Regulativ for
it-sikkerhed i
Københavns Kommune

Indholdsfortegnelse

I medfør af § 5 i Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning, samt i medfør af ledelsesretten udsteder Københavns Kommune følgende it-sikkerhedsregulativ for Københavns Kommune:

Kapitel 1

Regulativets anvendelsesområde og formål

§ 1. It-sikkerhedsregulativet gælder for behandling af personoplysninger og værdioplysninger i Københavns Kommune, som helt eller delvis foretages ved hjælp af elektronisk databehandling, og for ikke-elektronisk databehandling af personoplysninger, der er eller vil blive indeholdt i et manuelt register.
Stk. 2. Det skal aftales med de selvejende og private institutioner mv., der har indgået driftsoverenskomst med kommunen, eller som kommunen udfører behandlinger for, at disse skal efterleve it-sikkerhedsregulativet.

§ 2. Formålet med it-sikkerhedsregulativet er navnlig at sikre, at enhver elektronisk 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 overholder de regler for behandling af personoplysninger, der er fastsat i lov om behandling af personoplysninger (persondataloven) med tilhørende bekendtgørelser mv.

Kapitel 2

Definitioner

§ 3. I it-sikkerhedsregulativet anvendes definitionerne i persondatalovens § 3. Herudover anvendes der følgende definitioner:

Beredskabsplan	Beredskabsplanen for Københavns Kommune.
Driftsmiljø	It-miljø af en eller flere servere, som afvikler applikationer. Miljøet kan være opdelt i flere miljøer til test, udvikling, produktion, uddannelse mv.
Fjernarbejdsplads	Ved fjernarbejdsplads forstås en permanent arbejdsplads uden for kommunens ejendomme, hvorfra medarbejderen kan udføre sit arbejde via en netværksforbindelse.
Fremmede netværk	Netværk, herunder trådløse, som ikke administreres og kontrolleres af kommunen.
Fællessystem	Et it-system, der som udgangspunkt anvendes af samtlige forvaltninger, f.eks. eDoc, KØR og Exchange.
Inddata	Papirbaseret eller elektronisk grundmateriale, hvorfra personoplysninger hentes til videre elektronisk databehandling med undtagelse af papirer fra papirbaserede sager.
Informationsaktiver	Omfatter databaser, registre, it-systemer, applikationer, filer, systemdokumentation, forretningsgange, driftsplaner, beredskabsplaner, nødplaner eller kontrakter.

It-ansvarlig	Ledende medarbejder i Koncernservice, der har ansvar for opbygning og anvendelse af it-driftsmiljø og kommunikationsforbindelser samt for de fysiske sikringsforanstaltninger inden for eget område og i forhold til kommunens netværk, netværksudstyr og servere m.v., som ejes af Koncernservice. Såfremt opbygning og anvendelse af it-driftsmiljø og kommunikationsforbindelser vedrører egne netværk i Børne- og Ungdomsforvaltningen henholdsvis Brandvæsnet, er den it-ansvarlige en ledende medarbejder fra Børne- og Ungdomsforvaltningen henholdsvis Brandvæsnet, som har ansvaret herfor.
It-beredskabsplan	Plan for iværksættelse af nødplaner, reetablering af it-systemer og begrænsning af skadevirkninger i tilfælde af større it-nedbrud mv.
It-platform	En it-teknisk platform, som skal understøtte et it-miljø. Begrebet benyttes til at angive forudsætningerne for, at en given applikation kan afvikles. Omfatter både programmel og maskinel.
It-sikkerhedsforskrift	Beskrivelse af sikkerhedsforanstaltninger for de enkelte it-installationer/anlæg.
It-sikkerhedsfunktion	Alle de personer og enheder, som har en funktion i relation til it-sikkerhedsarbejdet, jf. kapitel 3.
It-sikkerhedshandlingsplan	Plan for udmøntning af it-sikkerhedspolitikken og it-sikkerhedsregulativet i praksis.
It-sikkerhedsinstruks	Eventuel instruks fastsat af it-sikkerhedslederen til supplement af it-sikkerhedsregulativet.
It-sikkerhedsleder	Medarbejder, der inden for eget område fører tilsyn med, at it-sikkerhedsarbejdet bliver udført i overensstemmelse med de til enhver tid gældende it-sikkerhedsbestemmelser.
It-sikkerhedsregulativet	Regulativ for it-sikkerhed i Københavns Kommune udstedt i medfør af § 5 i Sikkerhedsbekendtgørelsen og ledelsesretten.
It-sikkerhedspolitik	Den af Borgerrepræsentationen vedtagne politik for kommunens it-sikkerhed.
It-system	System bestående af et antal sammenhængende it-baserede funktioner (applikationer, programmer, registre og data) med tilhørende automatiske og manuelle it-behandlingsprocesser og med bestemte relationer herimellem på et givent område.
It-udstyr	Udstyr og netværk, der indgår i en it-løsning.

Kommunen	Københavns Kommune.
Kommunens ejendomme	De af kommunen ejede, lejede eller benyttede ejendomme og lokationer.
Medarbejdere	Medarbejdere i kommunen og virksomheder, der er brugere af kommunens it-systemer, medarbejdere i selvejende og private institutioner og virksomheder, hvor dette er aftalt, medarbejdere i eksterne virksomheder, der er vikarer eller udfører it-opgaver for kommunen, og hvor adgangen til kommunens it-systemer er aftalt, samt medlemmer af Borgerrepræsentationen.
Mobilt it-udstyr	Ved mobilt it-udstyr forstås it-udstyr, der kan anvendes til lagring af data og / eller kommunikation med kommunens netværk, uden at denne anvendelse nødvendigvis er bundet til en bestemt lokation, eksempelvis PDA'er, bærbare pc'er, mobiltelefoner og usb-nøgler.
Persondataloven	Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.
Sikkerhedsbekendtgørelsen	Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning med senere ændringer.
Sikre områder	Krydsfelter, serverrum og andre områder, hvor der er it-udstyr, som kræver særlig sikkerhed, og hvor der er truffet beslutning om, at området skal være sikkert område.
Systemejer	Medarbejder, der har ansvar for det pågældende it-systems sikkerhedsløsning, opbygning og anvendelse.
Uddata	Resultatet af en elektronisk databehandling, som foreligger i elektronisk eller papirbaseret form.
Værdioplysninger	Oplysninger, der har en væsentlig økonomisk eller forvaltningsmæssig betydning for kommunen.
Væsentlige informationsaktiver	Aktiver, der indeholder fortrolige eller følsomme personoplysninger eller værdioplysninger.

Kapitel 3

Interne organisatoriske forhold

Borgerrepræsentationen

§ 4. Borgerrepræsentationen vedtager kommunens it-sikkerhedsregulativ og it-sikkerhedspolitik.

Stk. 2. It-sikkerhedspolitikken skal beskrive det overordnede it-sikkerhedsniveau, de organisatoriske rammer for kommunens håndtering af it-sikkerhedsrisici og de overordnede retningslinier for udformningen af it-sikkerheds- og kontrolforanstaltninger.
Stk. 3. It-sikkerhedspolitikken skal revurderes mindst hvert 2. år. Resultatet heraf skal godkendes af Borgerrepræsentationen efter indstilling fra Borgerrepræsentationens Sekretariat og Økonomiudvalget.

Økonomiudvalget

§ 5. Økonomiudvalget fører det overordnede tilsyn med kommunens it-sikkerhed og koordinerer it-sikkerhedsarbejdet i kommunen.

§ 6. En forvaltnings fravigelser fra it-sikkerhedsregulativet kan kun ske på baggrund af en godkendelse fra Økonomiudvalget og efter forudgående høring af Borgerrepræsentationens Sekretariat.
Stk. 2. Borgerrepræsentationens Sekretariat fører en fortegnelse over Økonomiudvalgets beslutninger om fravigelser fra it-sikkerhedsregulativet og orienterer årligt udvalget for it-sikkerhed herom.

Borgerrepræsentationens Sekretariat

§ 7. Borgerrepræsentationens Sekretariat fører det daglige tilsyn med overholdelsen af kommunens it-sikkerhedsbestemmelser og koordinerer kommunens it-sikkerhedsarbejde på vegne af Økonomiudvalget.
Stk. 2. Borgerrepræsentationens Sekretariat kan træffe beslutning om principielle it-sikkerhedsmæssige spørgsmål. Dette sker som udgangspunkt efter indstilling fra it-sikkerhedslederen for det område, som spørgsmålet vedrører.
Stk. 3. Borgerrepræsentationens Sekretariat tilrettelægger informations- og uddannelsesaktiviteter for medarbejdere, der varetager kommunens it-sikkerhedsfunktioner.
Stk. 4. Borgerrepræsentationens Sekretariat rådgiver kommunen om it-sikkerhedsmæssige forhold.
Stk. 5. Borgerrepræsentationens Sekretariat kan afkræve enhver medarbejder i kommunen oplysninger, som har betydning for varetagelsen af tilsynsfunktionen.

Overborgmesteren og borgmestrene

§ 8. Overborgmesteren og den enkelte borgmester har ansvaret for it-sikkerhedsarbejdet inden for hver deres forvaltningsområde.

