FORRETNINGS-CIRKULÆRE FOR INFORMATIONS-SIKKERHED

FORRETNINGSCIRKULÆRE FOR INFORMATIONS-SIKKERHED

Forretningscirkulære for informationssikkerhed fastsætter regler for informationssikkerheden i Københavns Kommune og er bindende for alle kommunens enheder, herunder forvaltningerne, Borgerrådgiveren, Databeskyttelsesrådgiveren samt Intern Revision.

Forretningscirkulære for informationssikkerhed er udstedt i medfør af Københavns Kommunes Regulativ for informationssikkerhed og er en del af kommunens samlede regelsæt på informationssikkerhedsområdet.

I overensstemmelse med kommunens regelhierarki kan der i tilknytning til alle forhold i dette forretningscirkulære fastsættes yderligere bindende regler i form af fællesadministrative eller forvaltningsspecifikke forretningsgange, ligesom der kan udstedes vejledende retningslinjer.

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

Figur 1: Regelhierarki for Københavns Kommune

Forretningscirkulære for informationssikkerhed er baseret på den internationale standard for informationssikkerhed, ISO27001. ISO-standardens områder er i dette forretningscirkulære fordelt på 10 forskellige sikkerhedsområder:

#	Sikkerhedsområde
1	Informationssikkerhedspolitik ISO 27001 område 5
2	Personalesikkerhed ISO 27001 område 7
3	Styring af aktiver ISO 27001 område 8
4	Adgangsstyring ISO 27001 område 9
5	Fysisk sikring og miljøsikring ISO 27001 område 11
6	Driftssikkerhed ISO 27001 område 12
7	Kommunikationssikkerhed (netværkssikkerhed) ISO 27001 område 10, 13
8	Anskaffelse, udvikling og vedligehold af systemer ISO 27001 område 14
9	Leverandørforhold ISO 27001 område 15
10	Styring af informationssikkerhedsnedbrud samt informationssikkerheds-aspekter ved nød-, beredskabs- og reetableringsstyring ISO 27001 område 16, 17

Inden for de 10 sikkerhedsområder er der fastsat en række 'regler' i kursiv (ISO-kontroller). I tilknytning til reglerne er angivet en uddybende tekst, som i varierende omfang præciserer omfanget af reglen. De enkelte sikkerhedsområder kan i øvrigt som nævnt ovenfor været suppleret af bindende forretningsgange og vejledende retningslinjer.

Københavns Kommune har valgt at have en risikobaseret tilgang til fastlæggelsen af et passende informationssikkerhedsniveau. Heri ligger blandt andet, at de regler, der er fastsat i dette forretningscirkulære er udtryk for det risikobaserede sikkerhedsniveau, der som minimum skal gælde for kommunen. Dette udelukker imidlertid ikke, at der som supplement til reglerne ud fra en risikobaseret vurdering kan være behov for at fastsætte yderligere sikkerhedsforanstaltninger på konkrete områder eller i forhold til bestemte it-systemer. Som tillæg til de enkelte sikkerhedsområder kan der i fællesadministrative forretningsgange fastsættes nærmere regler for risikovurderinger for udvalgte områder.

AKTØRER

Med dette forretningscirkulære fastsættes en rolle- og ansvarsfordeling for aktiviteter ift. informationssikkerhed. Denne beskrives ud fra aktørerne "udførende", "ansvarlig", "rådgivende" og "informeret". Aktørernes ansvar og forpligtelser er beskrevet herunder og gælder for alle aktiviteter i forretningscirkulæret, hvor de er angivet.

Udførende

De(n) aktør(er), som i praksis udfører på aktiviteten.

Ansvarlig

Den aktør, som har det endelige ansvar for, at aktiviteten udføres.

Rådgivende

De(n) aktør(er), som de(n) udførende skal rådføre sig med ift. den pågældende aktivitet.

Det fremgår af afsnitsteksten i det tilhørende afsnit, hvorvidt udførende er forpligtet til at rådføre sig med de(n) rådgivende ved en angivelse af, hvorvidt aktiviteten udføres i samarbejde med de(n) rådgivende.

