Koncessionskontrakt vedr. ekspeditionen af pas, kørekort og øvrige borgerserviceopgaver.

Københavns Kommune

Kultur- og Fritidsforvaltningen

Bilag 9a

IT-sikkerhedsdokumenter

1 INDHOLD

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:

1 KAPITEL 1 – ANVENDELSESOMRÅDE OG FORMÅL

§ 1. It-sikkerhedsreglerne i Københavns Kommune er samlet på kommunens intranet i en it-sikkerhedshåndbog, som indeholder:

It-sikkerhedspolitikken: It-sikkerhedspolitikken fastlægger det overordnede niveau for it-sikkerheden i kommunen.

It-sikkerhedsregulativ for Københavns Kommune: It-sikkerhedsregulativet skal beskrive de organisatoriske rammer for kommunens håndtering af it-sikkerhedsrisici.

En række uddybende It-sikkerhedsregler for Københavns Kommune: De uddybende It-sikkerhedsregler for Københavns Kommune indeholder de resterende it-sikkerhedsregler for kommunen.

Stk. 2. It-sikkerhedshåndbogen baseres på ISO-standarden for informationssikkerhed (ISO 27001 – 27002 om Informationsteknologi – Sikkerhedsteknikker – Ledelsessystemer for informationssikkerhed (ISMS) og Krav)

Stk. 3. It-sikkerhedshåndbogen skal løbende tilpasses lovgivningen, den teknologiske udvikling samt internationale, statslige, fælleskommunale og regionale standarder.

Stk. 4. It-sikkerhedshåndbogen gælder for alle relevante interessenter - herunder samtlige af kommunens medarbejdere.

Stk. 5. It-sikkerhedshåndbogen 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. 6. Det skal aftales med de selvejende og private institutioner mv., der har indgået driftsoverenskomst med kommunen, eller som kommunen udfører databehandling for, at disse skal efterleve it-sikkerhedshåndbogen.

§ 2. It-sikkerhedshåndbogen skal leve op til ISO-standarden for informationssikkerhed. I beslutninger om it-sikkerhed skal der gennemføres en afvejning de it-sikkerhedsmæssige risici med de forretningsmæssige behov for effektivitet i kommunen og høj borgerservice. Dette skal bl.a. 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 følger de regler for behandling af personoplysninger, der er fastsat i lov om behandling af personoplysninger (persondataloven) med tilhørende bekendtgørelser mv.

§ 3. De begreber der er anvendt i Regulativ for It-sikkerhed er defineret i Bilag 1 bagest i dette regulativ.

2 KAPITEL 2 - INTERNE ORGANISATORISKE FORHOLD. BESKRIVELSE AF HVEM, DER HAR ANSVARET FOR IT-SIKKERHEDEN.

2.1 BORGERREPRÆSENTATIONEN

§ 4. Borgerrepræsentationen vedtager kommunens it-sikkerhedspolitik og it-sikkerhedsregulativ efter indstilling fra Koncernservice i Økonomiforvaltningen.

Stk.2. It-sikkerhedspolitikken fastlægger det overordnede niveau for it-sikkerheden i kommunen. Stk. 3 It-sikkerhedsregulativet skal beskrive de organisatoriske rammer for kommunens håndtering af it-sikkerhedsrisici.

2.2 ØKONOMIUDVALGET

§ 5. Økonomiudvalget varetager den umiddelbare forvaltning af kommunens overordnede og tværgående it-sikkerhedsforhold.

Stk. 2. Økonomiudvalget er ansvarligt for at fastsætte de uddybende it-sikkerhedsregler for kommunen.

Stk. 3. Ændringer i de uddybende it-sikkerhedsregler, der ikke har væsentlig indflydelse på it-sikkerhedsniveauet eller ikke har økonomiske konsekvenser for forvaltningerne, delegeres til Koncernservice i Økonomiforvaltningen.

Stk. 4. It-sikkerhedsfunktionen orienterer mindst en gang årligt Økonomiudvalget om its-ikkerhedsbrud og status på it-sikkerhedsarbejdet i kommunen, samt afgivne dispensationer for og ændringer af de uddybende it-sikkerhedsregler.

