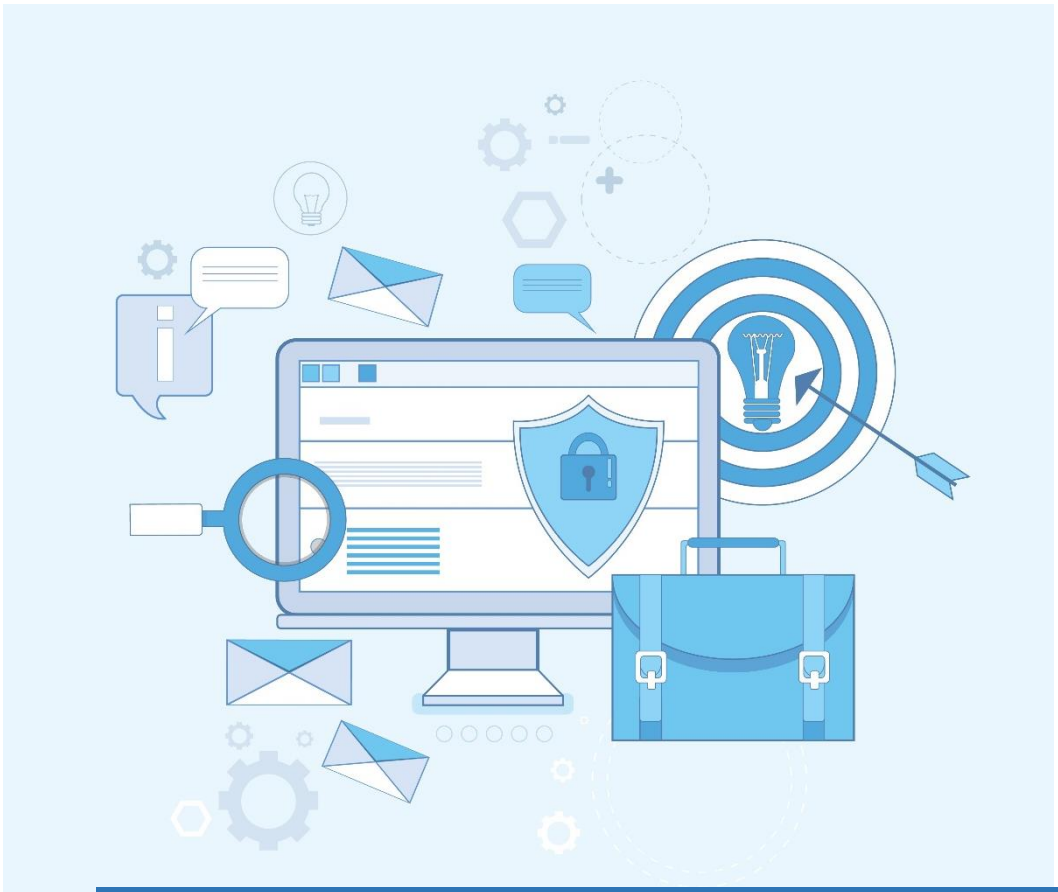


Introduktion til informations-sikkerhed og organisering af sikkerhedsarbejdet i Randers Kommune

Til systemejere i Randers Kommune

Indholdsfortegnelse

Hvad er Informationssikkerhed?

Informationssikkerhed handler om, at sikre fortrolighed, integritet og tilgængelighed for Randers Kommunes informationer. Som systemejer i Randers Kommune, har du ansvaret for at sikre informationssikkerheden i det enkelte system.

F I T

Fortrolighed: Kun autoriserede personer har ret til at tilgå informationerne

Integritet: Sikre datas 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

Informationssikkerhedsstandarden ISO 27001 og relationen til de databeskyttelsesretslige regler

Indenfor informationssikkerhed er ISO 27001 den internationale standard for styring. Ved at etablere processer for styring af informationssikkerhed med ISO 27001 sikrer vi, at direktionen kan træffe bevidste valg omkring sikringen af informationer og data.