Informeret

De(n) aktør(er), som de(n) udførende skal informere om progression i udførelsen af aktiviteten.

INDHOLD

Forretningscirkulære for informationssikkerhed 1

Aktører 3

Udførende 3

Ansvarlig 3

Rådgivende 3

Informeret 3

1. Sikkerhedsområde 1 – informationssikkerhedspolitik 6

1.1. Organisering af informationssikkerhed 6

1.2. Generelt for informationssikkerhed i kommunen 6

2. Sikkerhedsområde 2 - Personalesikkerhed 7

2.1. Ved ansættelsen 7

2.2. Under ansættelsen 7

2.3. Ved ansættelsesforholdets ophør 8

3. Sikkerhedsområde 3 - Styring af aktiver 9

3.1. Fortegnelse over informationsaktiver 9

3.2. Ansvar for informationsaktiver 10

3.3. Medarbejdernes brug af informationsaktiver 10

3.4. Tilbagelevering og ombytning af aktiver 11

3.5. Klassifikation af data 11

3.6. Opbevaringsperiode for data (sletning og arkivering) 12

4. Sikkerhedsområde 4 - Adgangsstyring, brugerrettede politikker mm. 13

4.1. Funktionsadskillelse 13

4.2. Adgang til netværk og netværkstjenester 13

4.3. To-faktor-autentifikation og adgangskoder 16

4.4. Brugerrettede instrukser 18

5. Sikkerhedsområde 5 - Fysisk sikkerhed og miljøsikring 20

5.1. Fysisk sikkerhed 20

5.2. Sikre og kontrollerede områder 20

5.3. Åbne administrationsområder og modtagelsesområder 21

5.4. Åbne og delvist åbne områder 21

5.5. Tv- og videoovervågning 21

5.6. Beskyttelse af udstyr 22

5.7. Forsyningssikkerhed 22

5.8. Transmission af data 23

5.9. Bortskaffelse af it-udstyr 23

6. Sikkerhedsområde 6 - Driftsikkerhed 24

6.1. Driftsafviklingsprocedurer ... 24
6.2. Kapacitetsstyring ... 24
6.3. Skadevoldende programmer og ondsindet kode ... 24
6.4. Backup ... 25
6.5. Logning og overvågning ... 26
7. Sikkerhedsområde 7 - Kommunikationssikkerhed (netværkssikkerhed) ... 29
7.1. Styring af netværkssikkerhed ... 29
7.2. Kryptografi ... 29
7.3. Elektronisk handel og betaling ... 30
7.4. Ind- og uddata ... 30
8. Sikkerhedsområde 8 - Anskaffelse, udvikling og vedligeholdelse ... 31
8.1. Sikkerhed i forhold til indkøb og nyudvikling af systemer ... 31
8.2. Ændringer af systemer mv. ... 31
8.3. Styring af programkildekode i større driftsmiljøer ... 32
8.4. Adskillelse af udviklings- og testmiljøer fra produktionsmiljøer ... 32
8.5. Udførelse af test ... 32
8.6. Anvendelse af testdata ... 32
9. Sikkerhedsområde 9 - Leverandørforhold ... 34
10. Sikkerhedsområde 10 - Styring af informationssikkerhedshændelser samt informationssikkerhedsaspekter mv. ... 35
10.1. Ansvar og procedurer ... 35
10.2. Rapportering af informationssikkerhedshændelser ... 35
10.3. Beredskabsstyring ... 36
10.4. Risikovurderinger af it-systemer og it-infrastruktur ... 36
10.5. It-revisioner ... 37
Ændring og ajourføring ... 38

1. SIKKERHEDSOMRÅDE 1 – INFORMATIONSSIKKERHEDSPOLITIK

1.1. Organisering af informationssikkerhed

Ansvar og roller på informationssikkerhedsområdet skal være klart defineret, godkendt af Økonomiudvalget og kommunikeret til medarbejdere.

