Skanderborg Kommune

Sikkerhedsorganisationen

Ledelsessystem for informationssikkerhed baseret på ISO 27001:2017

i Skanderborg Kommune

Version 1.0

Januar 2021

Indhold

Indledning 2
Organisering 2
Byrådet 4
Direktionen ved kommunaldirektøren 4
Databeskyttelsesrådgiveren (DPO) 4
Informationssikkerhedsgruppen 4
Digitaliserings- og it-chefen 5
Informationssikkerhedskoordinatoren og it-sikkerhedskonsulenten 5
Systemejere 5
It-medarbejdere 5
Koncerncheferne 6
Kitos-ansvarlige 6
Medarbejdere 6
Bilag 1 Informationssikkerhedsorganisationens sammensætning og tilhørende opgavebeskrivelser 7
Bilag 2 metodevalg 11

Indledning

Skanderborg Kommune har etableret et ledelses- og styringssystem for organisationens informationssikkerhed, som beskrives her.

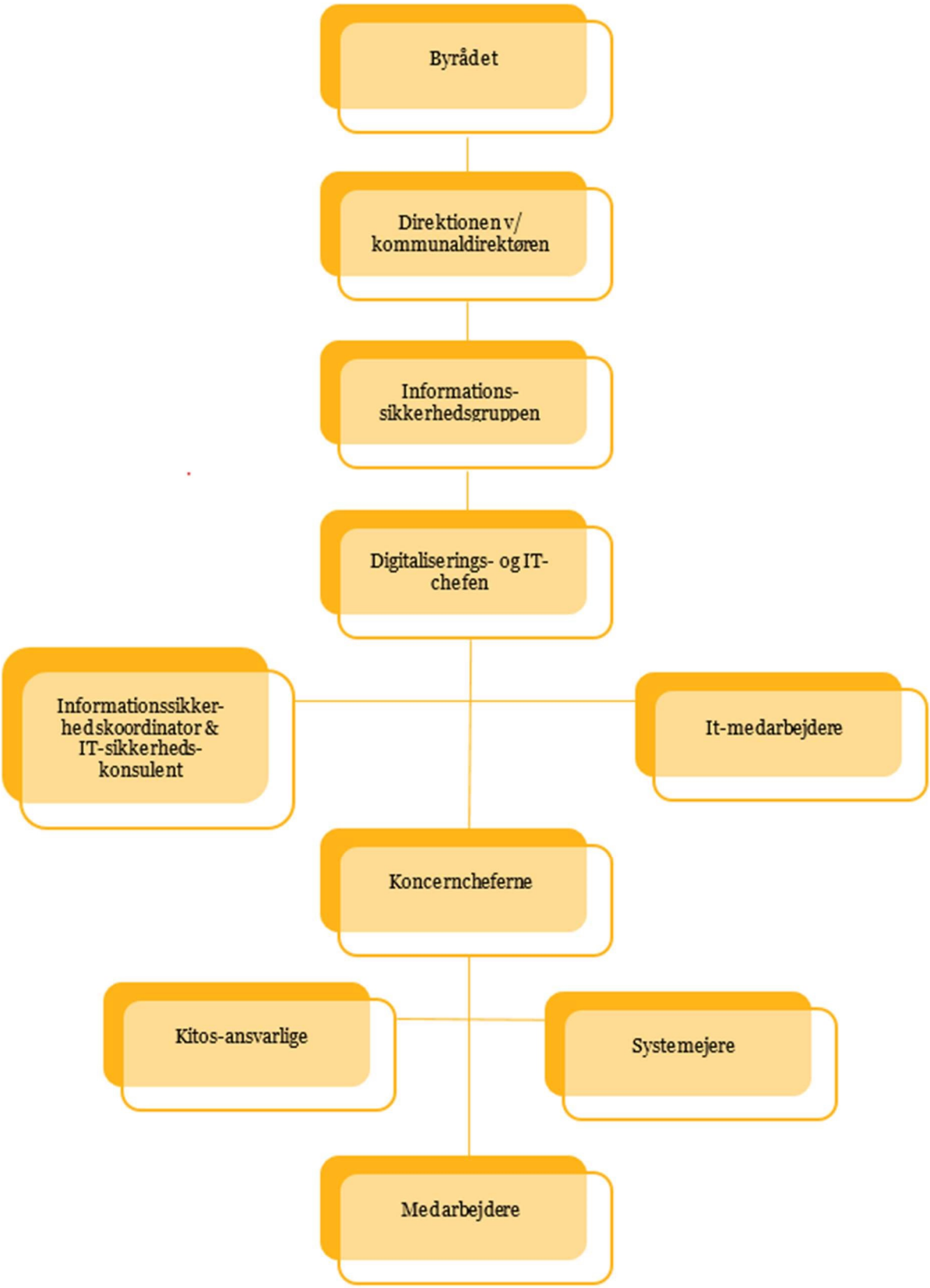
Ledelsessystemet følger den internationale standard for informationssikkerhed, ISO 27001, og definerer roller, ansvar og beføjelser, som er placeret hos aktørerne i ledelsessystemet. Derudover er krav i databeskyttelsesforordningen indarbejdet.

