FORRETNINGS-CIRKULÆRE FOR ORGANISERING AF INFORMATIONS-SIKKERHED

INDLEDNING

Forretningscirkulære for organisering af informationssikkerhed fastsætter de nærmere regler for ansvarsfordelingen for informationssikkerhedsarbejdet i Københavns Kommune.

Forretningscirkulæret er udarbejdet i henhold til *Informationssikkerhedsregulativet for Københavns Kommune* og kommunens vision om: "Lovlig forvaltningsvirksomhed og tryghed for borgerne og virksomhederne i mødet med Københavns Kommune."

Forretningscirkulæret er bindende og dermed obligatorisk at følge for alle enheder under Borgerrepræsentationen, herunder kommunens forvaltninger og underliggende enheder samt kommunens uafhængige enheder. Den enkelte forvaltning/enhed har overfor den administrativt ansvarlige borgmester og Økonomiudvalget ansvaret for, at forretningscirkulæret efterleves i den pågældende enhed.

Forretningscirkulæret indgår i det overordnede regelhierarki i Københavns Kommune som illustreret i figuren nedenfor.

STYRINGSDOKUMENT	STYRINGSMÆSSIGT INDHOLD	OPGAVEANSVARLIG	BESLUTNINGS-KOMPETENCE	KOMMUNIKATION
Love og bekendtgørelser	Fastsætter de overordnede rammer for kommunens drift og tilrettelæggelse af faglige og administrative opgaver.	Eksternt	Folketinget	Implementeres i interne regler og via interne orienteringsskrivelser
Styrelsesvedtægten for Københavns Kommune	Fastsætter de overordnede rammer for kommunens delegation af roller og ansvar til de stående udvalg, herunder formaliseres kommunens faglige organisering.	Borgerrepræsentationen	Borgerrepræsentationen med orientering til ekstern revision	Fælles portal + via interne orienteringsskrivelser
Informationssikkerheds-regulativet inkl. bilag samt politikker og strategier	Fastsætter rammerne for forvaltning af kommunens informationssikkerhed og it med udgangspunkt i kommunens styrelsesvedtægt.	Økonomiforvaltningen	Borgerrepræsentationen	Fælles portal + via interne orienteringsskrivelser
Fællesadministrative forretningscirkulærer	Definerer styringselementerne for kommunens administrative hovedprocesser med udgangspunkt i relevant faglig lovgivning og rammevilkårene i Informationssikkerhedsregulativet.	Økonomiforvaltningen	Økonomiudvalget	Fælles portal + via interne orienteringsskrivelser
Fællesadministrative forretningsgange	Indeholder beskrivelse og kortlægning af de processer der defineres i cirkulæret, herunder en beskrivelse af aktiviteter samt dokumentation af risikovurdering. I forretningsgangen tages også stilling til fordeling af roller og ansvar.	Økonomiforvaltningen	Økonomiforvaltningen efter koordinering med It-kredsen	Fælles portal + via interne orienteringsskrivelser
Forvaltningsspecifikke forretningsgange	Indholdet defineres i de enkelte forvaltninger under hensyn til lovgivning og andre interne styringsdokumenter.	Fagforvaltningen	Forvaltningens direktion	Fælles portal + via interne orienteringsskrivelser
Arbejdsgangs-beskrivelser, vejledninger mv.	Indeholder praktisk vejledning til udførelse af handlinger, herunder skærmprint og detailforklaring til de processer i de overliggende forretningsgange. I vejledningen uddybes beskrivelsen af roller og ansvar.	Fagforvaltningen	Ansvarlige kontorchef	Fælles portal + via interne orienteringsskrivelser

Figur 1: Regelhierarki for Københavns Kommune.