Krav om ISO/IEC 27001 i den offentlige sektor

Randers Kommune er, grundet den fælles offentlige digitaliseringsstrategi, i dag underlagt at følge principperne i standarden ISO/IEC 27001. Standarden er derudover et godt afsæt til at håndtere kravene i EU's databeskyttelsesforordning, der trådte i kraft i maj 2018.

Hvorfor ISO/IEC 27001? 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 organisationens 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, benyttede best practices etc.

Kravene til systemejere i Randers Kommune er fundet med udgangspunkt i ISO 27001s kontroller i anneks A. Alle ansvarsområder for informationssikkerhed skal defineres og fordeles jf. ISO 27001 A.6.1.1, samt skal der jf. ISO 27001 A.8.1.2 udpeges en ejer i organisationen for hvert aktiv (en systemejer).

Ifm. efterlevelse af kravene i ISO 27001, har Randers Kommune et ledelsessystem (ISMS) hvor regelsæt, politikker, kontroller m.m. håndteres. Praktisk tilgås dette i systemet *Control Manager*, som omfatter hele Randers Kommunes informationssikkerhedshåndbog.

Databeskyttelsesforordningen

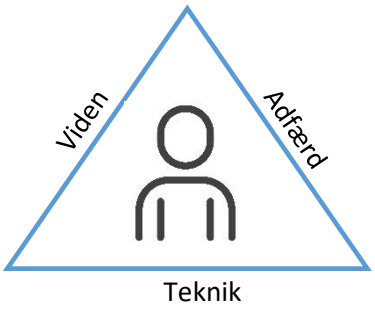
Hvis du er systemejer for et system, der behandler personoplysninger, skal dit system overholde reglerne i EUs databeskyttelsesforordning (GDPR) og den danske databeskyttelseslov. Ud over kendskab til lovgivningen, skal du også kende til Randers Kommunes politikker, procedurer og retningslinjer indenfor området.

Informationssikkerhedsniveau i Randers kommune

Informationssikkerheden i Randers Kommune skal ligge på et niveau, der sikrer overholdelse af lov- og myndighedskrav, kontraktlige forpligtelser samt forpligtelser over for de aktører, der er forpligtet til at anvende Randers Kommune.

Sikkerhedsniveauet skal have et afbalanceret omfang, således at der samtidig med høj sikkerhed kan fastholdes en effektiv og fleksibel opgaveløsning. Randers Kommune ønsker dermed ikke at sikre sig for enhver pris, men ønsker at være bevidst om risici, og forholde sig aktivt og fagligt tilfredsstillende til disse, hvormed et tilstrækkeligt sikkerhedsniveau etableres.

For at kunne implementerer et tilfredsstillende modenhedsniveau af informationssikkerhed, skal der i der tages udgangspunkt i viden, adfærd og teknik.



Uden disse tre elementer, kan informationssikkerheden ikke fungere i praksis. Ingen af elementerne kan stå alene, da de alle er grundsten for en succesfuld implementering.

Fx hvis en medarbejder ikke har den nødvendige viden, så ville denne ikke kunne udvise korrekt adfærd eller bruge den korrekte tekniske understøttelse.