Formålet med systemet er at sikre, at topledelsen i Skanderborg Kommune påtager sig ansvaret for at etablere, implementere, vedligeholde og løbende forbedre informationssikkerheden i overensstemmelse med standardens og forordningens krav.

Organisering

I forbindelse med arbejdet er der forskellige roller og ansvarsfordelinger.

Skanderborgs kommunaldirektør er øverste formelle ansvarlige chef for den administrative styring af informationssikkerhedsindsatsen og skal sikre overordnet prioritering og ressourcetildeling. Derudover er kommunaldirektøren og direktionen formelt ansvarlig for at sikre den fornødne kontrol med efterlevelse af informationssikkerhedspolitikken.


Byrådet
Direktionen v/ kommunaldirektøren
Informations-sikkerhedsgruppen
Digitaliserings- og IT-chefen
Informationssikker-hedskoordinator & IT-sikkerheds-konsulent
It-medarbejdere
Koncerncheferne
Kitos-ansvarlige
Systemejere
Medarbejdere

Byrådet

Byrådet er overordnet ansvarlig i forhold til Skanderborg Kommunens overholdelse af databeskyttelsesforordningen og databeskyttelseslovens bestemmelser. Byrådet skal godkende den overordnede standard for informationssikkerhed.

Byrådet orienteres om konkrete sikkerhedsbrud, hvor kommunaldirektøren finder dette relevant, og hvis rapporten for sikkerhedshændelser generelt giver anledning til det.

Direktionen ved kommunaldirektøren

Direktionen ved kommunaldirektøren har det øverste formelle ansvar for styringen af informationssikkerhedsindsatsen og skal sikre overordnet prioritering og ressourcetildeling.

Direktionen skal endvidere sikre etableringen af en tværfaglig informationssikkerhedsgruppe, hvis opgaver er at etablere, implementere, vedligeholde og forbedre ledelsessystemet for informationssikkerhed.

Databeskyttelsesrådgiveren (DPO)

Varetagelsen af databeskyttelsesrådgiverens opgaver er udliciteret til advokatfirmaet Bech-Bruun, som har udpeget en fast person til at varetage Skanderborg kommunes interesser.

DPO'en informerer og rådgiver kommunen om dens forpligtelser i forhold til at efterleve databeskyttelseslovgivningen og fører tilsyn med og gennemfører kontroller på området.

DPO'en rapporterer mindst én gang årligt til informationssikkerhedsgruppen og byrådet.

Informationssikkerhedsgruppen

Informationssikkerhedsgruppen er tværfaglig og udgøres af koncernledelsen samt digitaliserings- og it-chefen. Informationssikkerhedskoordinatoren er sekretær for gruppen.

Gruppen etablerer en sikkerhedsorganisation, der placerer ansvaret for udmøntning af de gældende informationssikkerhedsregler.

Gruppen udarbejder den overordnede standard for informationssikkerhed, der beskriver rammerne for arbejdet med informationssikkerhed i Skanderborg Kommune.

Gruppen skal sikre udarbejdelsen og vedligeholdelse af de uddybende informationssikkerhedsregler og de underliggende specifikke retningslinjer, vejledninger, strategier og planer.

Gruppen godkender den overordne standard for informationssikkerhed og de uddybende informationssikkerhedsregler, der beskriver de tekniske og organisatoriske sikkerhedsforanstaltninger.

Gruppen behandler konkrete tværgående sikkerhedsspørgsmål og udstikker rammerne for implementering og kommunikation af beslutninger vedrørende informationssikkerhed. Informationssikkerhedsgruppen skal i den forbindelse sikre, at arbejdet med informationssikkerhed også har øvrige lederes opbakning.