2.3 OVERBORGMESTEREN OG BORGMESTRENE

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

2.4 ØKONOMIFORVALTNINGEN KONCERNSERVICE, IT-SIKKERHEDSFUNKTIONEN, DEN DRIFTSANSVARLIGE

§ 7. Koncernservice udgør et selvstændigt it-sikkerhedsområde under Økonomiforvaltningen. It-sikkerhedsfunktionen er for tiden placeret i Koncernservice. Koncernservice er bl.a. ansvarlig for fællessystemer, drift og It-sikkerhedsfunktionen.

Stk. 2. Koncernservice udfører udvalgte myndighedsopgaver i forhold til hele kommunen. Endvidere udføres it-opgaver efter bestilling fra den øvrige del af kommunen.

Stk. 3. Koncernservice er ansvarlig for at it-sikkerheden på standardydelser fra Koncernservice ydelseskatalog. Ved forvaltningernes bestilling af andre ydelser hos Koncernservice er forvaltningens bestiller (eller den systemejer/projekt-ejer der er ansvarlig for forvaltningens initiativ på området) ansvarlig for sikkerheden i

forbindelse med bestilling af ydelser. herunder at der i nødvendigt omfang indgås aftale om de nærmere vilkår og it-sikkerhedskrav i forbindelse med bestilling af ydelsen. Koncernservice kan rådgive med forslag til sikkerhedsforanstaltninger og aftaler med Den Driftsansvarlige.

Stk. 4. Koncernservice løser it-sikkerhedsopgaver på vegne af henholdsvis forvaltningerne, Intern Revision og Borgerrådgiverinstitutionen. Dette omfatter f.eks.: Varetagelse af systemejerskab. Varetagelse af ansvaret for kommunens fælles netværk. Endvidere står Brugeradministrationen i Koncernservice for oprettelser, lukning og ændring af autorisationer. Dog kan Servicedesken i Koncernservice give nyt password.

Stk. 5 Koncernservice Direktion skal sikre, at der fastsættes uddybende It-sikkerhedsregler for Københavns Kommune. Ændringer i de uddybende It-sikkerhedsregler for Københavns Kommunen skal godkendes af Koncernservice Direktion efter forudgående høring af forvaltningerne. Dispensation fra de uddybende It-sikkerhedsregler kan kun ske på baggrund af en godkendelse fra Koncernservice direktion. 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 driftes af Koncernservice. Endvidere skal Koncernservice fastsætte retningslinjer for integration og netværkskommunikation til eksternt driftede løsninger.

Stk. 6 Direktionen for Koncernservice kan udpege en Driftsansvarlig samt mindst en stedfortræder for denne.

§ 8. It-sikkerhedsfunktionen er placeret i Koncernservice i Økonomiforvaltningen. i Københavns Kommune.

Stk. 2 It-sikkerhedsfunktionen fører det daglige tilsyn med overholdelsen af kommunens it-sikkerhedsbestemmelser og koordinerer kommunens it-sikkerhedsarbejde.

Stk. 3. It-sikkerhedsfunktionen tilrettelægger informations- og uddannelsesaktiviteter for medarbejdere, der varetager kommunens It-sikkerhedsfunktioner.

Stk. 4. It-sikkerhedsfunktionen rådgiver kommunen om it-sikkerhedsmæssige forhold.

Stk. 5. It-sikkerhedsfunktionen kan afkræve enhver medarbejder i kommunen oplysninger, som har betydning for varetagelsen af tilsynsfunktionen.

Stk. 6. It-sikkerhedsfunktionen skal sikre at der sker kontrol af adgangsrettigheder og autorisationer, der er givet til medarbejderne.

Stk. 7. It-sikkerhedsfunktionens opgaver, jf. stk. 1-6, varetages for Brandvæsenets egne it-systemer af en it-sikkerhedsleder for Brandvæsenet.

Stk. 8. It-sikkerhedsfunktionen kan komme med påbud til alle ansatte og enheder i kommunen om hvorledes man skal forholde sig i relation til it-sikkerhed.

Stk. 9. Som led i den almindelige revision af kommunen skal der også foretages revision af it-sikkerheden. It-sikkerhedsfunktionen aftaler med revisor hvorledes it-sikkerhedsrevisionen skal udføres.