§ 9. Overborgmesteren og de enkelte borgmestre udpeger inden for eget forvaltningsområde en eller flere it-sikkerhedsledere samt mindst en stedfortræder for hver it-sikkerhedsleder.
Stk. 2. Kompetencen til at udpege it-sikkerhedsledere og stedfortrædere kan delegeres til den administrerende direktør.

Direktionerne

§ 10. Direktionen har inden for eget forvaltningsområde ansvar for fastlæggelse af it-sikkerhedsniveauet og for gennemførelse af risikovurderinger. It-sikkerhedsniveauet skal fastlægges under hensyntagen til kommunens overordnede it-sikkerhedsniveau.
Stk. 2. Direktionen for Koncernservice har ansvar for fastlæggelse af it-sikkerhedsniveauet inden for eget område og i forhold til kommunens netværk samt netværksudstyr og servere m.v., som ejes af Koncernservice. Som led i fastlæggelsen af it-sikkerhedsniveauet har di-

rektionen ansvar for gennemførelse af risikovurderinger. It-sikkerhedsniveauet skal fastlægges under hensyntagen til kommunens overordnede it-sikkerhedsniveau.
S*tk. 3.* Direktionen skal inden for eget område iværksætte de foranstaltninger, der er nødvendige for at opnå en tilstrækkelig it-sikkerhed.
Stk. 4. Direktionen er inden for eget område ansvarlig for, at medarbejdere, som varetager it-sikkerhedsfunktioner, er i besiddelse af de nødvendige kompetencer.
Stk. 5. Direktionen udpeger inden for eget område en systemejer for hvert it-system samt mindst en stedfortræder for hver systemejer. Systemejerskabet skal varetages inden for den forvaltning, som i medfør af styrelsesvedtægten skal løse den faglige opgave, som it-systemet skal understøtte.
Stk. 6. Direktionen for Koncernservice skal udpege en systemejer for hvert af de fællessystemer, som Koncernservice er ansvarlig for.
Stk. 7. Direktionen for Koncernservice skal udpege en it-ansvarlig samt mindst en stedfortræder for denne.
Stk. 8. Direktionen for Børne- og Ungdomsforvaltningen kan udpege en it-ansvarlig samt en stedfortræder for denne for forvaltningens eget netværk, netværksudstyr og servere m.v.
Stk. 9. Ledelsen for Brandvæsnet kan udpege en it-ansvarlig samt en stedfortræder for denne for Brandvæsnets eget netværk, netværksudstyr og servere m.v.
Stk. 10. Den it-ansvarlige skal være en ledende medarbejder med tilknytning til den strategiske ledelse.

Revisionsdirektoratet

§ 11. Direktøren for Revisionsdirektoratet er it-sikkerhedsleder for Revisionsdirektoratet.

Borgerrådgiveren

§ 12. Borgerrådgiveren er it-sikkerhedsleder for Borgerrådgiverinstitutionen.

It-sikkerhedsledere

§ 13. It-sikkerhedslederen fører inden for eget område tilsyn med de øvrige it-sikkerhedsfunktioner, og med at it-sikkerhedsarbejdet, herunder arbejdet med den fysiske sikkerhed, bliver udført i overensstemmelse med de til enhver tid gældende it-sikkerhedsbestemmelser.
Stk. 2. It-sikkerhedslederen kontrollerer løbende inden for eget område alle adgangsrettigheder og autorisationer, der er givet til medarbejderne.
Stk. 3. It-sikkerhedslederen kan afkræve Koncernservice oplysninger, som har betydning for varetagelsen af tilsynsfunktionen.
Stk. 4. Beslutninger, som vedrører Koncernservice, kan kun træffes efter forudgående høring af Koncernservice.
Stk. 5. It-sikkerhedslederen rådgiver inden for eget område om it-sikkerhedsmæssige forhold og tilrettelægger informations- og uddannelsesaktiviteter om it-sikkerhed for områdets medarbejdere.
Stk. 6. It-sikkerhedslederen vurderer inden for eget område, om der er behov for at fastsætte regler i en it-sikkerhedsinstruks, som supplerer it-sikkerhedsregulativet. It-sikkerhedslederen udarbejder i givet fald en it-sikkerhedsinstruks, som godkendes af vedkommende borgmester, og som skal revideres mindst hvert 2. år.

Systemejere

§ 14. Systemejeren er ansvarlig for et it-systems funktionalitet, opbygning, anvendelse og sikkerhedsløsning samt for at iværksætte de nødvendige foranstaltninger til beskyttelse af it-systemet og de person- og værdioplysninger, der er indeholdt heri.
Stk. 2. Systemejeren skal godkende den it-ansvarliges procedurer for driftsafviklingen, herunder driftsplanen. Driftsplaner udarbejdet af eksterne samarbejdspartnere skal tillige godkendes af systemejeren. Driftsafviklingsprocedurer for it-systemer, der er væsentlige informationsaktiver, skal være dokumenterede, ajourførte og tilgængelige for driftsafviklingspersonalet og andre med et arbejdsbetinget behov herfor. Systemejeren skal endvidere sikre, at den it-ansvarlige indgår aftale om it-beredskab for så vidt angår det it-system, som henhører under systemejeren.
Stk. 3. Ved brug af eksterne samarbejdspartnere er systemejeren ansvarlig for, at der i forhold til det pågældende it-system træffes de nødvendige it-sikkerhedsforanstaltninger, herunder at der i nødvendigt omfang indgås aftaler om de nærmere vilkår og it-sikkerhedskrav i forbindelse med samarbejdet.
Stk. 4. Udveksling af person- og værdioplysninger i form af udtræk fra et it-system til et andet (dataudveksling) skal uanset udtræksmediet ske i henhold til retningslinier udarbejdet af systemejeren for det it-system, som er genstand for udtrækket.
Stk. 5. Systemejeren sikrer, at it-systemet kan logge i fornødent omfang, jf. sikkerhedsbekendtgørelsens § 19, og at logoplysningerne behandles i overensstemmelse med gældende it-sikkerhedskrav.
Stk. 6. Systemejeren sikrer, at it-sikkerhedskravene iagttages ved design, test, implementering og opgradering af it-systemer og ved systemændringer. Hvis integration af it-systemer indebærer en øget it-sikkerhedsrisiko, skal denne risiko vurderes nærmere af systemejeren med inddragelse af den it-ansvarlige og godkendes af direktionen for Koncernservice henholdsvis Børne- og Ungdomsforvaltningen og Brandvæsnets ledelse efter indstilling fra den it-ansvarlige.

It-ansvarlige

§ 15. Den it-ansvarlige skal sikre, at opbygning og anvendelse af kommunens it-platform, driftsmiljø og kommunikationsforbindelser er i overensstemmelse med de it-sikkerhedsmæssige krav og den til enhver tid gældende it-strategi.
Stk. 2. Den it-ansvarlige udarbejder it-sikkerhedsforskrifter for it-installationer, såfremt det skønnes nødvendigt. It-sikkerhedsforskrifterne skal revideres mindst hvert 2. år.
Stk. 3. Den it-ansvarlige har ansvaret for sikkerheden på it-platforme.
Stk. 4. Den it-ansvarlige i Koncernservice har ansvaret for de fysiske sikringsforanstaltninger inden for eget område og i forhold til kommunens netværk samt netværksudstyr og servere m.v., som ejes af Koncernservice.
Stk. 5. Den it-ansvarlige skal sikre, at udviklings-, test- og uddannelsesmiljøer holdes adskilt fra produktionsmiljøet.

Koncernservice

§ 16. Koncernservice udgør et selvstændigt it-sikkerhedsområde under Økonomiforvaltningen og har egen it-sikkerhedsleder.
Stk. 2. Koncernservice udfører på et kontraktuelt grundlag it-opgaver efter bestilling fra den øvrige del af kommunen.
Stk. 3. Ved bestilling af ydelser hos Koncernservice er bestillerenheden ansvarlig for, at der træffes de nødvendige it-sikkerhedsforanstaltninger, herunder at der i nødvendigt omfang indgås aftale om de nærmere vilkår og it-sikkerhedskrav i forbindelse med bestilling af ydelsen.

§ 17. Følgende it-sikkerhedsopgaver skal løses af Koncernservice på vegne af forvaltningerne:

a) brugeradministration,

b) varetagelse af systemejerskabet for fællessystemer,
c) varetagelse af ansvaret for kommunens fælles netværk, jf. § 15.

Stk. 2. Koncernservice kan ligeledes løse de i stk. 1 nævnte it-sikkerhedsopgaver for Revisionsdirektoratet og Borgerrådgiveren.
Stk. 3. Følgende it-sikkerhedsopgaver kan løses af Koncernservice på vegne af forvaltningerne henholdsvis Revisionsdirektoratet og Borgerrådgiveren:

a) varetagelse af systemejerskabet for andre systemer end fællessystemer,
b) ekspedition af anmodninger om indsigt efter persondataloven,
c) vurdering af behandlingssikkerhed hos eksterne leverandører og databehandlere,
d) review af kravspecifikationer for systemejerne ved anskaffelse, udvikling og ændring af it-systemer,
e) vurdering af sikkerhedsløsninger i de it-systemer, der anskaffes,
f) medvirke ved tests af it-systemers sikkerhedsløsning,
g) bestilling af autorisationsoversigter, til brug for opfølgning,
h) bestilling af sikkerhedsrapporter og logudskrifter til brug for den løbende kontrol og ad hoc kontroller.