INDHOLD

Indledning 1
Kapitel 1 – Anvendelsesområde og formål 5
Kapitel 2 – Borgerrepræsentationen 5
Kapitel 3 – Økonomiudvalget 5
Kapitel 4 – Overborgmesteren og borgmestrene 6
Kapitel 5 – Chefen for Intern Revision, Databeskyttelsesrådgiveren og Borgerrådgiveren 6
Kapitel 6 – Forvaltningerne 6
Kapitel 7 – Supplerende ansvarsbestemmelser for Økonomiforvaltningen 8
Kapitel 8 – Supplerende ansvarsbestemmelser for Børne- og Ungdomsforvaltningens pædagogiske netværk 10
Kapitel 9 – Systemansvarlig chef 11
Kapitel 10 – Forretningsmæssig systemejer 11
Kapitel 11 – Teknisk systemejer 12
Kapitel 12 – Autorisationsansvarlige 13
Kapitel 13 – Ledere 13
Kapitel 14 – Alle ansatte 14
Kapitel 15 – Ikrafttrædelse og ændringer 14

KAPITEL 1 – ANVENDELSESOMRÅDE OG FORMÅL

§ 1. Forretningscirkulære for organisering af informationssikkerhed udmønter de overordnede ansvarsbeskrivelser i Informationssikkerhedsregulativet for Københavns Kommune.

§ 2. I beslutninger om informationssikkerhed skal der gennemføres en afvejning af de sikkerhedsmæssige risici op mod kommunens behov for effektivitet og høj borgerservice (risikovurdering). Dette skal bl.a. sikre, at enhver håndtering af personoplysninger og værdioplysninger i Københavns Kommune sker på en betryggende og tillidsvækkende måde i forhold til kommunens borgere og virksomheder, og at kommunen følger de regler for behandling af personoplysninger, der er fastsat i databeskyttelsesforordningen og databeskyttelsesloven.

KAPITEL 2 – BORGERREPRÆSENTATIONEN

§ 3. Borgerrepræsentationen vedtager kommunens informationssikkerhedspolitik, informationssikkerhedsregulativ og kommunens overordnede sikkerhedsniveau efter indstilling fra Økonomiforvaltningen.

Stk. 2. Informationssikkerhedspolitikken fastlægger det overordnede niveau for informationssikkerheden i kommunen.

Stk. 3. Informationssikkerhedsregulativet beskriver de overordnede rammer for kommunens håndtering af informationssikkerhedsrisici.

Stk. 4. På baggrund af kommunens samlede risikovurdering træffer Borgerrepræsentationen beslutning om fastlæggelse af det generelle sikkerhedsniveau.

KAPITEL 3 – ØKONOMIUDVALGET

§ 4. Økonomiudvalget varetager den umiddelbare forvaltning af kommunens overordnede og tværgående it- og informationssikkerhedsforhold.

Stk. 2. Økonomiudvalget er ansvarlig for at fastsætte regler for informationssikkerhed i forretningscirkulærerne i medfør af kommunens informationssikkerhedsregulativ.

Stk. 3. Gennemførelse af redaktionelle konsekvensændringer i forretningscirkulærerne, der følger af Økonomiudvalgets beslutninger, kan uden videre foretages af Koncern IT.

Stk. 4. Økonomiforvaltningen orienterer mindst én gang årligt Økonomiudvalget om sikkerhedsbrud om status på informationssikkerhedsarbejdet i kommunen samt om dispensationer fra informationssikkerhedsreglerne.

KAPITEL 4 – OVERBORGMESTEREN OG BORGMESTRENE

§ 5. Overborgmesteren og den enkelte borgmester har ansvaret for informationssikkerhedsarbejdet inden for hver deres forvaltningsområde.

KAPITEL 5 – CHEFEN FOR INTERN REVISION, DATABESKYTTELSESRÅDGIVEREN OG BORGERRÅDGIVEREN

§ 6. Medmindre andet er anført, sidestilles chefen for Intern Revision, databeskyttelsesrådgiveren og Borgerrådgiveren i nærværende forretningscirkulære med kommunens forvaltninger og er dermed underlagt de samme forpligtelser og ansvarsområder.