§ 9. Den Driftsansvarlige har ansvaret for at de teknikunderstøttende applikationer som anvendes af eller driftes af kommunen, f.eks.; netværk og kommunikation, serverdrift, print, infrastruktur. pc-support, service-management m.m. er i overensstemmelse med de it-sikkerhedsmæssige krav og den til enhver tid gældende it-strategi.

Stk. 2. Den Driftsansvarlige skal i samarbejde med It-sikkerhedsfunktionen, udarbejde it-sikkerhedsforskrifter eller retningslinjer for it-installationer/driftsmiljø og de benyttede netværk. Stk. 3. Den Driftsansvarlige har ansvaret for sikkerheden på it-platforme.

Stk. 4. Den Driftsansvarlige 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 driftes af Koncernservice.

Stk. 5 Den Driftsansvarlige skal sikre, at der bliver taget backup af oplysninger på serverudstyr som driftes af kommunen - efter behov på en ekstern location.

Stk. 6. Den Driftsansvarlige kan dispensere hvis ikke udviklings-, test- og uddannelsesmiljøer med person eller værdi data, som driftes af kommunen holdes adskilt fra produktionsmiljøet.

Stk.7. Såfremt den Driftsansvarlige for henholdsvis Børne- og Ungdomsforvaltningen og Brandvæsnet skal træffe en beslutning vedrørende egne netværk, som kan påvirke sikkerheden i kommunens fælles netværk, skal den Driftsansvarlige i Koncernservice høres, forinden der træffes beslutning.

2.5 FORVALTNINGERNE

§ 10. Direktionen har inden for eget forvaltningsområde ansvar for fastlæggelse af it-sikkerhedsniveauet og for gennemførelse af risikovurderinger. It-sikkerhedsniveauet skal fastlægges indenfor de rammer som er opstillet i It-sikkerhedshåndbogen.

Stk. 2. Direktionen skal inden for eget område iværksætte de foranstaltninger, der er nødvendige for at opnå en tilstrækkelig it-sikkerhed, indenfor de rammer som er opstillet i It-sikkerhedshåndbogen.

Stk. 3. Direktionen er inden for eget område ansvarlig for, at de medarbejdere, som arbejder med It-sikkerhedsopgaver, er i besiddelse af de nødvendige kompetencer.

Stk. 4. Direktionen kan udpege en repræsentant fra ledelsen inden for eget område til at varetage koordineringen med Koncernservice inden for It-sikkerhedsområdet. Den der udpeges skal have et indgående kendskab til henholdsvis områdets organisation, opgaver og systemportefølje. Revisionschefen fra Intern Revision og Borgerrådgiveren fra Borgerrådgiverinstitutionen varetager koordineringen med Koncernservice inden for It-sikkerhedsområdet.

Stk. 5. Direktionen skal inden for eget område udpege en systemejer for it-systemer forvaltningen har ansvaret for samt mindst en stedfortræder for hver systemejer, hvor intet andet er besluttet er det direktionen der er stedfortræder. Koncernservice kan efter aftale overtage systemejerskabet for systemer indenfor den enkelte forvaltnings eget område. Hvis dette sker skal Koncernservice direktion udpege systemejerne samt mindst en

stedfortræder for hver af systemejerne. Direktionen for Koncernservice skal udpege en systemejer for hvert af de fællessystemer, som Koncernservice er ansvarlig for.

Stk. 6. Direktionen for Børne- og Ungdomsforvaltningen kan udpege en Driftsansvarlig samt en stedfortræder for denne for forvaltningens eget pædagogiske netværk, netværksudstyr og servere m.v. Hvis Børne- og Ungdomsforvaltningen ikke har udpeget en Driftsansvarlig varetages opgaven af Koncernservice. I forbindelse med Børne- og Ungdomsforvaltningens snitflader/deling af it-ressourcer med Koncernservice og kommunens administrative net er det den driftsansvarlige i Koncernservice der har ansvaret.

