Informationssikkerhed og ledelse

10 gode råd om informationssikkerhed i organisationen

Du skal

#01 — huske, at der også er tale om personhenførbare data, når du blot registrerer f.eks. et navn og en e-mail adresse.

#02 — sikre dig, at jeres arbejdsgange omkring databehandling er lovlige. Sørg for, at organisationen har lovgrundlag eller samtykke til at databehandle de oplysninger, som I råder over.

#03 — sørge for, at have passende databehandleraftaler med alle underleverandører, som I videregiver persondata til. Det gælder også virksomheder, som I midlertidigt giver adgang til jeres systemer. Husk at systemer som f.eks. Dropbox, Gmail og de bagvedliggende virksomheder, også er underleverandører. Bemærk at bl.a. USA ikke er på listen over de lande som EU regner for sikre, og der skal derfor mere til, før du kan udveksle persondata med virksomheder beliggende i USA.

#04 — sørge for, at jeres interne it-infrastruktur er sikret med backup, firewall og andre relevante tekniske foranstaltninger. Vær endvidere opmærksom på, at smartphones også kan udgøre en stor risiko. Sikkerhedshuller findes og rettes løbende, og du bør derfor sikre dig at jeres systemer er opdaterede.

#05 — sørge for, at personalet følger jeres instrukser omkring informationssikkerhed. Skriv det i ansættelsesbreve eller i personalehåndbogen.

MICO_ Sanocast

Informationssikkerhed og ledelse

10 gode råd om informationssikkerhed i organisationen

Du bør

#06 — uddanne og instruere personalet i god databehandlingsskik. Personalet bør vide, hvordan data skal behandles og at man eksempelvis i udgangspunktet ikke må videregive persondata til tredjepart. Som udgangspunkt skal personalet også vide, at man ikke skal stole blindt på det, der står i en e-mail.

#07 — sørge for, at I har "funktionsadskillelse". Hold data "on a need to know basis": Altså at det kun er de medarbejdere, som absolut har brug for en informationsbid, som har adgang til denne informationsbid. Hvis rengøringen ikke har brug for adgang til regnskabssystemet, så skal rengøringen heller ikke have adgang til regnskabssystemet.

#08 — uddelegere ansvaret for it-sikkerhed til relevante nøglepersoner, således at der er nogen der har ansvaret for at tage affære, hvis der opstår huller i informationssikkerheden.

#09 — være opmærksom på, at hjemmearbejdspladser og adgang til jeres systemer fra eksterne lokationer kan kræve ekstra fokus på it-sikkerheden. For i disse tilfælde har man ofte en mindre grad af kontrol over systemerne. I nogle tilfælde kan det også være nyttigt at begrænse adgang til systemerne, således at der er en adskillelse mellem privat- og arbejdsbrug. Benyt aldrig servere til privat brug. De er beregnet til arbejdsopgaver.

#10 — husk også, at fysisk sikkerhed er en del af informationssikkerheden. Kan en udefrakommende gå ind på kontoret og læse med på din skærm? Er der passende regler for, hvem der låser dørene? Hvem der slår alarmen til?

MICO_ Sanocast