Gruppen præciserer om nødvendigt informationssikkerhedskoordinatoren og it-sikkerhedskonsulentens beføjelser i forbindelse med kontrol af organisationens overholdelse af sikkerhedsregler og forpligtelser i henhold databeskyttelseslovgivningen.

Gruppen bidrager yderligere til arbejdet med informationssikkerheden i organisationen gennem engagement, synlig medvirken og præcis ansvarsplacering.

Digitaliserings- og it-chefen

Digitaliserings- og it-chefen har på tværorganisatoriske niveau ansvar for driften af tekniske sikkerhedsforanstaltninger og bidrager til implementering af organisatoriske foranstaltninger.

Digitaliserings- og it-chefen bidrager til informationssikkerhedsgruppen med nødvendig og relevant information og fremlægger rapporter om informationssikkerheden, hvor han finder behov for det.

Digitaliserings- og IT-chefen bidrager til udbredelse af informationssikkerheden i hele organisationen og indstiller til nødvendige ændringer, hvor behov opstår, samt sikrer en kontinuerlig indsats for bevidstgørelsen af nødvendigheden for informationssikkerhed i hele organisationen.

Informationssikkerhedskoordinatoren og it-sikkerhedskonsulenten

Informationssikkerhedskoordinatoren har som sin primære funktion at varetage den daglige koordinering af informationssikkerhedsindsatsen på tværs af organisationen med ansvar for den operationelle styring heraf.

Koordinatoren har ansvar for at holde sig orienteret både internt og eksternt om forhold, der har betydning for kommunens samlede informationssikkerhedsarbejde.

Koordinatoren fungerer som sekretær for informationssikkerhedsgruppen.

It-sikkerhedskonsulenten udfærdiger risikovurderinger og dokumentation af tværorganisatoriske it-processer, herunder beredskabsplaner.

Informationssikkerhedskoordinatoren og it-sikkerhedskonsulenten samarbejder med kolleger på alle niveauer og på tværs af organisationen

Systemejere

Der er udpeget en systemejer for alle it-systemer. Systemejeren udpeges inden for det område, hvor systemet anvendes. Systemejerskabet for systemer, der anvendes på tværs af flere fagområder i organisationen, placeres i hovedreglen i en stab. Systemejeren kan uddelegere opgaverne vedrørende it-sikkerhed, men ansvaret vil fortsat påhvile systemejeren.

Systemejer har ansvar for, at systemerne er registreret i kommunens løsning til overblik over it-systemer.

Systemejere har ansvar for informationssikkerheden i forbindelse med sine systemer i hele deres livscyklus, og systemejer skal i den forbindelse sikre, at den rette dokumentation er udarbejdety, og de rette kontroller gennemføres i henhold til Håndbog for systemejere.

It-medarbejdere

It-medarbejdere har et særligt ansvar for at være opmærksomme og varetage informationssikkerheden på deres respektive ekspertområder.

It-medarbejdere udfærdiger beredskabsplaner i samarbejde med it-sikkerhedskonsulenten og udfører kontroller på de områder, de er ansvarlige for.

It-medarbejdere indrapporterer sikkerhedshændelser og –brud, som de bliver opmærksomme på.

It-medarbejdere bidrager med teknisk information til beslutningsgrundlag for sikkerhedsforanstaltninger.

Koncerncheferne

Koncerncheferne er medlemmer af informationssikkerhedsgruppen sammen med direktionen. De er således bindeleddet til resten af organisationen og sikrer formidlinger af beslutninger og anden vigtig information vedrørende informationssikkerhed til medarbejderne i kommunen.

Koncerncheferne skal have fokus på informationssikkerhed i det daglige arbejde i deres områder og skal sikre tilstrækkelige ressourcer og vidensniveau til efterlevelse af regler og krav.

Koncerncheferne udpeger systemansvarlige, hvis der kan være tvivl om placeringen af denne rolle, og de udpeger områdets Kitos-ansvarlige.

Kitos-ansvarlige

I it-systemet Kitos registreres alle it-systemer, som er eller har været i anvendelse i Skanderborg Kommunen. Systemet fungerer således som det samlede overblik over systemlandskabet, det organisatoriske forankring, databehandlingen i systemerne samt efterlevelsesniveau for reglerne for behandling af personoplysninger.

Der er udpeget en Kitos-ansvarlig i hvert fag- eller stabsområde, og vedkommende har en koordinerende roller i at samle det nødvendige overblik over området systemer og administrationen heraf.