Stk. 7. Ledelsen for Brandvæsnet kan udpege en Driftsansvarlig samt en stedfortræder for denne for Brandvæsnets eget netværk, netværksudstyr og servere m.v. Hvis Brandvæsnet ikke har udpeget en Driftsansvarlig varetages opgaven af Koncernservice. I forbindelse med Brandvæsnets snitflader/deling af it-ressourcer med Koncernservice er det den driftsansvarlige i Koncernservice der har ansvaret.

Stk. 8. Ledelsen for Brandvæsnet udpeger en it-sikkerhedsleder for Brandvæsnets egne it-systemer. It-sikkerhedsfunktionen er stedfortræder for it-sikkerhedslederen for Brandvæsnet.

2.6 SYSTEMEJER

§ 11. Systemejeren skal sikre, at systemets funktionalitet og anvendelse løbende tilpasses og bedst muligt understøtter It-sikkerhedskravene samt forretningens og brugernes behov.

Stk. 2. Før anskaffelse af nye systemer skal systemejeren have godkendt anskaffelsen af systemet. Dette sker i forbindelse med registreringen i kommunens fortegnelse over it-system. I forbindelse med anskaffelsen af systemet skal der foreligge en kortfattet risikoanalyse. Systemejeren har mulighed for at få separat it-sikkerhedsgodkendelse af andet end nye systemer.

Stk. 3. Systemejerskabet skal varetages ud fra kommunens forretningsmæssige behov. Systemejeren er ansvarlig for it-systemets funktionalitet, opbygning, anvendelse og sikkerhedsløsning. Der kan indgås aftale mellem forvaltningen og leverandøren/driftcentret som beskriver niveauet for service. Ændringer i systemer som har snitflader/deling af it-ressourcer med Koncernservice og kommunens administrative net skal ske efter Koncernservice "change" procedure.

Stk. 4. Systemejer er ansvarlig for, at it-systemet kan anvendes mest muligt effektivt og at systemet løbende forbedres, så det bedst muligt understøtter arbejdsopgaverne og kommunens forretningsmæssige behov og lever op til kravene i It-sikkerhedshåndbogen. Der skal etableres processer, der sikre en stabil, effektiv og sikker drift af systemet.

Stk.5. Systemejer er ansvarlig for, at dokumentationen af systemer og processer er ajourført og tilgængelig for relevante medarbejdere. Endvidere har systemejer ansvar for, at der indgås aftale om it-beredskab efter kriterier og retningslinjer fastlagt i it-sikkerhedshåndbogen, og systemejeren skal endvidere bidrage til kommunens it-beredskabsplan.

Stk. 6. Ved brug af eksterne samarbejdspartnere/leverandører er systemejer ansvarlig for, at der indgås en databehandler-/it-sikkerhedsaftale, hvor sikkerhedsforanstaltninger i forbindelse med samarbejdet/leverancerne er beskrevet. Nye aftaler baseres på den standard, der er fastlagt i it-sikkerhedshåndbogen.

Stk. 7. Systemejeren skal sikre, at it-systemet kan logge behandling af data, når det er krævet i de uddybende It-sikkerhedsregler og som følge af gældende lovgivning.

Stk. 8. Hvis integration af it-systemer indebærer en øget it-sikkerhedsrisiko, skal denne risiko vurderes nærmere af systemejeren med inddragelse af den Driftsansvarlige og It-sikkerhedsfunktionen.

Stk. 9. Systemejer står til rådighed for kommunen med oplysninger om it-systemet så vidt som dette er sikkerhedsmæssigt forsvarligt. Stk. 10. Hvis direktionen endnu ikke har udpeget en systemejer, varetages systemejerskabet af lederen af det område, som anskaffer systemet eller af en af denne udpeget projekt-ejer, hvis ansvaret for et systemet er overdraget til en anden leder er det denne som varetager systemejers opgaver. For mindre vigtige systemer, som ikke indeholder væsentlige økonomioplysninger eller følsomme personoplysninger består systemejers rolle i at være system-kontaktperson. System-kontaktpersonens rolle, begrebet system og om der skal udpeges en systemejer for landsdækkende og tværsektorielle systemer, som anvendes af kommunen er beskrevet i de uddybende It-sikkerhedsregler for Københavns Kommune.