Ansvaret for opfyldelsen af reglerne på informationssikkerhedsområdet er fastsat i Forretningscirkulære for organisering af informationssikkerhed i Københavns Kommune, som omfatter alle kommunens forvaltninger, Borgerrådgiveren, Databeskyttelsesrådgiveren og Intern Revision.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Klar definition af ansvar og roller på informations-sikkerhedsområdet	ØKF (Koncern IT)	Økonomiudvalget	-	Forvaltningerne, Borgerrådgiveren, Databeskyttelses-rådgiveren og Intern Revision

1.2. Generelt for informationssikkerhed i kommunen

Der skal fastsættes passende tekniske og organisatoriske sikkerhedsforanstaltninger med henblik på at sikre kommunens informationsaktiver.

Reglen om at fastsætte passende tekniske og organisatoriske sikkerhedsforanstaltninger er et tværgående princip for alt informationssikkerhedsarbejde i kommunen og gælder uanset, om der er fastsat andre udtrykkelige informationssikkerhedsregler for et givent område. Den nævnte regel følger også af de enkelte forvaltningers pligt til at varetage informationssikkerheden inden for eget område, jf. § 7, stk. 1, i Forretningscirkulære for organisering af informationssikkerhed.

Med 'kommunens informationsaktiver' sigtes navnlig til infrastrukturelementer, it-systemer, computere, mobile enheder, printere, scannere og data, jf. afsnit 3.1. Når 'data' er omfattet af informationsbegrebet, har det endvidere den betydning, at f.eks. personoplysninger om borgere skal sikres, og dermed skal hensynet til borgerne også inddrages i kommunens fastlæggelse af et passende informationssikkerhedsniveau.

Med 'passende' sigtes der endvidere til, at hver forvaltning ud i en risikobaseret afvejning skal inddrage hensynet til sikringen af kommunens aktiver – det vil med andre ord sige, at jo større risiko, der er forbundet med et område, jo højere skal sikkerhedsniveauet være.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Fastsættelse af et passende teknisk og organisatorisk informationsniveau	Forvaltningen	Forvaltningens direktion	Forvaltningens digitaliserings-enhed og evt. ØKF (Koncern IT)	Forvaltningens digitaliserings-enhed

2. SIKKERHEDSOMRÅDE 2 - PERSONALESIKKERHED

2.1. Ved ansættelsen

Det påhviler den nærmeste leder at sikre, at alle nye medarbejdere i forbindelse med ansættelse instrueres i relevante informationssikkerhedsregler og regler for persondatabeskyttelse. Det skal i øvrigt sikres, at de ansatte er bekendt med, at de er underlagt reglerne om tavshedspligt, jf. de til en hver tid gældende bestemmelser i forvaltningsloven og straffeloven.

For øvrige krav til ansættelse henvises til Forretningscirkulære – Løn og Personale og Forretningscirkulære for persondatabeskyttelse. Medarbejderen skal i forbindelse med sin tiltræden informeres om kommunens regler for informationssikkerhed og databeskyttelse samt, hvis dette er relevant, gennemgå kommunens uddannelsesprogram om informationssikkerhed og databeskyttelse.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Instruktion af nye medarbejdere om informations-sikkerhedsregler	Nærmeste leder	Forvaltningens direktion	Forvaltningens digitaliserings-enhed og evt. ØKF (Koncern IT)	Forvaltningens digitaliserings-enhed
Informere om tavshedspligt	Nærmeste leder	Forvaltningens direktion	Forvaltningens forvaltningsretlige funktion	-

2.2. Under ansættelsen

Alle medarbejdere i Københavns Kommune med adgang til kommunens it-systemer, enheder og data skal være bekendt med egne opgaver og eget ansvar i forhold til informationssikkerhed og databeskyttelse, jf. afsnit 2.1.