Medarbejdere

Alle medarbejdere skal bidrage til, at Skanderborg Kommune lever op til gældende databeskyttelseslovgivning og interne regler for informationssikkerhed.

Alle medarbejdere i kommunen har derfor et ansvar for at holde sig orienteret om gældende informationssikkerhedsregler og retningslinjer både generelt og i forbindelse med vedkommendes aktuelle ansvarsområde og arbejdsopgaver.

Alle medarbejdere har pligt til at være opmærksomme på trusler mod informationssikkerheden og indrapportere brud på sikkerheden til nærmeste leder og/eller systemejer og til 7-9-13 Servicedesk.

Afrapportering

Der foretages regelmæssig afrapportering af status på informationssikkerhed samt ad hoc ved vigtige hændelser med betydning for organisationen, herunder alvorlige brud på sikkerheden.

Status på informationssikkerhed skal som minimum én gang årligt forelægges informationssikkerhedsgruppen. Resultat af it-revision rapporteres også til informationssikkerhedsgruppen.

Rapporteringen foregår ved databeskyttelsesrådgiveren og/eller Digitaliserings- og IT-chefen.

Bilag 1 Informationssikkerhedsorganisationens sammensætning og tilhørende opgavebeskrivelser

	Byrådet
Opgaver	• Godkender og beslutter den overordnede sikkerhedspolitik • Godkender omfanget af Informationssikkerheden • Bidrager til en ledelsesmæssig forankring af informationssikkerheden.
Særlige forhold	Ingen

	Direktionen ved kommunaldirektøren
Opgaver	• Modtager status på informationssikkerheden • Beslutter omfanget for informationssikkerheden • Sikrer den overordnede prioritering af informationssikkerheden • Sikrer fornøden ressourcetildeling til området • Bidrager til en ledelsesmæssig forankring af informationssikkerheden
Særlige forhold	Ingen

	Databeskyttelsesrådgiveren (DPO)
Opgaver	• Rapporterer direkte til øverste ledelsesniveau • Underretter og rådgiver kommunen om dens forpligtelser i henhold til databeskyttelsesforordningen og overvåger overholdelsen. • Overvåger overholdelsen af kommunens standarder og retningslinjer for beskyttelses af personoplysninger, herunder fordeling af ansvar, oplysningskampagner og uddannelse af medarbejdere. • Rådgiver i forbindelse med konsekvensanalyser • Samarbejder med tilsynsmyndigheden på kommunens vegne
Særlige forhold	Ingen

	Informationssikkerhedsgruppen
Opgaver	• Indhenter og gennemgår status på efterlevelse af sikkerhedsregler og –procedurer • Igangsætter nødvendige ændringer eller forbedringer af informationssikkerheden • Tager stilling til ønsker og behov for informationssikkerhedsforanstaltninger fra organisationen ud fra en risikobaseret tilgang og indgående kendskab til organisationens fag- og stabsområder samt kontraktholdere • Sikrer at systemejerne er bekendt med opgaver inden for deres ansvarsområder, og at der føres kontrol med efterlevelsen • Foretager en regelmæssig vurdering af det aktuelle tværgående risikobillede Sikre en løbende revurdering af informationssikkerhedsstandarden og de uddybende informationssikkerhedsregler på grundlag af rapportering efter tilsyn og kontroller • Indstilles til byrådet om ændringer i informationssikkerhedsstandarden, når der skønnes behov for dette • Sikrer bevidsthed om og uddannelse i informationssikkerhedsarbejde i organisationen

	• Tilegner sig et godt kendskab til og forståelse for databeskyttelseslovgivningen og informationssikkerhedsstandarderne ISO 27001 og 27002
Særlige forhold	Ingen

	Digitaliserings- og it-chef
Opgaver	• Med godt kendskab til og forståelse for ISO 27001 inddrager • Informationssikkerhedsgruppen med nødvendig og relevant information • Fremlægge rapporter på informationssikkerheden for informationssikkerhedsgruppen • Kommunikere informationssikkerheden ud i hele organisationen • Indstille behov for ændringer i informationssikkerhedspolitikken • Igangsætte ændringer eller forbedringer af informationssikkerheden • Sikre fokus og awarenes i hele organisationen • Have overblik over handlinger og justeringer på informationssikkerheden Have indgående kendskab til eget forretningsområde
Særlige forhold	Indgår i informationssikkerhedsgruppen og har kompetence til at iværksætte selvstændige beredskabstiltag