2.7 FUNKTIONSADSKILLELSE

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

2.8 AUTORISATIONSANSVARLIGE

§ 13. Den Autorisationsansvarlige varetager de opgaver der er i forbindelse med bestilling af autorisationer og rettigheder til medarbejderne. Dvs. bestilling af oprettelser, flytning, ændringer og sletninger af medarbejdere normalt hos koncernservice brugeradministration. Den autorisationsansvarlige har ansvaret for, at der bestilles de rettigheder, som medarbejderne har behov for arbejdsmæssigt.

Stk. 2 It-sikkerhedsfunktionen fører en liste over hvem der er godkendt som Autorisationsansvarlige. Den lokale leder er ofte den autorisationsansvarlige. Lederen har mulighed for at uddelegere bestillingsopgaven til en bemyndiget medarbejder, som herved bliver autorisationsansvarlig.

2.9 LEDERE

§ 14. 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 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.

Stk. 2. Medarbejderens personaleansvarlige 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-sikkerhedsfunktionen nærmere fastlagt procedure.

Stk. 3. Medarbejderens personaleansvarlige skal orientere medarbejderen om tavshedspligtens indhold og at tavshedspligten er gældende også efter ansættelsesforholdets ophør.

Stk. 4. En leder som er ansvarlig for en omstrukturering skal - i god tid - sørge for at sikre, at der etableres de nødvendige elektroniske kommunikations tiltag. Eksempelvis skal kontorpostkasser, sikre postkasser m.m. nedlukkes hvis en enhed lukkes.

Stk.5. Den lokale ledelse har inden for eget område ansvaret for, at der etableres en tilstrækkelig fysisk sikring af lokaler m.v.

2.10 Alle ansatte

§ 15. Alle medarbejderne skal medvirke til at beskytte kommunens person- og værdioplysninger og skal agere i henhold til dette it-sikkerhedsregulativ og de uddybende it-sikkerhedsregler som fastsættes af It-sikkerhedsfunktionen.

3 Kapitel 3 – Risikostyring

§ 16. It-sikkerhed skal afvejes med hensynet til effektiviteten i opgaveløsningen i forvaltningerne. Stk. 2. Direktionen har inden for eget forvaltningsområde ansvar for at fastlægge et passende it-sikkerhedsniveau ud fra en risikovurdering. For så vidt angår Intern Revision og Borgerrådgiverinstitutionen og Brandvæsnet påhviler ansvaret henholdsvis Revisionschefen, Borgerrådgiveren og Beredskabschefen.

Stk. 3. 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 driftes af Koncernservice. Som led i fastlæggelsen af it-sikkerhedsniveauet har direktionen ansvar for gennemførelse af risikovurderinger.

Stk. 4. Medmindre Borgerrepræsentation konkret beslutter andet fastlægges Borgerrepræsentationens eget it-sikkerhedsniveau af direktionen for Økonomiforvaltningen. Som led i fastlæggelsen af it-sikkerhedsniveauet har Økonomiforvaltningens direktion ansvar for gennemførelse af risikovurderinger af Borgerrepræsentationens eget sikkerhedsniveau.

Stk.5. Direktionen skal tage stilling til, om it-sikkerhedsniveauet er passende. Hvis it-sikkerhedsniveauet ikke er passende, skal der iværksættes tiltag, så det ønskede it-sikkerhedsniveau opnås. Ledelsesrepræsentanten skal orientere vedkommende fagudvalg og It-sikkerhedsfunktionen om direktionens beslutning.

Stk.6. Risikovurderinger skal udarbejdes efter It-sikkerhedsfunktionen anvisninger. It-sikkerhedsfunktionen stiller it-værktøjer m.m. til rådighed for forvaltningerne, og rådgiver forvaltningerne om udarbejdelsen af risikovurderinger.

Stk. 7. Risikovurderinger skal udarbejdes inden udgangen af hvert ulige år og ved væsentlige ændringer i risikobilledet.

Stk. 8. It-sikkerhedsfunktionen udarbejder på baggrund af de respektive risikovurderinger en samlet risikovurdering for kommunen.

Stk. 9. Den samlede risikovurdering skal udarbejdes inden udgangen af 1. kvartal i hvert ulige år. Stk. 10. På baggrund af den samlede risikovurdering træffer Borgerrepræsentationen beslutning om fastlæggelse af kommunens overordnede it-sikkerhedsniveau.