Stk. 4. Koncernservice kan dog udføre samtlige af de opgaver, som henhører under it-sikkerhedslederen for Økonomiforvaltningen, så længe Koncernservice udgør et selvstændigt it-sikkerhedsområde under denne forvaltning.
Stk. 5. Varetagelse af systemejerskabet, jf. stk. 1, litra b og stk. 3, litra a, forudsætter, at Koncernservice har ansvaret for – og den fornødne kompetence til løsning af de faglige opgaver, som it-systemet understøtter.
Stk. 6. Varetagelse af de i stk. 3, litra b-h og stk. 4 nævnte opgaver forudsætter, at den eller de personer, som skal løse opgaverne, organisatorisk er placeret i samme enhed som it-sikkerhedslederen for Koncernservice. Opgaverne vil dog aldrig kunne løses af personer, som organisatorisk er placeret i brugeradministrationen.

§ 18. Såfremt Ledelsesinformation i Koncernservice udfører opgaver for andre end kommunen, skal opgaveudførelsen holdes adskilt fra de opgaver, som varetages for kommunen.

Funktionsadskillelse

§ 19. En medarbejder kan ikke samtidig varetage funktionen som it-sikkerhedsleder, systemejer eller it-ansvarlig.

Organisering af internt samarbejde

§ 20. Den it-ansvarlige træffer beslutning i forhold til de opgaver, som henhører under dennes ansvarsområde, jf. § 15.
Stk. 2. Såfremt den it-ansvarlige for henholdsvis Børne- og Ungdomsforvaltningen og Brandvæsnet skal træffe en beslutning vedrørende egne netværk, som kan påvirke sikkerheden i kommunens fælles netværk, skal den it-ansvarlige i Koncernservice høres, forinden der træffes beslutning.
Stk. 3. Bestillerenheden i en forvaltning kan gøre indsigelse mod en beslutning, som træffes af den it-ansvarlige i Koncernservice, jf. stk. 1. Indsigelsen har opsættende virkning. Den it-ansvarlige i Koncernservice skal herefter iværksætte en høring af forvaltningernes bestillerenheder.
Stk. 4. Såfremt der ikke kan opnås enighed, jf. stk. 3, skal den it-ansvarlige forelægge sagen for kredsen af administrerende direktører med henblik på beslutning.

§ 21. Der skal etableres et udvalg for it-sikkerhed og et samarbejdsforum for henholdsvis it-sikkerhedslederne og systemejerne for væsentlige fælles- og fagspecifikke it-systemer.

Stk. 2. Samarbejdsforaene har til opgave at koordinere it-sikkerhedsarbejdet inden for funktionerne og drøfte it-sikkerhedsmæssige forhold.
Stk. 3. Samarbejdsforaene refererer til udvalget for it-sikkerhed. Foraene orienterer udvalget om principielle diskussioner, og forbereder og indstiller sager til drøftelse i udvalget, jf. § 22.
Stk. 4. Formanden og næstformanden for samarbejdsforummet for systemejere udpeges for en 2-årig periode af forummets medlemmer på det førstkommende møde efter it-sikkerhedsregulativets ikrafttræden. Formandskabet for samarbejdsforummet for it-sikkerhedsledere varetages til enhver tid af Borgerrepræsentationens Sekretariat.
Stk. 5. Formanden forbereder og leder møderne og udsender dagsordener og referater fra møderne.
Stk. 6. Møder i samarbejdsforaene skal afholdes mindst én gang hver fjerde måned.

§ 22. Udvalget for it-sikkerhed består af henholdsvis 2 repræsentanter for samarbejdsforummet for it-sikkerhedsledere, formanden og næstformanden for samarbejdsforummet for systemejere, den it-ansvarlige i Koncernservice samt den daglige leder af brugeradministration i Koncernservice. Formandskabet varetages af Borgerrepræsentationens Sekretariat.
Stk. 2. De 2 repræsentanter for samarbejdsforummet for it-sikkerhedsledere udpeges for en 2-årig periode af samarbejdsforummets medlemmer på det førstkommende møde efter it-sikkerhedsregulativets ikrafttræden
Stk. 3. Udvalget har til opgave at drøfte it-sikkerhedsmæssige forhold, herunder fravigelser fra it-sikkerhedsregulativet, jf. § 6, og it-sikkerhedsbrud, jf. § 80, stk. 2. Drøftelserne sker på baggrund af indstilling fra de respektive samarbejdsfora eller fra Borgerrepræsentationens Sekretariat. Udvalget kan tilkendegive dets holdning til it-sikkerhedsmæssige problemstillinger.
Stk. 4. Såfremt en sag særligt vedrører en forvaltning eller enhed, som ikke er repræsenteret i udvalget, har en it-sikkerhedsrepræsentant herfor mulighed for at deltage under drøftelse af sagen.
Stk. 5. Udvalget refererer til kredsen af administrerende direktører. Udvalget skal årligt orientere kredsen af administrerende direktører om udvalgets arbejde og kan indstille sager til beslutning.
Stk. 6. Formanden forbereder og leder møderne og udsender dagsordener og referater fra møderne.
Stk. 7. Møder i it-sikkerhedsudvalget skal afholdes mindst én gang hver fjerde måned.

Kapitel 4

Organisering af eksternt samarbejde

§ 23. Forud for indgåelse af aftale med en ekstern samarbejdspartner og som led i et eventuelt udbud skal it-sikkerheden hos samarbejdspartneren vurderes, såfremt dette skønnes nødvendigt.
Stk. 2. Ved indgåelse af aftaler med eksterne samarbejdspartnere skal samarbejdspartneren underskrive en tavshedspligtserklæring, hvis samarbejdspartneren som led i samarbejdet får adgang til kommunens fortrolige og følsomme personoplysninger og værdioplysninger. Det nærmere indhold af tavshedspligtserklæringen fremgår af et af Borgerrepræsentationens Sekretariat udarbejdet paradigma.
Stk. 3. Ved indgåelse af aftaler med eksterne samarbejdspartnere, der indebærer, at samarbejdspartneren skal foretage databehandling på kommunens vegne, skal der indgås en databehandleraftale, hvis indhold er i overensstemmelse med et at Borgerrepræsentationens Sekretariat udarbejdet paradigma herom.
Stk. 4. Ansvaret for indgåelse af de i stk. 1-3 nævnte aftaler påhviler den, der indgår aftale med samarbejdspartneren.

§ 24. Ved udveksling af person- og værdioplysninger i form af udtræk fra et system til et andet (dataudveksling) skal de nærmere omstændigheder for udvekslingen afklares. Ansvaret for den nævnte afklaring påhviler den, som foranlediger udtrækket foretaget.

Kapitel 5

Risikovurdering og -håndtering

§ 25. Direktionen har inden for eget forvaltningsområde ansvar for at fastlægge et passende it-sikkerhedsniveau ud fra en risikovurdering.
Stk. 2. Direktionen for Koncernservice har ansvar for at fastlægge it-sikkerhedsniveauet inden for eget område og i forhold til kommunens netværk samt netværksudstyr og servere m.v., som ejes af Koncernservice. Som led i fastlæggelsen af it-sikkerhedsniveauet har direktionen ansvar for gennemførelse af risikovurderinger.
Stk. 3. It-sikkerhedsniveauet skal fastlægges under hensyntagen til kommunens overordnede it-sikkerhedsniveau, der fremgår af kommunens it-sikkerhedspolitik.
Stk. 4. Den praktiske gennemførelse af risikovurderingen påhviler it-sikkerhedslederen med bistand fra systemejerne og den it-ansvarlige.
Stk. 5. Koncernservice kan – som led i risikovurderingen, jf. stk. 2 - foretage en dokumenteret test af it-sikkerhedsniveauet i internt og eksternt netværksudstyr og servere m.v.
Stk. 6. Direktionen skal på baggrund af en indstilling fra it-sikkerhedslederen tage stilling til, om it-sikkerhedsniveauet er passende. Hvis it-sikkerhedsniveauet ikke er passende, skal der iværksættes tiltag, så det ønskede it-sikkerhedsniveau opnås. It-sikkerhedslederen skal orientere vedkommende fagudvalg og Borgerrepræsentationens Sekretariat om direktionens beslutning.
Stk. 7. Der skal udføres en detaljeret risikoanalyse for de områder, hvor risikovurderingen begrunder det. Ansvaret for gennemførelse af risikoanalyser påhviler it-sikkerhedslederen. Risikoanalyserne skal resultere i en handlingsplan, som it-sikkerhedslederen forelægger direktionen til godkendelse.

§ 26 Risikovurderinger skal udarbejdes på grundlag af et af Borgerrepræsentationens Sekretariat udarbejdet paradigma.
Stk. 2. Risikovurderinger skal udarbejdes inden udgangen af hvert ulige år og ved væsentlige ændringer i risikobilledet.