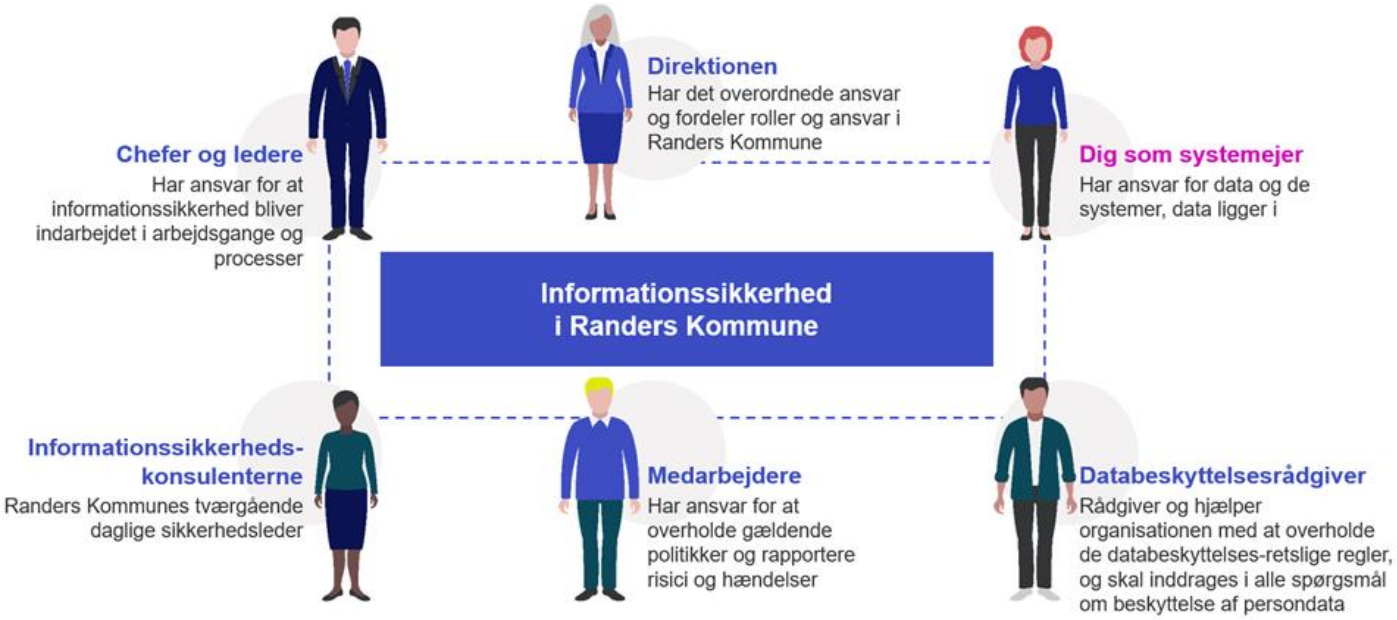
Organisering af sikkerhedsarbejdet i Randers kommune jf. Randers kommune informationssikkerhedspolitik

I Randers Kommune er kommunaldirektøren den øverste sikkerhedsansvarlige, hvor direktionen udgøre det strategiske niveau i forbindelse med informationssikkerhed. Det taktiske niveau udgør sekretariatschefgruppen (fungerer som Randers Kommunes informationssikkerhedsudvalg), som referer til direktionen.

Informationssikkerhed er en integreret del af det generelle ledelsesansvar, og følger den decentrale model på alle ledelsesniveauer svarende til den pågældendes leders organisatoriske placering og ledelsesansvar. Det er lederens ansvar at sikre forankring af informationssikkerhed i forretningsprocesser og aktiviteter. Lederen er rollemodel i forhold til informationssikkerhed. Det er dermed en leders opgave at orientere sine medarbejdere om informationssikkerhed.

Som en del af informationssikkerhedsarbejdet i Randers Kommune udpeges system- og dataejere, som bl.a. har ansvar for retningslinjer og instrukser for egne systemer.

Randers Kommunes medarbejdere har ansvar for at holde sig orienteret om informationssikkerhedspolitikkens regler og procedurer og på baggrund heraf udvise omhu i den daglige anvendelse af informationsaktiverne.



Alle medarbejdere – med og uden ledelsesansvar – har en forpligtelse til at overholde kommunens informationssikkerhedspolitik og –regler. Alle har derved en rolle i arbejdet med informationssikkerhed.

Principper for udvælgelse af systemejer

Principper for udvælgelse af systemejer er i Randers Kommune således:

- En systemejer udpeges som udgangspunkt indenfor det fagområde eller kontraktområde, hvor systemet anvendes.
- Er der tale om et system, der anvendes på tværs af forvaltninger placeres systemejerskabet som hovedreglen i en stab.
- Det overordnede systemejerskab kan placeres hos direktører, fag- eller stabschefer eller ledere med direkte reference til fag- og stabschefer. Systemejer kan være den budgetansvarlige.