Stk. 11. Som led i risikovurderingen skal It-sikkerhedsfunktionen sikre, at der til enhver tid findes en ajourført fortegnelse over alle væsentlige informationsaktiver.

Stk. 12. Styring af it-sikkerhedshændelser: Ved konstatering af brud eller formodning om brud på it-sikkerhedsbestemmelserne eller andre væsentlige it-sikkerhedshændelser, skal den, der konstaterer disse sikre, at it-sikkerhedsfunktionen underrettes herom. Hvis it-sikkerhedshændelsen har relation til et bestemt system, skal systemejeren også underrettes. Systemejer skal endvidere i relevant omfang orientere den lokale ledelse i forvaltningen.

Stk. 13. It-beredskabsstyring: It-sikkerhedsfunktionen 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. De Driftsansvarlige for Koncernservice, Børne- og Ungdomsforvaltningen og Brandvæsnet har indenfor hver deres område ansvaret for at indgå aftale om it-beredskab.

4 KAPITEL 4 - LOVBESTEMTE KRAV

§17. De respektive direktioner henholdsvis Revisionschefen og Borgerrådgiveren 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.

§ 18. Det daglige ansvar for overholdelsen af reglerne i persondataloven i forbindelse med behandling af personoplysninger påhviler de respektive direktioner henholdsvis Revisionschefen og Borgerrådgiveren.

5 KAPITEL 5 - IKRAFTTRÆDELSE OG ÆNDRINGER

§ 19. It-sikkerhedsregulativet for Københavns Kommune træder i kraft fra godkendelsen af It-sikkerhedsregulativet i Borgerrepræsentationen. Samtidig ophæves it-sikkerhedsregulativet, godkendt af Borgerrepræsentationen den 16. december 2010.

Stk. 2. Koncernservice Direktion skal sikre, at det hvert år, inden udgangen af juni måned, vurderes om der er behov for ændringer i it-sikkerhedspolitikken, i it-sikkerhedsregulativet eller de uddybende It-sikkerhedsregler.

Stk. 3. Ændringer i it-sikkerhedspolitikken og it-sikkerhedsregulativet skal godkendes af Borgerrepræsentationen.

6 Bilag 1 – Definitioner

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

6.1 Autorisationsansvarlig

Leder eller bemyndiget medarbejder, som varetager opgaver i forbindelse med bestilling af autorisationer til medarbejderne.

6.2 Bestiller

I hver forvaltning, er der udpeget en person til at bestille større ydelser hos Koncernservice.

6.3 Den Driftsansvarlige

Ledende medarbejder i Koncernservice, der har det it-sikkerhedsmæssige 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. It-sikkerhedsfunktionen kan kontrollere dette samt fastsætte regler for dette. Såfremt opbygning og anvendelse af it-driftsmiljø og kommunikationsforbindelser vedrører egne netværk opgaver i Børne- og Ungdomsforvaltningen henholdsvis Brandvæsnet, er den Driftsansvarlige en ledende medarbejder fra Børne- og Ungdomsforvaltningen henholdsvis Brandvæsnet, som har ansvaret herfor.

6.4 ISO 27001 - International standart for it-sikkerhed

ISO 27001 handler om Informationsteknologi - Sikkerhedsteknikker – ledelsessystemer for informationssikkerhed(ISMS) – krav. ISO 27002 handler om Informationsteknologi – Sikkerhedsteknikker – Regler for informationssikkerhed (Code of Practice for information security management).

6.5 It-chef

Person på minimum kontorchefniveau, der i hver forvaltning har det overordnede ansvar for forvaltningens it-udvikling og it-understøttelse af forretningsmålene.

6.6 It-sikkerhedshåndbog

It-sikkerhedsreglerne i Kommunen er samlet i en it-sikkerhedshåndbog, som indeholder:

o It-sikkerhedspolitikken

o It-sikkerhedsregulativ for Københavns Kommune

o En række uddybende It-sikkerhedsregler for Københavns Kommune.

6.7 IT-SIKKERHEDSFUNKTION

Enhed som i henhold til beslutning i Borgerrepræsentationen varetager kommunens it-sikkerhedsopgaver i samarbejde med forvaltningerne.