Stk. 2. Databeskyttelsesrådgiverens rolle og opgaver er i øvrigt fastsat i databeskyttelseslovgivningen samt i kommunens informationssikkerhedsregulativ og i forretningscirkulære for persondatabeskyttelse – dokumentation og compliance.

KAPITEL 6 – FORVALTNINGERNE

Overholdelse af regler for informationssikkerhed

§ 7. Hver forvaltning har inden for eget område, herunder i forhold til fagsystemer, ansvaret for at overholde kommunens informationssikkerhedsregler, jf. nærværende forretningscirkulære, forretningscirkulære for informationssikkerhed samt kommunens øvrige forretningscirkulærer og forretningsgange. Den enkelte forvaltning har i øvrigt ansvaret for at fastlægge informationssikkerhedsniveauet under hensyn til det aktuelle risikobillede, jf. § 17.

Stk. 2. Ansvaret for informationssikkerhedsniveauet i tværgående fagsystemer, jf. forretningscirkulære for it-anskaffelser, skal efter aftale placeres hos én af de forvaltninger, som anvender det pågældende tværgående it-system.

Stk. 3. Forvaltningerne har inden for eget område ansvaret for at sikre, at specifik lovgivning af betydning for it-sikkerheden og eksterne it-sikkerhedskrav for det pågældende område bliver identificeret, dokumenteret og overholdt.

Stk. 4. Det daglige ansvar for overholdelsen af reglerne i databeskyttelsesforordningen og tilhørende lovgivning i forbindelse med behandling af personoplysninger påhviler forvaltningerne.

Organisatoriske forhold

§ 8. Hver forvaltning har inden for eget område ansvaret for, at de medarbejdere, som arbejder med informationssikkerhedsopgaver, er i besiddelse af de nødvendige kompetencer.

Stk. 2. Hver forvaltning har ansvaret for at sikre, at medarbejdere er uddannet og instrueret i, hvordan overholdelsen af kommunens informationssikkerhedsregler konkret overholdes inden for forvaltningens eget område.

Stk. 3. Hver forvaltning har ansvaret for at sikre, at medarbejdere ikke varetager modstridende funktioner (funktionsadskillelse) på informationssikkerhedsområdet, som f.eks. systemejer og autorisationsansvarlig.

Stk. 4. Hver forvaltning har ansvaret for at udpege en GDPR-koordinator, jf. forretningscirkulære for persondatabeskyttelse – dokumentation og compliance.

Stk. 5. Forvaltningernes digitaliseringschefer deltager i det tværgående forum Digitaliseringschefkredsen.

Stk. 6. Forvaltningernes it-ansvarlige direktører deltager i det tværgående forum IT-kredsen.

Risikovurderinger og -styring

§ 9. Hver forvaltning har inden for eget forvaltningsområde ansvaret for at bistå Koncern IT med gennemførelse af risikovurderinger af it-systemer, jf. § 17.

Stk. 2. På baggrund af de foretagne risikovurderinger har hver forvaltning ansvaret for at træffe nødvendige sikkerhedsforanstaltninger med henblik på at opnå et tilstrækkeligt sikkerhedsniveau, jf. § 7, stk. 1. Forvaltningen har i den forbindelse ansvar for at forholde sig til konsekvenserne af, at et forretningsunderstøttende it-system ikke er tilgængeligt i en given periode.

Systemejerskab

§ 10. Hver forvaltning har ansvaret for, at alle it-systemer inden for eget ansvarsområde er angivet i kommunens liste over systemaktiver, at it-systemerne har gennemgået relevante vurderinger, jf. § 13, og herefter fortsat oppebærer en ibrugtagningstilladelse, også ved væsentlige ændringer.

Stk. 2. Hver forvaltning har inden for eget område ansvaret for at udpege en chef, som er ansvarlig for it-systemet og som udpeger en person med ansvar for det forretningsmæssige systemejerskab samt en person med ansvar for det tekniske systemejerskab, jf. § 21, § 22 og § 23.

