er muligt benytte dig af Follow-You-print.

Personoplysninger og andre fortrolige oplysninger skal altid opbevares i fagsystemer eller kommunens ESDH system, Acadre. Denne type oplysninger kan undtagelsesvist opbevares i Outlook, OneDrive eller på Sharepoint dog højst i 30 dage.

Gem aldrig denne type oplysninger lokalt på computeren, i skytjenester som fx Dropbox og lignende eller på fx USB.

Læs om den gode journaliseringspraksis her.

Opslag i IT-systemer

Du må kun søge oplysninger frem, der er relevante for dit arbejde.

Du må ikke lave søgninger på dig selv, din familie, venner, naboer og lignende. Hvis du er i tvivl, kontakt din nærmeste leder.

Alle opslag i kommunens IT-systemer bliver logget. Loggen bliver brugt ved mistanke om misbrug.

Virus, Phishing og suspekte hjemmesider

Kommunen har tekniske foranstaltninger, der skal forhindre virus, phishingangreb, ransomware og visning af mistænkelige hjemmesider, men de fanger ikke alt.

Modtager du en mistænkelig mail, så slet den. Svar ikke på den og åbn aldrig vedhæftede filer eller links.

Besøg ikke mistænkelige eller anstødelige hjemmesider. Vær kritisk, opmærksom og brug altid din sunde fornuft.

Bliver du ramt, eller er du i tvivl, så kontakt IT-Helpdesk på tlf.: 7376 7827.

Som leder

Som leder er det dit ansvar, at dine medarbejdere kender til disse regler.

Det er også dit ansvar, at dine medarbejdere deltager i den awareness-træning, der bliver sendt ud fra IT-afdelingen, og at der bliver ryddet op i de observationer, der modtages fra Aabenraa DataKvalitet (Adoxa).

Som leder har du ansvaret for dine medarbejderes IT-adgange. Derfor er skal du bestille dine medarbejderes IT-brugere ved ansættelse og bestille deres nedlæggelse ved fratrædelse. IT-adgange bliver bestilt af ledere eller en udpeget medarbejder, ved hjælp af processkema lavet i AdHocIT.

Personalekort

Medarbejderens personalekort, er medarbejderens personlige ansvar.

Ved medarbejders fratrædelse, er det lederens ansvar at kortet bliver afleveret.