§ 27. Borgerrepræsentationens Sekretariat udarbejder på baggrund af de respektive risikovurderinger en samlet risikovurdering for kommunen.
Stk. 2. Den samlede risikovurdering skal udarbejdes inden udgangen af 1. kvartal i hvert lige år.
Stk. 3. På baggrund af den samlede risikovurdering træffer Borgerrepræsentationen beslutning om fastlæggelse af kommunens overordnede it-sikkerhedsniveau. Det overordnede it-sikkerhedsniveau fremgår af kommunens it-sikkerhedspolitik.

Liste over behandlinger og anmeldelsespligt

§ 28. Som led i risikovurderingen skal it-sikkerhedslederen udarbejde en liste over alle anvendte it-systemer samt de databehandlinger, der foretages på it-sikkerhedslederens område, og det skal i den forbindelse også vurderes og dokumenteres, i hvilket omfang der er pligt til at foretage anmeldelse af behandlingen, jf. stk. 3.
Stk. 2. It-sikkerhedslederen skal inden for eget område orienteres om de behandlinger, som påtænkes iværksat.
Stk. 3. It-sikkerhedslederen skal inden for eget område og efter forudgående at have rådført sig med Borgerrepræsentationens Sekretariat foretage anmeldelse til Datatilsynet af alle anmeldelsespligtige behandlinger før behandlingerne påbegyndes, jf. dog også persondatalovens § 44. Anmeldelser skal i videst muligt omfang ske ved tilslutning til de af KL og Datatilsynet udarbejdede fællesanmeldelser.

§ 29. Såfremt it-sikkerhedslederen vurderer, at der i forbindelse med iværksættelsen af nye aktiviteter påtænkes foretaget en behandling af følsomme oplysninger, som er af meget indgribende karakter, skal beslutning herom træffes af de respektive fagudvalg efter indstilling fra systemejeren for det it-system, som behandlingerne påtænkes foretaget i.
Stk. 2. Beslutning om iværksættelse af de i stk. 1 nævnte behandlinger, som vedrører flere forvaltninger, træffes af de respektive fagudvalg i forening.

Væsentlige informationsaktiver

§ 30. Som led i risikovurderingen skal it-sikkerhedslederen sikre, at der til enhver tid findes en ajourført fortegnelse over alle væsentlige informationsaktiver inden for it-sikkerhedslederens ansvarsområde med undtagelse af disketter, cd'er, usb-nøgler eller lignende mobile lagringsmedier.
Stk. 2. Af fortegnelsen over væsentlige informationsaktiver skal for hvert enkelt aktiv fremgå, hvem der er aktivets ejer, og hvilken type af oplysninger aktivet indeholder. Endvidere skal der være taget stilling til arkivering og eventuel sletning af oplysninger. Fortegnelsen skal udarbejdes på grundlag af et af Borgerrepræsentationens Sekretariat udarbejdet paradigma.

Kapitel 6

It-sikkerhedshandlingsplan

§ 31. Borgerrepræsentationens Sekretariat udarbejder en it-sikkerhedshandlings-plan, der skal sikre, at it-sikkerhedspolitikken udmøntes i praksis.
Stk. 2. It-sikkerhedshandlingsplanen skal forelægges for Økonomiudvalget til orientering.

Kapitel 7

Adfærdsregler

Kommunikation og lagring

§ 32. Al kommunikation mv. skal som udgangspunkt foregå via kommunens fælles it-netværk.
Stk. 2. Når kommunikation mv. ikke foregår via kommunens fælles it-netværk, må der kun anvendes it-systemer, internetservices, programmer, kommunikationsforbindelser, mv., der er godkendt af den it-ansvarlige.

§ 33. Alle oplysninger skal lagres på serverdrev, der er godkendt af den it-ansvarlige.

Kryptografi

§ 34. Den it-ansvarlige skal etablere en generel krypteringsløsning og udarbejde et nøglehåndteringssystem, som understøtter anvendelse af kryptografi.
Stk. 2. Der må ikke anvendes andre former for kryptering end de af den it-ansvarlige godkendte.

Brug af Internet

§ 35. Medarbejdere må anvende kommunens internetadgang til arbejdsmæssige formål. Hvis det ikke generer den arbejdsrelaterede anvendelse, må kommunens internetadgang tillige benyttes til private formål under forudsætning af, at den private anvendelse ikke er i

strid med kommunens værdigrundlag eller i øvrigt ikke stiller kommunen i et dårligt lys. Ved enhver brug af kommunens internetadgang skal kommunens it-sikkerhedspolitik overholdes.
Stk. 2. Den it-ansvarlige fastlægger sikkerhedsindstillingerne for webbrowsere og administrerer indstillingerne centralt. Der må kun anvendes godkendte webbrowsere. Medarbejderne må på ingen måde forsøge at omgå eller bryde disse it-sikkerhedsforanstaltninger.
Stk. 3. Den it-ansvarlige kan i fornødent omfang fastsætte regler om tung og vedvarende trafik.
Stk. 4. Den it-ansvarlige skal sikre, at filer, der hentes fra Internettet, scannes for virus umiddelbart efter, at de er hentet, og inden de åbnes.
Stk. 5. Kommunen kan af tekniske og it-sikkerhedsmæssige hensyn foretage maskinel registrering (logning) af medarbejdernes brug af Internettet mv.
Stk. 6. Kommunen kan herudover undtagelsesvis overvåge medarbejderes anvendelse af Internettet og øvrig datakommunikation efter forudgående godkendelse fra it-sikkerhedslederen for det pågældende område, hvis der i det konkrete tilfælde skønnes at være behov herfor.
Stk. 7. Medarbejderen vil altid være orienteret om overvågningen, medmindre der er tilstrækkeligt tungtvejende grunde til ikke at gøre dette. I givet fald skal medarbejderen, når de tungtvejende grunde ikke længere taler imod en sådan orientering, orienteres om overvågningen.

Brug af e-mail

§ 36. Medarbejdere skal anvende kommunens e-mailsystemer til arbejdsmæssige formål. Hvis det ikke generer den arbejdsrelaterede anvendelse, må kommunens e-mailsystemer tillige benyttes til private formål under forudsætning af, at den private anvendelse ikke er i strid med kommunens værdigrundlag eller i øvrigt ikke stiller kommunen i et dårligt lys. Ved enhver brug af kommunens e-mailsystemer skal kommunens it-sikkerhedspolitik overholdes.
Stk. 2. E-mails der indeholder fortrolige og følsomme personoplysninger eller værdioplysninger, og som sendes over Internettet eller andre åbne netværk, skal altid krypteres med godkendt software. Krypterede e-mails modtages i og afsendes fra sikre e-postkasser i kommunen.
Stk. 3. Den it-ansvarlige skal så vidt muligt etablere filtre, der forhindrer medarbejderne i at modtage og sende e-mails mv., der anses for at udgøre en særlig risiko for it-sikkerheden.
Stk. 4. Modtager en medarbejder alligevel en e-mail, som den pågældende af it-sikkerhedsmæssige årsager er utryg ved, må denne ikke åbnes, før den it-ansvarlige har godkendt dette. Såfremt private e-mails helt eller delvist tilbageholdes af it-sikkerhedsmæssige årsager, vil medarbejderne normalt kunne få udleveret en kopi af disse mails på en diskette eller lignende. Sådanne e-mails må ikke åbnes på kommunens it-udstyr.

§ 37. Medarbejdere skal markere private e-mails med teksten "privat" i emnefeltet eller gemme private e-mails i en folder, hvor teksten "privat" indgår i folderens navn.
Stk. 2. Kommunen kan undtagelsesvis skaffe sig adgang til e-mails og oplysninger hos medarbejdere, hvis dette sker af arbejdsmæssige eller it-sikkerhedsmæssige hensyn og efter forudgående godkendelse fra it-sikkerhedslederen for det pågældende område.
Stk. 3. Kommunen vil i videst muligt omfang søge at undgå at åbne private e-mails og oplysninger, og dette vil kun ske, hvis de interesser, der nødvendiggør, at medarbejderens e-mails og oplysninger åbnes, efter en konkret vurdering gør dette berettiget, jf. det anførte herom i straffelovens § 263.
Stk. 4. Medarbejderen vil altid være orienteret om, at kommunen skaffer sig adgang til e-mails og oplysninger, medmindre it-sikkerhedslederen for det pågældende område forud herfor har godkendt, at der er tilstrækkeligt tungtvejende grunde til ikke at gøre dette. I givet fald skal medarbejderen, når de tungtvejende grunde ikke længere taler herfor, orienteres herom.

Stk. 5. I tilfælde af, at kommunen uden medarbejderens viden af it-sikkerhedsmæssige hensyn skaffer sig adgang til medarbejderens e-mails mv., skal arbejdet udføres ved tilstedeværelse af to medarbejdere.
Stk. 6. Den enkelte medarbejder kan af hensyn til varetagelsen af arbejdsopgaver give andre medarbejdere adgang til vedkommendes e-mails og oplysninger.