Stk. 3. Det forretningsmæssige systemejerskab og det tekniske systemejerskab kan varetages af én og samme person eller flere personer i forening inden for rammerne af bestemmelserne i § 22 og 23.

Stk. 4. Hver forvaltning har ansvaret for, at der udpeges mindst én stedfortræder for hver systemejer (både forretningsmæssig og teknisk). Hvor intet andet er besluttet, er det direktionen, der er stedfortræder.

Stk. 5. Det tekniske systemejerskab kan efter aftale overlades til Koncern IT. Hvis dette sker, skal direktionen i Koncern IT udpege en teknisk systemejer samt mindst én stedfortræder. Det forretningsmæssige systemejerskab kan derimod ikke overdrages til Koncern IT.

KAPITEL 7 – SUPPLERENDE ANSVARSBESTEMMELSER FOR ØKONOMIFORVALTNINGEN

§ 11. Økonomiforvaltningen varetager det daglige ansvar for Økonomiudvalgets tværgående opgaver på it- og informationssikkerhedsområdet i kommunen.

Stk. 2. Medmindre Borgerrepræsentationen beslutter andet, fastsætter Økonomiforvaltningen endvidere niveauet for Borgerrepræsentationens eget informationssikkerhedsniveau.

Stk. 3. Økonomiforvaltningen kan delegere varetagelsen af tværgående opgaver på it- og informationssikkerhedsområdet til enheder inden for egen forvaltning.

Koncern IT – Informationssikkerhedsregler

§ 12. Koncern IT har ansvaret for, at der fastsættes regler for informationssikkerhed for kommunen.

Stk. 2. Koncern IT kan give dispensation fra regler fastsat i medfør af nærværende forretningscirkulære og de øvrige forretningscirkulærer under Informationssikkerhedsregulativet, medmindre den pågældende regel af fastlagt ved lov.

Koncern IT – Anskaffelse og ibrugtagning

§ 13. Koncern IT har ansvar for at vurdere alle it-systemer, der meldes ind i kommunens systemregister. De nærmere regler herfor er beskrevet i forretningscirkulære for it-anskaffelser.

Koncern IT – Drift mv.

§ 14. Koncern IT har ansvaret for driften af generiske administrative it-systemer, jf. forretningscirkulære for it-anskaffelser, samt for kommunens netværk, herunder netværksudstyr og servere mv. I tilknytning hertil har Koncern IT ansvaret for at opretholde et passende informationssikkerhedsniveau for såvel it-systemer som netværket, jf. nærværende forretningscirkulære, forretningscirkulære for informationssikkerhed samt kommunens øvrige forretningscirkulærer og forretningsgange.

Stk. 2. Koncern IT kan lukke et ibrugtaget it-system, som en forvaltning er ansvarlig for, hvis en sikkerhedshændelse i tilknytning til it-systemet medfører, at andre it-systemer og/eller den fælles infrastruktur lider skade. Hvis der er uenighed om beslutningen, følger eskalationen kommunens normale beslutningsveje (evt. ved forelæggelse for It-kredsen) og med endelig beslutning i Økonomiudvalget.

Stk. 3. Koncern IT har ansvaret for at fastsætte retningslinjer for integration og netværkskommunikation mellem it-systemer og andre it-løsninger.

Stk. 4. Inden Koncern IT træffer beslutninger vedrørende netværk, som kan påvirke sikkerheden i det pædagogiske netværk, skal Børne- og Ungdomsforvaltningen høres.

Stk. 5. Koncern IT har ansvaret for at udpege en systemansvarlig chef, som videre har ansvaret for at udpege en forretningsmæssig systemejer og en teknisk systemejer, jf. § 21, § 22 og § 23, for hvert af de generiske administrative it-systemer, som Koncern IT er ansvarlig for.