	IT-medarbejdere
Opgaver	• Medvirker til overholdelse af informationssikkerheden • Implementerer ønskede forandringer til sikring af datasikkerheden • Udfører fornødne kontroller • Bidrager til løsningsmodeller for øget informationssikkerhed
Særlige forhold	Ingen

	Informationssikkerhedskoordinator og it-sikkerhedskonsulent
Opgaver	• Medvirker til overholdelse af informationssikkerheden • Implementerer ønskede forandringer til sikring af datasikkerheden • Udfører fornødne kontroller • Bidrager til løsningsmodeller for øget informationssikkerhed
Særlige forhold	• Kommer med forslag til opdatering af kommunens informationssikkerhedsstandard og uddybende informationssikkerhedsregler • Evaluerer og benchmarker organisationens sikkerhed • Gennemfører risikovurderinger i samarbejde med systemejere • Registrerer og rapporterer kritiske hændelser • Skaber opmærksomhed om informationssikkerhed blandt organisationens medarbejdere (awareness) • Indkalder til møder og fungerer som sekretær for informationssikkerhedsgruppen • Vejleder og sparrer med de Kitos-ansvarlige samt koordinerer møder for dem • Holder sig ajour med lovgivning og eksterne sikkerhedskrav samt inkorporerer disse krav i sikkerhedsarbejdet under hensyntagen til organisatoriske forhold • Medvirker til it-revision og opfølgning herpå • Medvirker til gennemførelse af databeskyttelsesrådgiverens tilsyn med kommunens efterlevelse af regler og standarder

	• Fungerer som kommunens kontaktpunkt til den eksterne databeskyttelsesrådgiver og andre relevante eksterne samarbejdspartnere inden for informationssikkerhed
Særlige forhold	Ingen

	Koncerncheferne
Opgaver	• Er medlemmer af informaitonssikkerhedsgruppen • Sikrer formidling af informaiton og beslutninger fra informationssikkerhedsgruppen til medarbejderne inden for sit område • Sikrer generel opmærksmhed på informationssikkerhed i det daglige arbejde • Sikrer medarbejdernes deltagelse i lokale eller tværgående uddannelsesaktiviteter inden for omformationssikekrhed • Udpeger Kitos-ansvarlige
Særlige forhold	Ingen

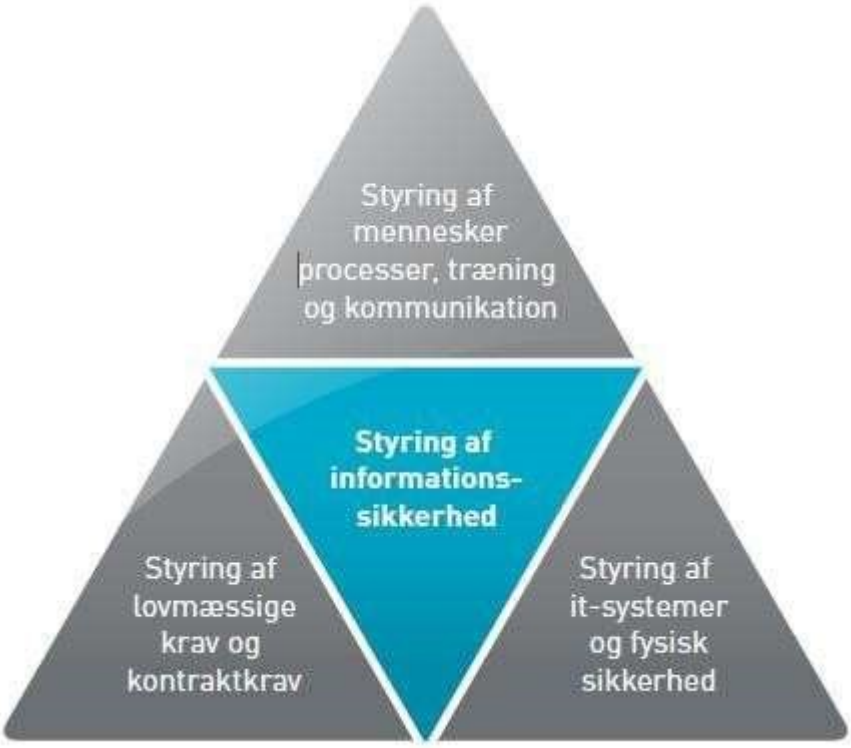
	Systemejerne
Opgaver	• Registrere alle foreskrevne oplysninger om it-systemet i Kitos • Udarbejde procedurer, retningslinjer og instrukser vedrørende systemet inden for rammerne af den sikkerhedsstandard, som topledelsen har fastlagt • Føre løbende kontrol med overholdelsen af procedurer, retningslinjer og instrukser • Indgå og forny aftaler med leverandører i samarbejde med Digitaliserings- og it-chefen • Sikre at der er indgået en databehandleraftale, hvor eksterne behandler persondata på vegne af kommunen. • Kontrollere at databehandleren fortsat overholder kravene i databehandleraftalen • Sikre at alle nødvendige oplysninger til dokumentation for efterlevelse af databeskyttelsesforordningen er registreret i SBSYS og så vidt muligt i Kitos • Autorisere brugeradgange jf. proceduren for systemet. Det skal herunder sikres, at rettighedsniveauet er i overensstemmelse med Skanderborg Kommunes generelle sikkerhedsretningslinjer • Gennemgå alle brugerprofiler mindst hver halve år for at identificere inaktive profiler eller tilsvarende, der skal fjernes eller ændres. • Sikre at brugere af systemet systematisk modtager fyldestgørende træning i brug af systemet • Sikre at der årligt foretages en risikovurdering for it-systemet i samarbejde med IT/Digitalisering og Innovation • Sikre at opdatering af anvendt software finder sted • Forhåndsgodkende, hvis data fra driftsmiljøet skal kopieres til et testmiljø • Skal have en "exit-strategi" på plads i tilfælde af leverandørers misligholdelse af aftaler • Udarbejde og vedlige passende beredskabsplaner • Instruere en evt. dataejer i, hvordan data skal håndteres i it-systemet.
Særlige forhold	Ingen