Kapitel 8

Medarbejderne

Ansættelse af medarbejdere

§ 38. Alle medarbejdere skal senest på tiltrædelsestidspunktet og som en integreret del af ansættelsesaftalen erklære at være bekendt med, at vedkommende er underlagt reglerne om tavshedspligt, jf. forvaltningslovens § 27 og straffelovens § 152 og §§ 152 c-152 f. Ansvaret herfor påhviler medarbejderens nærmeste overordnede.
Stk. 2. Ved ansættelse af medarbejdere skal den leder, der underskriver ansættelsesaftalen, sikre, at der i fornødent omfang og under hensyn til stillingens karakter, er gennemført en undersøgelse af medarbejderens forhold.

Under ansættelsesforholdet

§ 39. Den nærmeste overordnede er ansvarlig for, at medarbejderen er informeret om sine opgaver og ansvar i forhold til it-sikkerheden, inden medarbejderen får adgang til kommunens it-systemer og oplysninger. Til brug herfor udarbejdes et eller flere elektroniske introduktionsforløb om it-sikkerhedsreglerne.
Stk. 2. Alle medarbejdere gennemgår som led i et introduktionsforløb om it-sikkerhed en elektronisk udgave af kommunens it-sikkerhedspolitik og it-sikkerhedsregulativ. Ved afslutningen af dette introduktionsforløb anmodes medarbejderen om at tilkendegive, om reglerne er læst og forstået. Hvis medarbejderen bekræfter dette, gives vedkommende i fornødent omfang adgang til kommunens it-systemer og oplysninger.
Stk. 3. Såfremt medarbejderen derimod tilkendegiver, at den pågældende har behov for yderligere instruktion om it-sikkerhedsreglerne, skal den nærmeste overordnede sikre, at medarbejderen modtager den fornødne instruktion.
Stk. 4. Den nærmeste overordnede kan iværksætte en undersøgelse af medarbejderens forhold, såfremt dette skønnes nødvendigt.

Ved ansættelsesforholdets ophør

§ 40. Medarbejderens nærmeste overordnede 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 en af it-sikkerhedslederen for det pågældende område nærmere fastlagt procedure.
Stk. 2. Medarbejderens nærmeste overordnede skal orientere medarbejderen om tavshedspligtens indhold efter ansættelsesforholdets ophør.

Kapitel 9

Fysisk sikkerhed

§ 41. Den lokale ledelse har inden for eget område ansvaret for, at der etableres en tilstrækkelig fysisk sikring af de områder, hvor der sker elektronisk databehandling af personoplysninger og værdioplysninger, og at kravene i it-beredskabsplanen for det pågældende forvaltningsområde til enhver tid overholdes.
Stk. 2. Den it-ansvarlige i Koncernservice har ansvaret for, at der etableres en tilstrækkelig fysisk sikring, jf. stk. 1, i forhold til kommunens netværk samt netværksudstyr og servere m.v., som ejes af Koncernservice.

Beskyttelse af udstyr, herunder ind - og uddata

§ 42. It-udstyr skal beskyttes, så risikoen for skader og uautoriseret adgang minimeres.
Stk. 2. It-udstyr, der benyttes til behandling af personoplysninger eller værdioplysninger, skal placeres på en sådan måde, at det er beskyttet mod adgang fra uvedkommende.

§ 43. Adgangen til ind- og uddata, der indeholder personoplysninger eller værdioplysninger, skal begrænses til medarbejdere, der har et arbejdsbetinget behov herfor.
Stk. 2. De i stk. 1 nævnte ind- og uddata skal til enhver tid opbevares således, at de ikke kommer til uvedkommendes kendskab, og som minimum ved aflåsning af lokalet, når dette forlades.
Stk. 3. I områder, som anvendes til betjening af borgere, og hvor der er offentlig adgang, skal ind- og uddata, som omfatter fortrolige eller følsomme personoplysninger eller værdioplysninger opbevares aflåst i skabe, skuffer eller lignende, når de ikke benyttes.
Stk. 4. De i stk. 1 nævnte ind- og uddata skal tilintetgøres på betryggende vis, f.eks. ved makulering, når der ikke længere er et sagligt behov for disse og senest 5 dage herefter.
Stk. 5. Ved fysisk transport af ind- og uddata skal der, når henses til oplysningernes karakter, anvendes en betryggende transportform. Vurderingen heraf skal foretages af systemejeren for det system, som ind- og uddataene hidrører fra og efter inddragelse af it-sikkerhedslederen for det pågældende område.

§ 44. Printere, der benyttes til udskrivning af personoplysninger eller værdioplysninger, skal placeres i lokaler, hvortil der ikke er offentlig adgang, eller forsynes med en teknisk facilitet, der kun muliggør udskrivning af dokumenter, når medarbejderen står ved printeren og giver tilladelse hertil.

§ 45. Stationært it-udstyr må kun fjernes fra kommunens ejendomme efter forudgående skriftlig godkendelse fra it-sikkerhedslederen for det område, hvor it-udstyret er placeret.
Stk. 2. Servere, netværksudstyr m.v., som ejes af Koncernservice, må kun fjernes fra kommunens ejendomme efter forudgående skriftlig godkendelse fra den it-ansvarlige i Koncernservice.

§ 46. Den it-ansvarlige i Koncernservice skal fastsætte regler for, hvilket it-udstyr, der skal tyverisikres gennem mærkning.

§ 47. Den it-ansvarlige i Koncernservice skal beskytte kabler til datakommunikation mod uautoriserede indgreb og skader. Faste kabler og udstyr skal mærkes klart og entydigt. Dokumentation for kabelføring skal opdateres, når den faste kabelføring ændres.

§ 48. Personoplysninger eller værdioplysninger skal så vidt muligt slettes effektivt og på en sikker måde fra it-udstyr, der repareres eller vedligeholdes uden for kommunens ejendomme.
Stk. 2. Såfremt der skal ske gendannelse af it-udstyr, hvor sletning af de i stk. 1 nævnte oplysninger ikke er hensigtsmæssig eller i situationer, hvor sletning ikke er mulig, skal der indgås en databehandleraftale med den eksterne samarbejdspartner, jf. det anførte i § 20 herom.

Stk. 3. Ved salg og øvrig genbrug af it-udstyr skal de i stk. 1 nævnte oplysninger slettes effektivt og på en sikker måde.
Stk. 4. Bortskaffelse af it-udstyr, som indeholder de i stk. 1 nævnte oplysninger, skal ske ved destruktion.
Stk. 5. Ansvaret for den i stk. 1-4 nævnte sletning og bortskaffelse påhviler den it-ansvarlige i Koncernservice.

Sikre og kontrollerede områder

§ 49. Krydsfelter, serverrum og andre steder, hvor netværksudstyr er placeret, anses altid som sikre områder.
Stk. 2. Den it-ansvarlige skal fastsætte retningslinier for fysisk sikring herunder om godkendelse af personale med adgang til de i stk. 1 nævnte områder, om eventuel overvågning af personale, om meddelelse af oplysninger herom, om anvendelse af alarmsystemer, beskyttelse mod brand og vandskader, eventuel etablering af køling og ventilation, beskyttelse med nødstrømsanlæg og kapaciteten heraf samt om andre foranstaltninger til beskyttelse af de i stk. 1 nævnte områder. Retningslinierne skal revideres mindst hvert 4. år.
Stk. 3. Der skal føres en fortegnelse over de i stk. 1 nævnte områder.

§ 50. Den lokale ledelse skal i samarbejde med it-sikkerhedslederen træffe beslutning om, hvilke andre områder der, udover de i § 49, stk. 1 nævnte, skal være sikre områder. Der skal føres en fortegnelse over disse områder.
Stk. 2. Den lokale ledelse fastsætter i samarbejde med it-sikkerhedslederen retningslinier for fysisk sikring herunder om godkendelse af personale med adgang til sikre områder, om eventuel overvågning af personale, om meddelelse af oplysninger herom, om anvendelse af alarmsystemer, beskyttelse mod brand og vandskader, eventuel etablering af køling og ventilation, beskyttelse med nødstrømsanlæg og kapaciteten heraf samt om andre foranstaltninger til beskyttelse af sikre områder. Retningslinierne skal revideres mindst hvert 4. år.

§ 51. Den lokale ledelse træffer i samarbejde med it-sikkerhedslederen herudover beslutning om, hvilke områder, som offentligheden ikke normalt skal have adgang til, og som dermed skal anses som kontrollerede områder. Den lokale ledelse fastsætter i samarbejde med it-sikkerhedslederen om nødvendigt nærmere retningslinier for sikkerheden på sådanne kontrollerede områder. Eventuelle retningslinier herom skal revideres mindst hvert 4. år.