Stk. 6. Koncern IT har ansvaret for, at der udpeges mindst én stedfortræder for hver systemejer (både forretningsmæssig og teknisk) på kommunens generiske administrative it-systemer. Hvor intet andet er besluttet, er det direktionen, der er stedfortræder.

Stk. 7. Koncern IT har ansvaret for it-sikkerheden på standardydelser fra Koncern IT's servicekatalog.

Stk. 8. Koncern IT skal sikre, at der til enhver tid findes en ajourført fortegnelse over alle væsentlige it-aktiver, der er nødvendige for driften af kommunens tværgående infrastruktur.

Stk. 9. Koncern IT har ansvar for at yde rådgivning, udarbejde informationsmateriale om kommunens overordnede informationssikkerhedsregler og for at afholde kurser med henblik på uddannelse af de forretningsmæssige og tekniske systemejere.

Koncern IT – Monitorering mv.

§ 15. Koncern IT har ansvaret for monitorering af kommunens it-systemer og netværk.

Stk. 2. Koncern IT har ansvaret for at logge drifts- og sikkerhedsrelevante aktiviteter på kommunens netværk.

Stk. 3. Koncern IT har ansvaret for at udføre efterforskningsarbejde ved sikkerhedshændelser og persondatabrud på generiske administrative it-systemer og kommunens infrastruktur.

Stk. 4. Koncern IT kan udføre undersøgelser og kontrol af drifts- og sikkerhedstilstanden af kommunens it-systemer og netværk, herunder udføre sårbarhedsscanninger og penetrationstest.

Stk. 5. Koncern IT kan bistå ved udtræk af lograpporter på de it-systemer, hvor KIT er ansvarlig for driften, i forbindelse med bl.a. personalesager, stikprøvekontroller, ledelsestilsyn mv.

Koncern IT – Tilsyn og revision

§ 16. Koncern IT fører tilsyn med overholdelsen af kommunens informationssikkerhedsbestemmelser.

Stk. 2. Koncern IT skal kontrollere opbygningen af og anvendelsen af især infrastruktur/netværk.

Stk. 3. Koncern IT kan fra forvaltningerne, medarbejdere og eksterne parter, der løser opgaver for kommunen, forlange oplysninger om forhold, der har betydning for varetagelsen af tilsynet med informationssikkerheden i kommunen.

Stk. 4. Koncern IT kan udstede påbud til forvaltningerne med henblik på, at kommunens regler for informationssikkerhed overholdes.

Stk. 5. Som led i den almindelige revision af kommunen skal der foretages revision af informationssikkerheden. Koncern IT aftaler med revisor, hvorledes revisionen skal udføres.

Koncern IT - Risikovurderinger

§ 17. Koncern IT har – med bistand fra kommunens forvaltninger – ansvaret for at gennemføre risikovurderinger af kommunens it-systemer med henblik på, at forvaltningerne kan træffe beslutning om sikkerhedsniveauet inden for egen forvaltning, jf. § 7, stk. 1.

Stk. 2. Koncern IT har ansvaret for at udarbejde værktøjer til risikovurderinger.

Stk. 3. Koncern IT har ansvaret for at yde rådgivning til forvaltningerne med henblik på håndtering af identificerede risici.

Stk. 4. På baggrund af de respektive risikovurderinger har Koncern IT ansvaret for at udarbejde en samlet risikovurdering for kommunen. Risikovurderingen skal være udarbejdet inden udgangen af 1. kvartal i hvert lige år.

Koncern IT – Beredskab

§ 18. Koncern IT har ansvaret for at fastlægge den overordnede it-beredskabsplan for kommunen.

Stk. 2. Koncern IT har ansvaret for, at der foreligger procedurer, der sikrer en tværorganisatorisk styring af it-beredskabet i tilfælde af større it-nedbrud mv.

Koncern IT - Brugeradministrationen og brugersupport

§ 19. Koncern IT har ansvaret for at varetage opgaver i forbindelse med brugeradministration og brugersupport.