Andre relevante roller (systemforvalter og daglig kontaktperson)

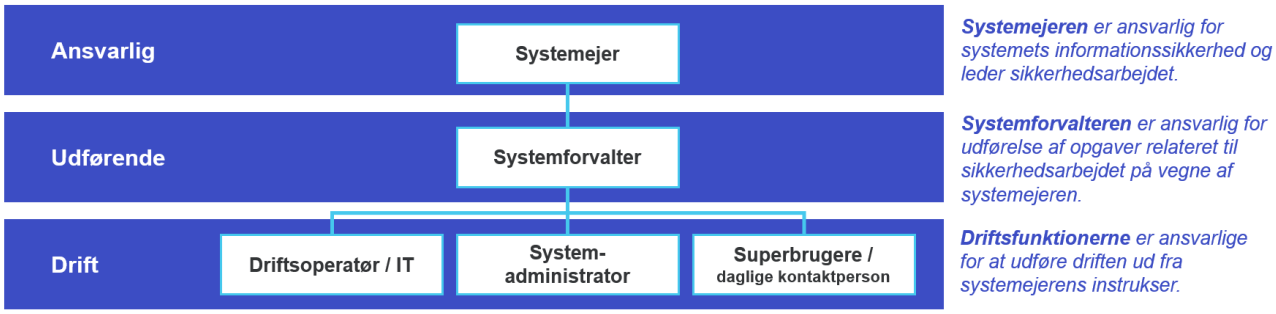
Alle systemer skal som minimum have udpeget en systemejer. Det kan dog flere steder være relevant at arbejde med en overordnet systemejer, en systemforvalter og evt. en daglig kontaktperson.

Det er op til systemejer om de andre roller også skal udpeges. Systemejer har ansvaret for at udpege en systemforvalter og evt. en kontaktperson, hvis dette ønskes.

Systemejeren kan uddelegere udførelsen af dennes opgaver til en eller flere systemforvaltere og evt. en daglig kontaktperson. ***Ansvaret kan dog aldrig uddelegeres.***

I forhold til informationssikkerhed har systemejeren ansvar for at sikre at opgaverne udføres. I praksis vil dette arbejde ofte være delegeret til en systemforvalter som er udførende på systemets sikkerhedsarbejde, og som styrer sikkerhedsarbejdet i forhold til driftsfunktionerne. En række specialistfunktioner (fx informationssikkerhedskonsulent, databeskyttelsesrådgiver, It-driftsmedarbejdere) vil desuden være konsulterende i forhold til både den ansvarlige og udførende ledelse af systemet.

Udover systemejer og –forvalter, kan der være personer der er udpeget til at varetage "øvrige aktiver", f.eks. It-udstyr, adgangsforhold, arkivskabe m.v. – de er ansvarlige for øvrige "aktiver" (se nedenstående figur).



Rollen som systemforvalter

Systemforvalteren er en person, der har indgående indsigt i systemets tekniske opbygning og anvendelse og som på den baggrund kan indgå i arbejdet med udarbejdelse af f.eks. risikovurderinger, beredskabsplaner og databehandleraftaler.

Hvis det giver mening indenfor det konkrete system, kan der udpeges flere systemforvaltere med forskellige roller.

Systemforvalter kan være den samme person som den overordnede systemejer. En systemforvalter kan både være en chef/leder eller en medarbejder.

Den overordnede systemejer kan uddelegere udførelsen af de systemejerens opgaver til systemforvalterne. Ansvaret kan dog aldrig uddelegeres.

Daglig kontaktperson

Den daglige kontaktperson kan være den samme person som systemforvalteren og kan evt. bruges som screening inden henvendelser sendes videre til systemforvalteren eller systemejeren, samt løse simple forespørgsler.

Systemoverblik

Alle systemer skal registreres i IT og Digitaliserings overbliksværktøj KITOS. Her knyttes systemer, roller og informationer om systemet sammen.

IT og Digitalisering følger løbende op på, om alle systemer har en systemejer og at de gældende systemejere er korrekt ajourført i KITOS.

Ved anskaffelse af nyt system eller nedlukning af eksisterende system, skal systemejer sikre at systemoverblikket i Kitos bliver ajourført.