Kapitel 10

Adgangsstyring

Adgangsstyring og brugeradgang

§ 52. Al adgang til kommunens it-systemer, servere, netværk og pc'er, der indeholder person- eller værdioplysninger, skal være betinget af konkrete autorisationer.
Stk. 2. Medarbejdere må alene få adgang til de oplysninger, som de har et sagligt behov for som led i deres arbejde.
Stk. 3. Oprettelse og vedligeholdelse af medarbejdere i kommunens it-systemer skal ske i brugeradministrationen i Koncernservice.
Stk. 4. Koncernservice skal udarbejde en eller flere procedurer for adgangsstyring og brugeradgang, jf. §§ 52-55 og § 59, stk.3. Proceduren eller procedurerne skal sendes i høring hos it-sikkerhedslederne. Proceduren eller procedurerne skal forelægges for Borgerrepræsentationens Sekretariat til godkendelse.
Stk. 5. Autorisationer til de enkelte medarbejdere tildeles efter anmodning fra dén overordnede, som har kendskab til hvilke it-systemer medarbejderen som led i sit arbejde har et

sagligt behov for at få adgang til. Anmodningen skal være umiddelbart tilgængelig for den pågældende medarbejders it-sikkerhedsleder.
Stk. 6. It-sikkerhedslederne opretter og ajourfører inden for eget område en oversigt over, hvilke overordnede, der jf. stk. 5 kan anmode om tildeling af autorisationer til de enkelte medarbejdere.

§ 53. Eksterne samarbejdspartnere, som har brug for adgang til et it-system af hensyn til drifts-, udviklings- og vedligeholdelsesopgaver, skal autoriseres hertil.
Stk. 2. Autorisation af eksterne samarbejdspartnere må kun finde sted, såfremt en entydig identifikation af den pågældende medarbejder kan finde sted. Dette skal som udgangspunkt ske i form af cpr-nummer.
Stk. 3. Autorisation sker på baggrund af en anmodning fra den ansvarlige for aftaleindgåelsen med den eksterne samarbejdspartner, som skal sørge for at indhente de fornødne oplysninger om samarbejdspartneren.
Stk. 4. Oprettelse skal ske i overensstemmelse med §§ 54-55.

§ 54. Hver medarbejder skal ved oprettelse tildeles en unik brugerident. Brugeridenten er personlig.
Stk. 2. Den unikke brugerident skal genereres i kommunens it-sikkerhedssystem.

§ 55. Ved oprettelse eller nulstilling af adgangskode skal medarbejderen tildeles en sikker midlertidig adgangskode, som skal ændres af medarbejderen umiddelbart ved første anvendelse.
Stk. 2. Udlevering af den midlertidige adgangskode skal ske på en sikker måde. Midlertidige adgangskoder skal opfylde de almindelige krav til adgangskoder, jf. § 60, stk. 4.
Stk. 3. Koncernservice udarbejder en procedure for, hvordan en brugers identitet fastslås, før en ny adgangskode må udleveres, og for hvorledes udleveringen skal ske.
Stk. 4. Såfremt der skal ske transmission af adgangskoder over Internettet eller andre åbne netværk, skal dette ske ved kryptering med godkendt software. Adgangskoder må ikke tastes i et læsbart felt.
Stk. 5. Standardadgangskoder fra systemleverandører skal ændres i forbindelse med installation af it-systemet.
Stk. 6. Indtastning af adgangskode kan erstattes af brug af id-kort eller lignende autentifikationsmekanisme med et tilsvarende eller højere sikkerhedsniveau.

§ 56. It-sikkerhedslederen skal inden for eget område kontrollere de tildelte autorisationer på baggrund af en daglig rapport fra det enkelte it-systems sikkerhedsmodul.
Stk. 2. It-sikkerhedslederen skal udover den i stk. 1 nævnte kontrol løbende gennemgå de tildelte brugerrettigheder med henblik på at sikre, at autorisationerne fortsat er i overensstemmelse med den enkelte medarbejders konkrete behov. Gennemgangen skal dokumenteres.
Stk. 3. It-sikkerhedslederen skal hvert halve år kontrollere, at medarbejdere, der er tildelt brugerrettigheder, som giver adgang til værdioplysninger eller fortrolige eller følsomme personoplysninger, jf. dog § 15 i sikkerhedsbekendtgørelsen, fortsat opfylder betingelserne for de tildelte brugerrettigheder.

§ 57. Ved omplacering af medarbejdere skal medarbejderens nye overordnede, som ved hvilke it-systemer medarbejderen som led i sit arbejde har et sagligt behov for at få adgang til, sikre, at medarbejderen alene har de brugerrettigheder, der herefter er sagligt behov for. Ændringerne skal meddeles brugeradministrationen.
Stk. 2. Ved overflytning af medarbejdere fra en forvaltning til en anden skal de pågældende medarbejdere som udgangspunkt nedlægges i den forvaltning de flytter fra og oprettes med ny brugerident i den nye forvaltning. Udgangspunktet kan fraviges ved overflytning af større grupper af medarbejdere.
Stk. 3. Ved overflytning af medarbejdere, jf. stk. 2, skal adgangsrettighederne tilpasses.

Stk. 4. Ophører ansættelsesforholdet, eller er der i en periode ikke den fornødne arbejdsmæssige brug for at kunne udnytte brugerrettigheder, hvilket f.eks. kan være tilfældet ved længerevarende orlov, skal brugerrettighederne inddrages.

§ 58. Systemejer meddeler de enkelte it-sikkerhedsledere de nærmere retningslinier for adgangsstyring til hvert enkelt system. Retningslinierne skal blandt andet beskrive, hvilke medarbejdergrupper der skal have adgang til it-systemet, samt hvilke oplysninger og funktioner den enkelte medarbejder kan få adgang til. Retningslinierne kan endvidere indeholde en beskrivelse af eventuel mulighed for anvendelse af rolleprofiler.
Stk. 2. Rolleprofiler som de i stk. 1 nævnte skal oprettes og vedligeholdes af systemejer i samarbejde med den enkelte it-sikkerhedsleder.

§ 59. Kontrol med afviste adgangsforsøg skal etableres ved login til kommunens netværk eller i forbindelse med login til it-systemer, der behandler værdioplysninger eller fortrolige eller følsomme personoplysninger, jf. dog sikkerhedsbekendtgørelsens § 15, således at forgæves forsøg på login logges automatisk.
Stk. 2. Hvis der konstateres mere end 5 på hinanden følgende forgæves login-forsøg, skal der automatisk blokeres for yderligere forsøg. Blokeringen rapporteres automatisk til it-sikkerhedslederen.
Stk. 3. Blokering for login kan ophæves af brugeradministrationen.

Medarbejderens ansvar

§ 60. Adgangskoder må ikke udlånes til andre. De er personlige og strengt fortrolige.
Stk. 2. Såfremt adgangskoden kompromitteres, eller der opstår mistanke herom, er det medarbejderens ansvar straks at underrette it-sikkerhedslederen og ændre kodeordet.
Stk. 3. Hvis flere medarbejdere benytter den samme arbejdsstation, skal den enkelte medarbejder logge på med egen brugerident, før der udføres arbejdsopgaver, og logge af, inden den næste medarbejder overtager arbejdspladsen.
Stk. 4. Adgangskoder i adgangskontrolsystemerne skal opfylde følgende krav:

- adgangskoder skal indeholde mindst 8 tegn,
- adgangskoder skal så vidt muligt indeholde kombinationer fra mindst tre af følgende kategorier; store bogstaver, små bogstaver, tal og specialtegn,
- der må ikke benyttes brugerident, navn eller datoer som en del af adgangskoden,
- adgangskoder skal skiftes efter højst 90 dage.

Stk. 5. Når en medarbejder forlader en tændt arbejdsstation, således at den er ude af den pågældendes synsvidde, skal den adgangskodebeskyttede skærmlås aktiveres. Alle arbejdsstationer skal have en skærmlås, der aktiveres automatisk efter højest 15 minutters inaktivitet.
Stk. 6. Adgangskoder til administratoradgang skal opbevares i en forseglet kuvert i et aflåst og brandsikkert pengeskab.

Styring af netværk

§ 61. Den it-ansvarlige har ansvaret for at beskytte det benyttede netværk. Installation af netværksudstyr må kun foretages af medarbejdere, der på forhånd er udpeget hertil, eller af personer, der har fået tilladelse hertil af den it-ansvarlige.
Stk. 2. Den it-ansvarlige har ansvaret for de benyttede internetforbindelser.
Stk. 3. Brug af trådløse netværk må kun ske efter tilladelse fra den it-ansvarlige.

§ 62. Den it-ansvarlige skal sikre, at medarbejdere alene får adgang til godkendte fælles netværk og dertil knyttede tjenester.
Stk. 2. Adgang til det interne netværk fra andre ejendomme end kommunens skal beskyttes med tofaktor-login, medmindre der foreligger en godkendelse heraf fra den it-ansvarlige.

§ 63. Den it-ansvarlige skal begrænse og styre adgangen til systemværktøjer, der kan påvirke eller omgå systemers eller enheders it-sikkerhed. Unødige systemværktøjer må ikke være installeret eller tilgængelige på medarbejderes computere. Adgangen til systemværktøjer skal begrænses til et minimum af godkendte medarbejdere.
Stk. 2. Hvis funktionsadskillelse er påkrævet, må medarbejdere ikke have adgang til både systemværktøjer og fagsystemer.
Stk. 3. Såfremt der i forbindelse med driftsproblemer, tests, genopretning el. lign. er et dokumenteret arbejdsbetinget behov for adgang til både systemværktøjer og brugersystemer, kan it-sikkerhedslederen for det pågældende område dog give tilladelse hertil.

