FORRETNINGS-CIRKULÆRE FOR ORGANISERING AF INFORMATIONS-SIKKERHED

FORRETNINGSCIRKULÆRE FOR ORGANISERING AF INFORMATIONSSIKKERHED

Forretningscirkulæret for organisering af informationssikkerhed i Københavns Kommune er udarbejdet i henhold til Informationssikkerhedsregulativet for Københavns Kommune. I forretningscirkulæret fastsættes de nærmere regler for ansvarsfordelingen for informationssikkerhedsarbejdet i kommunen.

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
Fællesadministratve 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

KAPITEL 1 – ANVENDELSESOMRÅDE OG FORMÅL

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

§ 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 en 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. Med mindre 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 underliggende forretningscirkulærer.

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 cirkulære, Forretningscirkulære for informationssikkerhed samt kommunens øvrige cirkulærer 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. Forretningscirkulærer for it-anskaffelser, skal efter aftale placeres hos én af de forvaltninger, som anvender det pågældende tværgående 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 DPO Business Partner, jf. Forretningscirkulære for persondata – dokumentation og compliance.

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

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 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 it-systemaktiver, at systemerne har gennemgået en vurdering, 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 ansvarlig person med et forretningsrelateret systemansvar samt en ansvarlig person for det tekniske systemejerskab, jf. §§ 21 og 22.

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 §§ 21 og 22.

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. Med mindre 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 informations-sikkerhed for kommunen.

Stk. 2. Koncern IT kan meddele dispensation fra regler fastsat i medfør af nærværende cirkulære, Forretningscirkulære for informationssikkerhed og Forretningscirkulære for it-anskaffelse.

Koncern IT – Anskaffelse og ibrugtagning

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

Koncern IT – Drift mv.

§ 14. Koncern IT har ansvaret for driften af generiske administrative systemer, jf. Forretningscirkulærer 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 systemer som netværket, jf. nærværende cirkulære, Forretningscirkulære for informationssikkerhed samt kommunens øvrige cirkulærer og forretningsgange.

Stk. 2. Koncern IT kan lukke et ibrugtaget system, som en forvaltning er ansvarlig for, hvis en sikkerhedshændelse i tilknytning til systemet medfører, at andre 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 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 forretningssystemejer og en teknisk systemejer, jf. §§ 21 og 22, for hvert af de generiske administrative 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). 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 og udarbejder informationsmateriale om kommunens overordnede informationssikkerhedsregler og for at afholde kurser med henblik på uddannelse af de tekniske systemejere.

Koncern IT – Monitorering mv.

§ 15. Koncern IT har ansvaret for monitorering af kommunens 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.

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

Stk. 5. Koncern IT kan bistå ved udtræk af lograpporter ved logopfølgning 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 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 brug for 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 brugeradministrationen og brugersupport.

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

Stk. 3. Koncern IT kan dog uddelegere ansvaret for tildeling og nulstilling af kodeord i specifikke systemer til forvaltningerne efter nærmere aftale.

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 systemer, der afvikles på dette netværk, samt i tilknytning hertil for at opretholde et passende informationssikkerhedsniveau for netværket og systemer, jf. nærværende cirkulære, Forretningscirkulære for informationssikkerhed samt kommunens øvrige cirkulærer 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 – FORRETNINGSRELATERET SYSTEMANSVAR

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

1) at have indsigt i eventuelle særlige lovkrav for det pågældende forvaltningsområde, som kan have indflydelse på de krav, der stilles til systemet
2) at have indsigt i hjemmelsgrundlaget for de oplysninger, som behandles i systemet
3) at systemet ikke indeholder oplysninger, som der ikke er hjemmel til at behandle, eller som skulle have været slettet
4) at der indgås eventuelt nødvendige databehandleraftaler og fortrolighedserklæringer
5) at der foretages eventuelt nødvendige konsekvensanalyser i overensstemmelse med Forretningscirkulære for persondata – dokumentation og compliance, hvis registreringen og anvendelsen af data ændrer sig
6) at der i samarbejde med den behandlingsprocesansvarlige og datastrømsansvarlige, jf. Forretningscirkulære for persondata – dokumentation og compliance, foretages registreringer i det system, som Databeskyttelsesrådgiveren stiller til rådighed for registrering af dataprocesser mv.
7) at have indsigt i forvaltningens udviklingsønsker til det pågældende system og bistå den tekniske systemejer, så systemets funktionalitet løbende tilpasses og understøtter kommunens behov
8) at godkende overtagelsesprøve fra leverandøren i forbindelse udvikling og ændring af systemer
9) at fungere som kontaktperson mellem Koncern IT og kommunens brugere af systemet.

Stk. 2. Ansvaret for udførelsen af de i stk. 1, nr. 1-7, 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. 9, også fungere som kontaktperson til disse personer og enheder.

KAPITEL 10 – TEKNISK SYSTEMEJER

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

1) at sikre, at systemfunktionalitet og -anvendelse løbende tilpasses og bedst muligt understøtter informationssikkerhedskravene samt forretnings- og brugerbehov
2) 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)
3) at der er etableret procedurer, der sikrer systemet en stabil, effektiv og sikker drift, og at disse er løbende dokumenteret
4) at der er indgået aftale om it-beredskabet efter de kriterier og retningslinjer, der er fastlagt i kommunens informationssikkerhedsregler
5) at der i relevant omfang kan foretages maskinel logning, når det kræves af lovgivning og/eller kommunens egne regler
6) at roller og rettigheder er beskrevet i forhold til brugeradministrationen i systemet
7) at der sker test inden migrering fra udvikling til produktion for at sikre det ønskede drifts- og it-sikkerhedsniveau

8) at dokumentationen af systemer og processer er ajourført og tilgængelig for relevante medarbejdere
9) at bistå med systemteknisk viden i forhold til udførelsen af det forretningsrelaterede systemansvar, jf. § 21.
10) at registreringen af systemet i kommunens liste over it-systemaktiver, jf. § 10, stk. 1, til stadighed er retvisende.

Stk. 2. For at varetage opgaven som teknisk systemejer skal det i § 14, stk. 9, omtalte kursus være gennemført.

KAPITEL 11 – AUTORISATIONSANSVARLIGE

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

Stk. 2. Den autorisationsansvarlige har ansvaret for at bestille oprettelser, flytning, ændringer og sletninger af autorisationer for medarbejdere, robotter, algoritmer og andre automatiserede løsninger hos Koncern IT således, at rettighederne til stadighed afspejler medarbejdernes arbejdsmæssige behov.

KAPITEL 12 – LEDERE

§ 24. 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 kommunes 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 procedure.

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 13 – ALLE ANSATTE

§ 25. 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 14 – IKRAFTTRÆDELSE OG ÆNDRINGER

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

Stk. 2. Ændringer i Forretningscirkulære for organisering af informationssikkerhed skal godkendes af Økonomiudvalget.

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

Forretningscirkulære for organisering af informationssikkerhed