Stk. 2. Koncern IT har ansvaret for at udarbejde procedurer for tildeling af rettigheder til it-systemer, herunder for hvordan en brugers identitet fastslås, før en ny adgangskode udleveres, og for hvordan udleveringen skal ske.

Stk. 3. Koncern IT kan uddelegere ansvaret for tildeling og nulstilling af adgangskoder i specifikke it-systemer til forvaltningerne efter dispensation.

Stk. 4. Koncern IT har ansvaret for at gennemføre oprettelser, flytninger, ændringer og sletninger af it-brugere samt autorisationer til robotter, algoritmer og andre automatiserede løsninger på baggrund af bestillinger fra den autorisationsansvarlige.

KAPITEL 8 – SUPPLERENDE ANSVARSBESTEMMELSER FOR BØRNE- OG UNGDOMSFORVALTNINGENS PÆDAGOGISKE NETVÆRK

§ 20. Børne- og Ungdomsforvaltningen har ansvaret for driften af det pædagogiske netværk, herunder netværksudstyr og servere mv. og for de it-systemer, der afvikles på dette netværk, samt i tilknytning hertil for at opretholde et passende informationssikkerhedsniveau for netværket og it-systemer, jf. nærværende forretningscirkulære, forretningscirkulære for informationssikkerhed samt kommunens øvrige forretningscirkulærer og forretningsgange.

Stk. 2. Inden Børne- og Ungdomsforvaltningen træffer beslutninger vedrørende egne netværk, som kan påvirke sikkerheden i kommunens fælles netværk, skal Koncern IT høres.

Stk. 3. Børne- og Ungdomsforvaltningen kan delegere varetagelsen af driften af det pædagogiske netværk, herunder varetagelsen af informationssikkerheden, til en driftsansvarlig enhed inden for egen forvaltning.

KAPITEL 9 – SYSTEMANSVARLIG CHEF

§ 21. Den systemansvarlige chef har ansvar for at udpege og placere en forretningsmæssig og teknisk systemejer for det it-system, vedkommende er ansvarlig for.

Stk. 2 Den systemansvarlige chef har ansvar for at sikre, at den forretningsmæssige systemejer og tekniske systemejer løfter alle opgaver beskrevet i § 22 og § 23 og i øvrige relevante forretningscirkulærer, for de it-systemer vedkommende har ansvar for.

Stk. 3. Den systemansvarlige chef har ansvar for at sikre sammenhæng mellem den overordnede styring af den samlede it-systemportefølje over væsentlige it-systemer og den konkrete varetagelse af opgaver og ansvarsområder i det pågældende it-system.

KAPITEL 10 – FORRETNINGSMÆSSIG SYSTEMEJER

§ 22. Forvaltningen har ansvaret for at udpege en person til at varetage følgende opgaver:

1) at holde sig orienteret i kommunens og forvaltningsspecifikke regelsæt
2) at indgå i relevante faglige fællesskaber omkring systemejerrollen
3) at have indsigt i eventuelle særlige lovkrav for det pågældende forvaltningsområde, som kan have indflydelse på de krav, der stilles til it-systemet
4) at have indsigt i hjemmelsgrundlaget for de oplysninger, som behandles i it-systemet
5) at it-systemet ikke indeholder oplysninger, som der ikke er hjemmel til at behandle, eller som skulle have været slettet
6) at roller og rettigheder er beskrevet i forhold til brugeradministrationen i it-systemet
7) at der indgås nødvendige databehandleraftaler og tavshedspligtserklæringer
8) at der foretages nødvendige konsekvensanalyser i overensstemmelse med forretningscirkulære for persondatabeskyttelse – dokumentation og compliance, hvis registreringen og anvendelsen af data ændrer sig
9) at der i samarbejde med den behandlingsprocesansvarlige og datastrømsansvarlige, jf. forretningscirkulære for persondatabeskyttelse – dokumentation og compliance, foretages registreringer i det it-system, som Databeskyttelsesrådgiveren stiller til rådighed for registrering af dataprocesser mv.
10) at have indsigt i forvaltningens udviklingsønsker til det pågældende it-system og bistå den tekniske systemejer, så it-systemets funktionalitet løbende tilpasses og understøtter kommunens behov
11) at styre økonomi for it-systemet i henhold til forretningsbehov
12) at sikre, at der sker kontrol af dataoverførsler fra fagsystemer til økonomisystemer for at sikre et korrekt regnskab