§ 64. Den it-ansvarlige skal sikre, at der installeres de nødvendige antivirusprodukter til beskyttelse af systemer og oplysninger. Der skal installeres antivirus på alle it-systemer, hvor dette er muligt. Antivirus skal løbende opdateres.

§ 65. Hvis en person med kendskab til administratoradgangskoder fratræder, skal disse adgangskoder ændres med det samme. Adgangskoder skal endvidere ændres med det samme, hvis udenforstående får kendskab til disse.
Stk. 2. Administratoradgangskoder skal følge samme minimumskrav som øvrige adgangskoder, dog skal de være mindst 12 tegn.
Stk. 3. Medarbejdere må ikke ændre opsætning eller indstilling på de arbejdsstationer, de benytter.

Mobilt it-udstyr, herunder fjernarbejdspladser

§ 66. Fjernarbejdspladser tillades, når it-sikkerhedspolitikken overholdes.
Stk. 2. Fjernarbejdspladser må ikke anvendes af andre end den medarbejder, som fjernarbejdspladsen er tiltænkt, eller af kommunens it-medarbejdere, hvis dette sker som led i udførelsen af en it-service, som f.eks. installation eller reparation.
Stk. 3. Fjernarbejdspladser skal stilles til rådighed for kommunen i forbindelse med it-sikkerhedskontroller, servicering mv.
Stk. 4. Personoplysninger eller værdioplysninger må ikke lagres på fjernarbejdspladsens harddisk medmindre dette er godkendt af it-sikkerhedslederen for det pågældende område, og oplysningerne er krypterede.
Stk. 5. Medarbejdere har pligt til at destruere udskrifter med fortrolige eller følsomme personoplysninger eller værdioplysninger på en sikker måde, når udskrifterne ikke længere skal anvendes. Dette kan f.eks. ske ved makulering.

§ 67. For at få adgang til kommunens interne netværk fra en fjernarbejdsplads, skal brugeren være autentificeret ved en tofaktor-login, og der skal anvendes en krypteret forbindelse.

§ 68. Den it-ansvarlige skal sikre, at antivirusprogrammer og adgangskontrolsystemer er installerede på mobilt it-udstyr og fjernarbejdspladser tillige med firewall eller anden tilsvarende sikkerhedsforanstaltning.
Stk. 2. Den it-ansvarlige skal løbende sikre, at de i stk. 1 nævnte antivirusprogrammer, adgangskontrolsystemer og firewall el. lign. er tilstrækkelige.
Stk. 3. Adgang til kommunens netværk må kun ske gennem sikkerhedsgodkendt it-udstyr. Der kan fra fjernarbejdspladser fås adgang til de samme applikationer, som fra medarbejderens sædvanlige kontorarbejdsplads.
Stk. 4. Der må ikke opbevares fortrolige eller følsomme personoplysninger eller værdioplysninger på mobilt it-udstyr, medmindre dette er godkendt af it-sikkerhedslederen for det pågældende område og oplysningerne er krypterede.
Stk. 5. Der må ikke behandles eller opbevares personoplysninger eller værdioplysninger på it-udstyr, der ikke tilhører kommunen medmindre der er indgået aftale herom, jf. § 1, stk. 2 eller § 20.

Kapitel 11

Anskaffelse, udvikling og vedligeholdelse af it-systemer

Anskaffelse af it-systemer

§ 69. Ved anskaffelse og udvikling af it-systemer skal systemejer sikre, at anskaffelsen og udviklingen lever op til de gældende it-sikkerhedskrav og kommunens it-strategi.
Stk. 2. Anskaffelse og udvikling af it-systemer kan alene ske efter forudgående godkendelse af sikkerhedsløsningen fra it-sikkerhedslederen for det område, hvor systemejerskabet er placeret. Systemejeren skal dokumentere over for it-sikkerhedslederen for det pågældende område, at anskaffelsen og udviklingen lever op til de gældende it-sikkerhedskrav.
Stk. 3. Inden anskaffelse og udvikling af et it-system skal systemejer nøje vurdere leverandøren.
Stk. 4. Systemejeren skal sikre, at leverandøren indgår en it-sikkerhedsaftale med kommunen og fremlægger en årlig revisorerklæring i henhold til "statsautoriserede revisorers revisionsstandard RS 3411 om generelle it-kontroller og applikationskontroller".
St. 5. Kravet om generelle it-kontroller og applikationskontroller, jf. stk. 4, kan dog fraviges, såfremt kravet ikke følger af lov eller bekendtgørelser fastsat i henhold til lov og efter en vurdering af leverandøren, jf. § 20, stk.1, samt en risikovurdering af kompleksiteten i den enkelte applikation set i forhold til det fastlagte it-sikkerhedsniveau.
Stk. 6. Systemejer skal foretage en risikovurdering af det nye it-system på baggrund af leverandørens tilbud, inden der indgås kontrakt om udvikling og inden ibrugtagning.
Stk. 7. Ved anskaffelse af væsentlige it-systemer eller ved it-systemopgraderinger, vedligeholdelse og videreudvikling skal systemejeren beskrive de enkelte it-sikkerhedskrav, og leverandøren skal dokumentere, at it-sikkerhedskravene overholdes.
Stk. 8. It-sikkerhedslederen skal inden for eget område tilse, at kun testede og godkendte it-systemer idriftsættes.
Stk. 9. Systemejer har ansvaret for, at relevante tests afholdes og skal godkende disse.

§ 70. Systemejeren har ansvaret for at vedligeholde dokumentation for ejendomsretten af licenser, originalmateriale og manualer i forhold til det it-system, som henhører under systemejeren.
Stk. 2. Den it-ansvarlige har ansvaret for at vedligeholde det materiale, som jf. stk. 1 ikke relaterer sig til et it-system, der varetages af en systemejer.
Stk. 3. Den it-ansvarlige har ansvaret for, at software-licensaftaler overholdes, og at der kun er installeret autoriserede it-systemer, hvortil kommunen har licens. Det er den it-ansvarliges ansvar, at der er et tilstrækkeligt antal licenser til rådighed.
Stk. 4. Medarbejdere må ikke kopiere, konvertere eller udtrække information fra billed- eller lydfiler mv. eller kopiere bøger, artikler, rapporter mv., medmindre dette er udtrykkeligt tilladt af rettighedshaveren. Medarbejdere må ikke forpligte kommunen ved at acceptere licensvilkår i software, som ikke er accepteret af den it-ansvarlige.

Anskaffelse af it-udstyr

§ 71. Ved anskaffelse af it-udstyr skal den it-ansvarlige foretage en risikovurdering for at sikre, at it-udstyret lever op til kravene i it-sikkerhedspolitikken og it-sikkerhedsregulativet, og at it-udstyret ikke medfører en øget risiko for it-sikkerhedshændelser. En øget risiko for it-sikkerhedshændelser kan accepteres efter forudgående godkendelse fra direktionen.
Stk. 2. Hvis risikovurderingen giver anledning hertil, kan den it-ansvarlige beslutte, at it-udstyret skal gennemgå en detaljeret risikoanalyse, inden det tages i brug.

Interne kontroller for it-systemer

§ 72. Systemejer skal sikre, at der udarbejdes de nødvendige beskrivelser af interne kontroller ved anvendelse af it-systemet, så der ved anvendelsen af it-systemerne sker en kontrol af oplysningernes korrekthed.

Styring af driftsmiljøer

§ 73. Den it-ansvarlige skal sikre, at der sker lagring og backup af oplysninger på serverudstyr. Det skal sikres, at der efter behov og i henhold til aftale tillige opbevares en sikkerhedskopi på en ekstern lokation. Den it-ansvarlige fastsætter nærmere retningslinier for sikkerhedskopieringen. Retningslinierne skal revideres mindst hvert 4. år.

§ 74. Ved migrering fra udvikling til produktion skal systemejer sikre, at leverandøren af et it-system gennemfører de tests, der er nødvendige for at sikre driftsniveau, it-sikkerhedsniveau og brugbarhed inden implementering. Godkendt software skal sikres mod uønskede ændringer.
Stk. 2. Testoplysninger skal udvælges, kontrolleres og beskyttes omhyggeligt. Oplysninger fra driftsmiljøet, der anvendes i testmiljøer, skal beskyttes på samme måde som i produktionsmiljøet og slettes omgående efter afsluttet test.
Stk. 3. Kildekode til udviklingsprojekter skal sikres mod uautoriseret adgang og opbevares forsvarligt. Vedligeholdelse og kopiering af kildekode skal følge en dokumenteret procedure for ændringsstyring.

It-sikkerhed i udviklings- og ændringsprocesser

§ 75. Al systemudvikling og -ændring skal gennemføres med de nødvendige it-sikkerhedsforanstaltninger.