6.8 UDDYBENDE IT-SIKKERHEDSREGLER

It-sikkerhedsregler fastsat af It-sikkerhedsfunktionen til supplering af it-sikkerhedsregulativet med samme gyldighed som it-sikkerhedsregulativet. Der kan anvendes et ISMS (Informations sikkerhedsmæssigt ledelsessystem til styring af it-sikkerhed). De uddybende It-sikkerhedsregler er for tiden en elektronisk udgave af ISO 27001 og 27002, som for tiden findes i den software pakke, som hedder "Secure Aware". (ISO 27001 - 2 er defineret ovenfor).

6.9 IT-SIKKERHEDSLEDER

Medarbejder i It-sikkerhedsfunktionen og Brandvæsnet, som udfører opgaver af it-sikkerhedsmæssig karakter samt fører tilsyn med, at it-sikkerhedsarbejdet bliver udført i overensstemmelse med de til enhver tid gældende it-sikkerhedsbestemmelser.

6.10 IT-SIKKERHEDSREGULATIVET

Regulativ for it-sikkerhed i Københavns Kommune

6.11 IT-SIKKERHEDSPOLITIK

Den af Borgerrepræsentationen vedtagne politik for kommunens it-sikkerhed.

6.12 KOMMUNEN

Københavns Kommune.

6.13 LEDELSESREPRÆSENTANT

En repræsentant for ledelsen i en forvaltning eller et it-sikkerhedsområde, som varetager koordineringen med Koncernservice og sikrer, at der træffes de nødvendige it-sikkerhedsmæssige beslutninger i den pågældende enhed.

6.14 MEDARBEJDER

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.

6.15 PERSONDATALOVEN

Lov nr. 429 af 31. maj 2000, med senere ændringer om behandling af personoplysninger.

6.16 PROJEKT-EJER

En projekt-ejer kan være udpeget til at varetage systemejerens funktion – så længe der ikke er udpeget en systemejer.

6.17 SIKKERHEDSBEKENDTGØRELSEN

Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning med senere ændringer.

6.18 SYSTEM

Systemer som kræver, at forvaltningerne har udpeget en selvstændig systemejer:

o Administrative systemer er systemer, der understøtter forvaltningens administrative opgaver f.eks. systemer som Kør, Lønsystemet, eller Flex.

o Fagsystemer er systemer, der understøtter forvaltningens kerneopgaver, f.eks. systemer som IMU, KMD BYG eller CSC omsorg.

Systemer, hvor forvaltningerne - afhængig af systemets placering og vigtighed – kan vælge selv at udpege en systemejer eller at aftale, at Koncernservice varetager systemejeropgaven:

o Desktop applikationer er lokal installeret software som understøtter forretningen, men ikke i sig selv indeholder data.

o Infrastruktur elementsystemer er systemer, der understøtter kerne it-driften som f.eks. Windows styresystem, antivirus, firewall, eller CMS.

o En systemplatform er en platform til at bygge andre løsninger på, men som i sig selv ikke har noget forretningsfunktionalitet. Fx Oracle SOA Suite, Oracle service bus.

o Apps er små applikationer til mobile enheder som smartphones og tablets. F.eks. systemer som er hentet fra Apple App store.

o Job eller batch-kørsler er små systemer uden brugergrænseflade, der fx trækker data ud om natten og laver beregninger og gemmer data igen.

o En systemgrænseflade er et API som andre systemer kan kommunikere med via protokoller som fx SOAP, REST

o Et undermodul er en ekstra tilføjet komponent eller et delsystem af systemet. o En hjemmeside/website er en løsning der præsentere information via en browser.

6.19 SYSTEMEJER

Medarbejder, der har ansvar for det pågældende itsystems sikkerhedsløsning, opbygning, anvendelse og for beskyttelse af de oplysninger, der indgår i systemet.

6.20 VÆRDIOPLYSNINGER

Oplysninger, der har en væsentlig økonomisk eller forvaltningsmæssig betydning for kommunen.

6.21 VÆSENTLIGE AKTIVER

Aktiver, der indeholder fortrolige eller følsomme informationsaktiver, personoplysninger eller værdioplysninger.