	Kitos-ansvarlige
Opgaver	• Koordinerer områdets registreringer i Kitos • Deltager i møder i gruppen for Kitos-ansvarlige • Holder sig orienteret om ændringer i Kitos
Særlige forhold	Udpeges af fag- og stabscheferne

	Medarbejderne
Opgaver	• Overholder regler og krav for informationssikkerhed og behandling af personoplysninger • Holder sig orienteret i det informationsmateriale, der stilles til rådighed og deltager i arrangementer om emnet • Opsøger aktivt afklaring af tvivlsspørgsmål • Er opmærksom på sikkerhedshændelser og melder dem til egen leder og 7-9-13 Servicedesk
Særlige forhold	Ingen

Bilag 2 metodevalg

Informationssikkerhedsreglerne er udarbejdet på baggrund af ISO 27002 med udgangspunkt i følgende agile værktøjer:



Systematisk informationssikkerhedsarbejde er en løbende proces faciliteret af en informationssikkerhedskoordinator og en it-sikkerhedskonsulent.

Kvalitetscirklen i informationssikkerhedsarbejdet

"Plan-do-check-act"-modellen anvendes i arbejdet med sikkerhed, fordi den giver en operationel tilgang til de mange procedurer og aktiviteter, som informationssikkerhedsarbejdet indeholder. Arbejdet med informationssikkerhed består af planlægning, implementering og vedligeholdelse, administration, kontrol, information og rådgivning om informationssikkerhed i organisationen.

Indsatsen skal afvejes ud fra hensynet til sikkerhed, brugervenlighed og økonomi. Det er vigtigt, at indsatsen er proportional med truslerne mod organisationen.

- Foretag risikovurdering
- Udarbejd informationssikkerhedspolitik
- Udarbejd handlingsplan
- Udarbejd Statement of Applicability (SoA)
- Få ledelsesgodkendelse af risikovurderingens resultat, SoA-dokument og informationssikkerhedspolitik

- Udarbejd/opdater sikkerhedspolitik
- Udarbejd/opdater retningslinjer
- Udarbejd/opdater beredskabsplan
- Opdater SoA-dokument
- Få ledelsesgodkendelse af sikkerhedspolitik, retningslinjer og beredskabsplan.

- Vurder og prioriter behov for ændringer i sikkerhedsarbejdet
- Opdater SoA-dokument
- Få ledelsesgodkendelse af notat med forbedringsforslag

- Gennemfør måling på sikkerhed
- Udarbejd/opdater ledelsesrapport på sikkerhed
- Opdater SoA-dokument
- Få ledelsesgodkendelse af sikkerhedsrapportering