



360 grader rundt om informationssikkerhed

Informationssikkerhed handler helt lavpraktisk om at sikre informationer og data, skabe digital tryghed og undgå informationsmisbrug.

Inden for informationssikkerhedsområdet taler man om tre grundlæggende principper for, hvordan man opretholder informationssikkerheden.

1. Vi skal sørge for, at alle kun har adgang til de informationer, de bør se
 - Det kendes også som princippet om **"fortrolighed"**
2. Vi skal sørge for, at vores informationer er korrekte og ikke bliver forvansket
 - Det kendes også som princippet om **"integritet"**
3. Vi skal sørge for, at alle har adgang til de informationer og systemer, de skal bruge i deres arbejde
 - Det kendes også som princippet om **"tilgængelighed"**

Hvad er din rolle i informationssikkerhedsarbejdet?

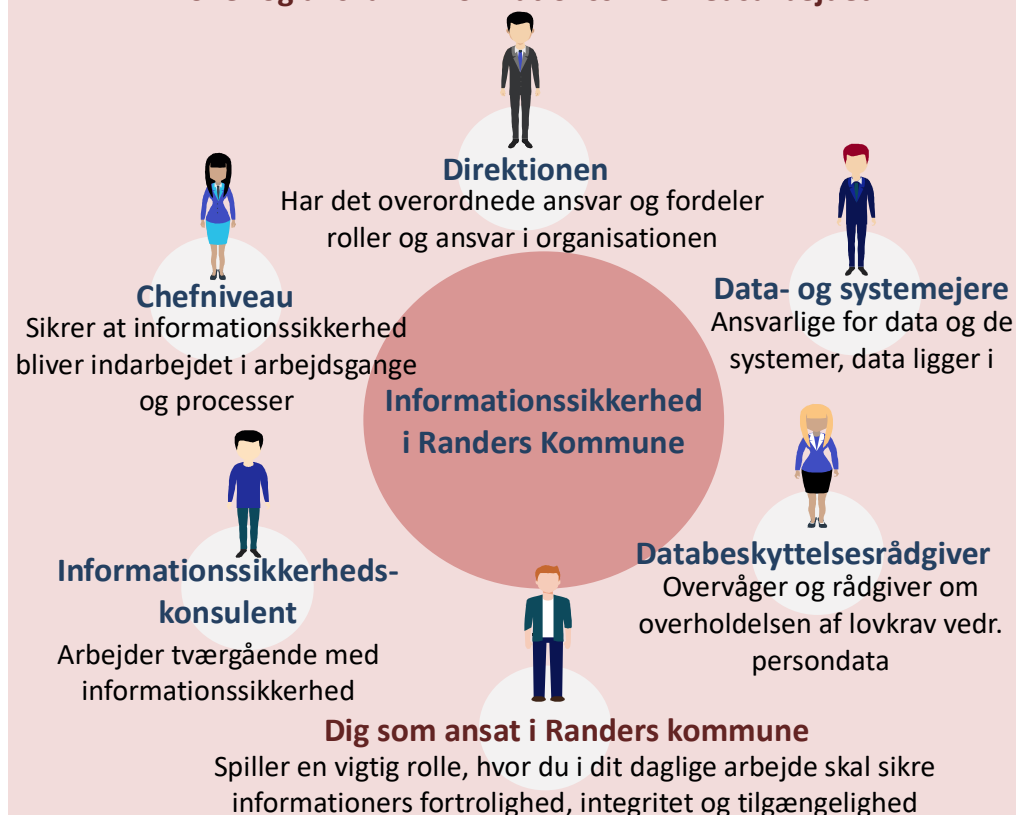
Som ansat i Randers Kommune, er du med til at sikre, de enkelte opgaver udføres på en måde, så vi som kommune samlet set efterlever lovgivningen, vores interne politikker – samt undgår alvorlige økonomiske tab og personlige konsekvenser mv.

Du skal:

- Overholde gældende politikker, fx informationssikkerhedspolitikken
- Udpege mangler i gældende politikker og efterlevelsen af disse
- Rapportere risici og brud på informationssikkerheden



Roller og ansvar i informationssikkerhedsarbejdet



Brug for mere viden eller hjælp?

Har du generelle spørgsmål til informationssikkerhed, kontakt da Randers Kommunes informationssikkerhedskonsulent, Carsten Povlsen på csp@randers.dk eller tlf.nr.: 5135 0964.

Har du spørgsmål til databeskyttelse, herunder behandling af personoplysninger, kontakt da Randers kommunes Databeskyttelsesrådgiver, Maiken Sørensen på dpo@randers.dk eller tlf.nr.: 5156 2800.

Sikkerhedshændelser

Det er vigtigt, at være opmærksom, når der sker en sikkerhedshændelse. I ISO 27000-standarden er det defineret som:
"En identificeret forekomst af en system-, tjeneste- eller netværkstilstand, der indikerer et muligt brud på informationssikkerhedspolitikken eller svigt af kontroller, eller en tidligere ukendt situation der kan være relevant for sikkerheden ..."

En informationssikkerhedshændelse kan samtidig være et brud på persondatasikkerheden. Det er dog kun de informationssikkerhedshændelser, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der betegnes som et brud på persondatasikkerheden.

Der er tale om et brud på informationssikkerheden når, en eller flere af de grundlæggende principper ikke er intakt, fx:

- ☐ Nogen har fået adgang til informationer, de ikke bør se = brud på fortroligheden
- ☒ Alle har adgang til de informationer, de skal bruge i deres arbejde (tilgængelighed)
- ☒ Vores informationer er korrekte (integritet)

Alle informationssikkerhedshændelser skal indberettes til informationssikkerhedskonsulenten, og alle brud på persondatasikkerheden skal indberettes til databeskyttelsesrådgiveren straks.

Mere materiale?

På Broen findes mere awareness-materiale omhandlende informationssikkerhed og databeskyttelse.

Meget af materialet er egnet til at printe ud og hænge op, så dine kolleger også kan få glæde af det.

INFORMATIONSSIKKERHED HVAD ER MIT ANSVAR SOM ANSAT I RANDERS KOMMUNE?

Hvordan styrker vi
informationssikkerheden i
praksis?

Arbejdet med løbende at styrke informationssikkerheden er et ansvar, der er fordelt ud på hele organisationen.