13) at sikre, at den indgåede kontrakt indsendes til Koncern IT, og at der følges op på leverandørers opfyldelse af krav
14) at samarbejde med den tekniske systemejer om en sikker og effektiv udfasning af et it-system ved at varetage den forretningsmæssige side af udfasningen, herunder ansvar for at overholde regler vedr. databeskyttelse samt opbevaring af it-systemets logs efter udfasning
15) at godkende overtagelsesprøve fra leverandøren i forbindelse med udvikling og ændring af it-systemer
16) at fungere som kontaktperson mellem Koncern IT og kommunens brugere af it-systemet

Stk. 2. Ansvaret for udførelsen af de i stk. 1, nr. 1-16, nævnte opgaver kan overlades til flere personer og enheder inden for egen forvaltning. I så fald skal den ansvarlige person som supplement til sin rolle som kontaktperson, jf. stk.1, nr. 16, også fungere som kontaktperson til disse personer og enheder.

Stk. 3. For at varetage opgaven som forretningsmæssig systemejer på henholdsvis generiske administrative it-systemer, infrastruktur, tværgående fagsystemer og fagsystemer skal det i § 14, stk. 9, omtalte kursus være gennemført. Se forretningscirkulære for it-anskaffelser for definitioner på ovenstående.

KAPITEL 11 – TEKNISK SYSTEMEJER

§ 23. Den tekniske systemejer har ansvaret for at varetage følgende opgaver:

1) at holde sig orienteret i kommunens og forvaltningsspecifikke regelsæt
2) at indgå i relevante faglige fællesskaber omkring systemejerrollen
3) at sikre, at systemfunktionalitet og -anvendelse løbende tilpasses og bedst muligt understøtter informationssikkerhedskravene samt forretnings- og brugerbehov
4) at enhver ændring, der har snitflader til og/eller deling af ressourcer med Koncern IT eller kommunens øvrige netværk, skal ske efter Koncern IT's procedurer for ændring af it-systemer (change)
5) at der er etableret procedurer, der sikrer it-systemet en stabil, effektiv og sikker drift, og at disse er løbende dokumenteret
6) at der er indgået aftale om it-beredskabet efter de kriterier og retningslinjer, der er fastlagt i kommunens informationssikkerhedsregler
7) at der i relevant omfang kan foretages maskinel logning, når det kræves af lovgivning og/eller kommunens egne regler
8) at der sker test inden migrering fra udvikling til produktion for at sikre det ønskede drifts- og it-sikkerhedsniveau
9) at dokumentationen af it-systemer og processer er ajourført og tilgængelig for relevante medarbejdere
10) at kunne forelægge retvisende og opdateret dokumentation for tildelte autorisationer i det givne it-system
11) at bistå med systemteknisk viden i forhold til udførelsen af det forretningsmæssige systemejerskab jf. § 22
12) at understøtte den forretningsmæssige budgetstyring af it-systemet ved at identificere kommende og nødvendige tekniske investeringsbehov for it-systemet
13) at registreringen af it-systemet i kommunens liste over it-systemaktiver, jf. § 10, stk. 1, til stadighed er retvisende

14) at samarbejde med den forretningsmæssige systemejer om en sikker og effektiv udfasning af et it-system ved at varetage den tekniske side af udfasningen, herunder opsigelse af infrastruktur-komponenter.