§ 76. Ved ændringer i et it-system gennemgås it-sikkerhedsforanstaltninger og interne kontroller for at sikre, at disse ikke forringes ved implementering af ændringer. Ændringer skal testes og godkendes af systemejer, inden de sættes i værk.
Stk. 2. Systemdokumentation skal opdateres ved ændringer.
Stk. 3. Der skal vedligeholdes en versionsstyring for alle systemændringer og et kontrolspor for alle ændringer.
Stk. 4. Ved ændring af driftsmiljøer skal kritiske forretningssystemer gennemgås og testes for at sikre, at ændringerne ikke medfører utilsigtede virkninger på kommunens daglige drift.
Stk. 5. Kildekode til applikationer under udvikling skal beskyttes med adgangskontrolsystemer.

§ 77. Ved systemudvikling, der udføres for kommunen af en ekstern leverandør, skal det aftales, at systemejer skal have adgang til at overvåge udviklingsprocessen.
Stk. 2. Leverandøren gennemfører afleveringstest og aktiviteter med henblik på dokumenteret løbende kvalitetssikring. Resultatet af afleveringstest skal godkendes af systemejer.
Stk. 3. Kildekode opbevares hos kommunen eller betroet samarbejdspartner. Kommunen kan kræve ophavsrettighederne til kildekode.

Sårbarhedsstyring

§ 78. Den it-ansvarlige skal godkende idriftsættelsen af nye it-systemer og nye versioner og opdateringer af eksisterende it-systemer samt de afprøvninger, der skal foretages, inden de kan godkendes og sættes i drift.

Stk. 2. Den it-ansvarlige skal sikre, at det løbende vurderes, om der er behov for at installere rettelser til operativsystemer i kommunens interne driftsmiljø. Nødvendige rettelser installeres senest en uge efter gennemførelse af en positiv funktions- og kompatibilitetstest.
Stk. 3. Den it-ansvarlige skal sikre, at det løbende vurderes, om større operativsystemopdateringer og programpakkeopdateringer ("service packs") skal installeres i kommunens interne driftsmiljø.

Kapitel 12

Styring af it-sikkerhedshændelser

§ 79. Ved konstatering af brud eller formodning om brud på it-sikkerhedsbestemmelserne skal it-sikkerhedslederen straks underrettes herom. Hvis it-sikkerhedslederen ikke træffes, rettes henvendelse til Borgerrepræsentationens Sekretariat, der hurtigst muligt herefter orienterer it-sikkerhedslederen.
Stk. 2. Dén, der konstaterer et it-sikkerhedsbrud eller har en formodning herom, skal til brug for underretningen af it-sikkerhedslederen øjeblikkeligt notere alle vigtige detaljer såsom typen af brud, den opståede fejl, beskeder på skærmen og usædvanlige hændelser.
Stk. 3. It-sikkerhedslederen skal straks iværksætte de foranstaltninger, der er nødvendige, for at korrigere de konstaterede fejl eller svagheder. It-sikkerhedslederen udarbejder et notat om alle rapporterede it-sikkerhedsbrud og om resultatet af de iværksatte foranstaltninger og orienterer skriftlig sin direktion og Borgerrepræsentationens Sekretariat herom.
Stk. 4. It-sikkerhedslederen orienterer én gang årligt og inden udgangen af 4. kvartal vedkommendes fagudvalg om konstaterede it-sikkerhedsbrud. Såfremt der er flere it-sikkerhedsområder, som hører under det samme fagudvalg, koordinerer it-sikkerhedslederne for disse områder en samlet forelæggelse for fagudvalget.
Stk. 5. Borgerrepræsentationens Sekretariat orienterer én gang årligt og inden udgangen af 1. kvartal i det i forhold til stk. 4 efterfølgende år Økonomiudvalget om konstaterede it-sikkerhedsbrud.

§ 80. Borgerrepræsentationens Sekretariat sikrer, at der sker opsamling og bearbejdning af oplysninger om it-sikkerhedshændelser.
Stk. 2. Borgerrepræsentationens Sekretariat skal orientere udvalget for it-sikkerhed om konstaterede it-sikkerhedsbrud.
Stk. 3. Borgerrepræsentationens Sekretariat vurderer mindst én gang om året, om periodens hændelser giver anledning til forbedringer af it-sikkerheden.

§ 81. Brugere, der observerer programfejl, som de ikke har oplevet før, skal rapportere dette til systemejeren eller til rette vedkommende med henblik på videreformidling til systemejeren.
Stk. 2. Ved computervirus eller mistanke om virusangreb skal der omgående rettes henvendelse til den it-ansvarlige.

§ 82. Koncernservice og eksterne samarbejdspartnere skal mindst en gang om måneden rapportere til relevante it-sikkerhedsledere, hvorvidt der er konstateret hændelser af betydning for it-sikkerheden og i bekræftende fald beskrive disse hændelser nærmere.

Kapitel 13

It-beredskabsstyring

§ 83. Borgerrepræsentationens Sekretariat har ansvaret for, at der foreligger procedurer, som sikrer en tværorganisatorisk styring af it-beredskabet i tilfælde af større it-nedbrud mv. til uddybning af kommunens beredskabsplan.
Stk. 2. Borgerrepræsentationens Sekretariat fastlægger i samarbejde med den it-ansvarlige i Koncernservice de overordnede retningslinier for udarbejdelse af it-beredskabsplanerne. It-beredskabsplanerne skal indeholde procedurer for iværksættelse af nødplaner, reetablering af it-systemer og begrænsning af skadevirkninger i tilfælde af større it-nedbrud.
Stk. 3. Direktionen henholdsvis Borgerrådgiveren og direktøren for Revisionsdirektoratet har inden for eget område ansvaret for, at der bliver udarbejdet en it-beredskabsplan som omfatter alle kritiske it-systemer og processer.
Stk. 4. It-sikkerhedslederen koordinerer inden for eget område arbejdet med udarbejdelse af it-beredskabsplaner og sikrer, at der foregår en tilstrækkelig uddannelse af medarbejdere i de fastlagte it-beredskabsprocedurer.
Stk. 5. I tilfælde af større it-nedbrud skal it-beredskabsplanen aktiveres af Borgerrepræsentationens Sekretariat gennem it-sikkerhedslederne, systemejerne og den it-ansvarlige.

§ 84. Den it-ansvarlige har ansvaret for at indgå aftale om it-beredskab, herunder den tekniske reetableringsplan med eksterne driftsleverandører og sikre, at disse bliver testet og vedligeholdt. It-sikkerhedslederen for det pågældende område og systemejerne for de it-systemer, som it-beredskabsplanen vedrører, skal medvirke ved test af it-beredskabsplanen.
Stk. 2. Systemejeren skal sikre, at der indgås aftale om it-beredskab for så vidt angår det it-system, som denne er systemejer for. Hvis flere it-systemer driftafvikles hos samme leverandør, skal it-beredskabsplanerne for disse it-systemer koordineres.

§ 85. Direktionen henholdsvis ledelsen har inden for eget område ansvaret for at sikre, at der er tegnet en tilstrækkelig forsikring af det af området anvendte it-udstyr, software, it-systemer og oplysninger.
Stk. 2. Direktionen for Koncernservice har, ud over det i stk. 1 nævnte, ansvaret for at sikre, at der er tegnet en tilstrækkelig forsikring for netværksudstyr og servere m.v., som ejes af Koncernservice.

Kapitel 14

Lovbestemte krav

§ 86. De respektive direktioner henholdsvis Borgerrådgiveren og direktøren for Revisionsdirektoratet skal inden for eget område sikre, at specifik lovgivning af betydning for it-sikkerheden og eksterne it-sikkerhedskrav for det pågældende område bliver identificeret, dokumenteret og overholdt.

§ 87. Det daglige ansvar for overholdelsen af reglerne i persondataloven i forbindelse med behandling af personoplysninger påhviler de respektive direktioner henholdsvis Borgerrådgiveren og direktøren for Revisionsdirektoratet.
Stk. 2. Medarbejdere skal særligt være opmærksomme på følgende forhold:

a) om reglerne i persondataloven skal iagttages og i givet fald,
b) om behandlingen overholder de grundlæggende krav og er hjemlet efter bestemmelserne i persondatalovens kapitel 4,
c) om kommunen har opfyldt en evt. oplysningspligt over for den registrerede,
d) om kommunen i fornødent omfang har givet den registrerede indsigt og behandlet evt. indsigelser mv.,
e) om der er en eventuel anmeldelsespligt, og i så fald om it-sikkerhedslederen er orienteret herom,
f) om it-sikkerhedsbestemmelserne er opfyldt.

Kapitel 15

Revision af it-sikkerhed

§ 88. Som led i den almindelige revision af kommunen skal også foretages revision af it-sikkerheden.

Kapitel 16

Ikrafttrædelse og ændringer

§ 89. It-sikkerhedsregulativet træder i kraft fra godkendelsen i Borgerrepræsentationen. Samtidig ophæves it-sikkerhedsregulativet, godkendt af Borgerrepræsentationen den 22. august 2002.

§ 90. Borgerrepræsentationens Sekretariat vurderer hvert år inden udgangen af juni måned, om it-sikkerhedsregulativet er i overensstemmelse med it-sikkerhedspolitikken, og om der er behov for ændringer i it-sikkerhedsregulativet.
Stk. 2. Ændringer i it-sikkerhedsregulativet skal godkendes af Borgerrepræsentationen efter indstilling fra Borgerrepræsentationens Sekretariat.