



ISO 27001

ISO 27001 er en international standard for styring af informationssikkerhed. Ved at etablere processer med ISO 27001 sikrer vi Randers kommune kan træffe bevidste og korrekte valg omkring sikringen af informationer samt data.

Krav om ISO 27001 i den offentlige sektor

Den nationale strategi for cyber- og informationssikkerhed (2014) stiller krav til statslige myndigheder skal arbejde systematisk efter sikkerhedsstandarden ISO 27001.

Med den seneste fællesoffentlige digitaliseringsstrategi (2016-2020), er den øvrige del af den offentlige sektor underlagt et krav om, at følge principperne i standarden.

Derfor er Randers Kommune i dag underlagt at følge principperne i ISO 27001. Standarden er desuden et godt afsæt for, at håndtere kravene i persondataforordning, der trådte i kraft i maj 2018.

Hvad er værdien?

Med en systematisk tilgang til styring af risici, kan Randers Kommune investere i informationssikkerhed, hvor det giver størst muligt afkast – hvad enten det indebærer beskyttelse af de fysiske rammer, it-tekniske kontroller eller en ændring af medarbejdernes adfærd.

Dette vil bl.a. kunne bidrage til sikring af compliance i forhold til love, regeringskrav, leverandøraftaler og benyttede best practices.



Du er med til at sikre, at Randers kommune er FIT

FIT står for:

➤ Fortrolighed

- At kun autoriserede personer har ret til at tilgå informationerne.

➤ Integritet

- Data er pålidelig, når de er komplette, korrekte og opdaterede.

➤ Tilgængelighed

- Det skal være muligt at tilgå systemer og data for autoriserede personer, når dette er nødvendigt.

På engelsk bruges begrebet CIA, som står for confidentiality, Integrity og availability

Randers Kommunes informationssikkerhedspolitik

Den overordnede organisering af informationssikkerhedsarbejdet og ansvaret for informationssikkerheden i Randers Kommune er beskrevet i informationssikkerhedspolitikken, som blev vedtaget d. 07.10.19 af Randers Kommunes Byråd.

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.

Gode tommelfingerregler



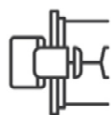
Låst skærm

Lås altid din PC, når du går fra den - benyt tastaturgenvejen **⌘ + L**. Husk også at låse smartphones og tablets.



Adgangskode

Lav unikke og gerne lange kodeord - og hold dine adgangskoder for dig selv.



Ryd op på dit skrivebord!

Hav ikke fortrolige og følsomme oplysninger på dit skrivebord - dette gælder også skrivebordet på din PC.



Print

Benyt Follow you-print når du printer - eller hent dine print med det samme.



Papir

Opbevar papir med fortrolige og følsomme oplysninger, hvor uvedkommende ikke har adgang til dem, fx i aflåste skabe.



Arkivering

Arkiver dine dokumenter i dit fagsystem eller SBSYS - ikke på dit skrivebord eller drev.



Registrering

Registrer kun oplysninger, som er relevante for sagen.



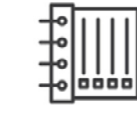
Behandlingshjemmel

Har du hjemmel til behandling af personoplysninger? - Husk at oplysninger må kun behandles til det formål, de er indhentet til.



Mail

Mails indeholdende fortrolige og følsomme personoplysninger, må max ligge 30 dage i Outlook. Journaliser løbende og slet i Outlook.



Kalender

Skriv ikke personoplysninger, som f.eks. CPR-nummer, i emnefeltet på kalenderaftaler i Outlook. Det samme er gældende i emnefeltet i mails, da det ikke krypteres.



Korrekt modtager?

Vær opmærksomhed på, om digital post sendes til rette modtager. Har du mere end en sag åben - så dobbeltjek modtageren og eventuelle bilag inden afsendelse.

GENEREL INTRODUKTION TIL INFORMATIONSSIKKERHED

Informationssikkerhed er sikring af informationers fortrolighed, integritet, og tilgængelighed. Dette er med til at skabe digital tryghed og sikring mod informationsmisbrug.