Stk. 2. For at varetage opgaven som teknisk systemejer på henholdsvis generiske administrative it-systemer, infrastruktur, tværgående fagsystemer og fagsystemer skal det i § 14, stk. 9, omtalte kursus være gennemført. Se forretningscirkulære for it-anskaffelser for definitioner på ovenstående.

KAPITEL 12 – AUTORISATIONSANSVARLIGE

§ 24. Den autorisationsansvarlige varetager de opgaver, der er uddelegeret fra nærmeste leder i forbindelse med bestilling og afbestilling af autorisationer og rettigheder til medarbejdere. Hvis der ikke er udpeget en autorisationsansvarlig, varetages opgaven af nærmeste leder.

Stk. 2. Den autorisationsansvarlige varetager bestillingen af oprettelser, flytninger, ændringer og sletninger af autorisationer for medarbejdere og eksterne konsulenter hos Koncern IT. Den autorisationsansvarliges leder har ansvaret for, at rettighederne til stadighed afspejler medarbejdernes arbejdsmæssige behov.

KAPITEL 13 – LEDERE

§ 25. Ledere skal på alle niveauer sikre, at det er muligt for medarbejderne at efterleve deres ansvar for at beskytte kommunens person- og værdioplysninger. Den personaleansvarlige leder er ansvarlig for, at medarbejderen fra ansættelsens start og gennem hele ansættelsesforholdet er informeret om sine opgaver og ansvar i forhold til informationssikkerheden.

Stk. 2. Den personaleansvarlige leder har ansvar for, at autorisationer til kommunens it-systemer tildeles korrekt og til enhver tid svarer til det behov for adgang til data, som den enkelte medarbejder har i forhold til opgaveløsningen. Dette gælder også ved omplacering af medarbejdere.

Stk. 3. Medarbejderens personaleansvarlige leder sikrer, at medarbejderen senest ved ansættelsesforholdets ophør afleverer it-udstyr og lignende, som tilhører kommunen, og at der sker inddragelse af medarbejderes adgangsrettigheder i henhold til kommunens procedurer.

Stk. 4. Medarbejderens personaleansvarlige leder skal orientere medarbejderen om tavshedspligtens indhold, og at tavshedspligten er gældende også efter ansættelsesforholdets ophør.

Stk. 5. En leder, der er ansvarlig for en omstrukturering, skal i god tid sørge for at sikre, at der etableres de nødvendige elektroniske kommunikationstiltag. Eksempelvis skal kontorpostkasser, sikre postkasser m.m. lukkes, hvis en enhed ophører.

Stk. 6. Den lokale ledelse har inden for eget område ansvaret for, at der etableres en tilstrækkelig fysisk sikring af lokaler, aktiver mv.

KAPITEL 14 – ALLE ANSATTE

§ 26. Alle medarbejderne skal medvirke til at beskytte kommunens person- og værdioplysninger og skal agere i henhold til kommunens informationssikkerhedsregler. Dette gælder også politikere, leverandører og eksterne samarbejdspartnere, der i forbindelse med kontakten til kommunen får adgang til kommunens data.

KAPITEL 15 – IKRAFTTRÆDELSE OG ÆNDRINGER

§ 27. Forretningscirkulære for organisering af informationssikkerhed træder i kraft fra godkendelsen i Økonomiudvalget.

Stk. 2. Forslag til ændringer af forretningscirkulæret forelægges af Økonomiforvaltningen for Økonomiudvalget til godkendelse.

Stk. 3. Redaktionelle ændringer, som ikke indebærer egentlige ændringer i forretningscirkulæret, kan godkendes af Økonomiforvaltningens direktion. Tilsvarende gælder ændringer, der som følge af Borgerrepræsentationens og Økonomiudvalgets beslutninger måtte indebære konsekvensrettelser i forretningscirkulæret.

Forretningscirkulære for organisering af informationssikkerhed