Alle medarbejdere får ved adgang til kommunens netværk brev om kommunens informationssikkerhedsregler og et link til kommunens regelsæt for informationssikkerhed, som de har pligt til at læse. Alle medarbejdere med adgang til kommunens it-systemer og data skal være orienteret om kommunens regler for informationssikkerhed og databeskyttelse.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Instruktion af medarbejdere om ansvar ift. informations-sikkerhedsregler	Nærmeste leder	Forvaltningens direktion	Forvaltningens digitaliserings-enhed og evt. ØKF (Koncern IT)	Forvaltningens digitaliserings-enhed

2.3. Ved ansættelsesforholdets ophør

Ved ansættelsens ophør gøres den afgående medarbejder bekendt med forhold, der rækker ud over ansættelsen, herunder tavshedspligt.

Tavshedspligt og fortrolighed vedr. kommunens data gælder også efter ansættelsesforholdets ophør, jf. de til en hver tid gældende bestemmelser i forvaltningsloven og straffeloven.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Instruktion af fratrædende medarbejdere om tavsheds-pligt	Nærmeste leder	Forvaltningens direktion	Forvaltningens forvaltningsretlige funktion	-

3. SIKKERHEDSOMRÅDE 3 - STYRING AF AKTIVER

3.1. Fortegnelse over informationsaktiver

Kommunen skal føre en ajourført fortegnelse over alle væsentlige informationsaktiver.

Alle forvaltninger skal – som led i varetagelsen af sit ansvar for informationssikkerhedsområdet inden for eget område, jf. Forretningscirkulære for organisering af informationssikkerhed § 7, stk. 1 – have et overblik over forvaltningens informationsaktiver med henblik på at kunne opretholde et passende informationssikkerhedsniveau.

Økonomiforvaltningen skal endvidere – som led i varetagelsen af sit ansvar for de tværgående opgaver på it- og informationssikkerhedsområdet i kommunen, jf. Forretningscirkulære for organisering af informationssikkerhed § 11, stk. 1 – have et overblik over informationsaktiver med henblik på at kunne opretholde et passende informationssikkerhedsniveau.

I den forbindelse skal der føres en fortegnelse over de væsentligste informationsaktiver:

- Infrastrukturelementer, f.eks. netværksaktiver, kabling, servere, routere og andet hardware.
- Systemer, f.eks. it-systemer, generiske administrative systemer, tværgående fagsystemer, jf. definitionen i Forretningscirkulære for it-anskaffelser afsnit 6
- Computere, herunder bærbare pc'ere
- Mobile enheder, f.eks. telefoner, smartphones og tablets.
- Andre væsentlige it-aktiver, f.eks. printere og scannere.
- Data, navnlig personoplysninger

Placeringen af informationsaktiver, som efter en konkret vurdering, kan betegnes som særligt kritiske for kommunens oprettelse af et passende informationssikkerhedsniveau, skal ligeledes registreres. Om placering af informationsaktiver i sikre områder se afsnit 5.1.

For så vidt angår registrering af personoplysninger, henvise Forretningscirkulære om databeskyttelses - dokumentation og compliance om til registrering af behandlingsprocesser og datastrømme.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Fortegnelse over alle væsentlige it-aktiver	Forvaltningens digitaliserings-enhed	Forvaltningen som har ansvar for det pågældende it-aktiv	ØKF (Koncern IT)	-

3.2. Ansvar for informationsaktiver

Ansvar for kommunens informationsaktiver skal være klart defineret.

Det skal fremgå af de i punkt 3.1. nævnte fortegnelser, hvilken forvaltningen der har ansvaret de pågældende informationsaktiver, som Københavns Kommune ejer.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Klar definition af ejerskab af og ansvar for it-aktiver	Forvaltningens digitaliserings-enhed	Forvaltningen som har ansvar for det pågældende it-aktiv	ØKF (Koncern IT)	-

3.3. Medarbejdernes brug af informationsaktiver

Kommunens informationsaktiver kan alene anvendes til formål, der ligger inden for kommunens virkeområde.

Kommunens informationsaktiver kan som udgangspunkt kun anvendes til arbejdsrelaterede formål og aktiverne må ikke anvendes på en måde, der udsætter kommunen for unødvendige sikkerhedsrisici. Der skal fastsættes nærmer regler for medarbejdernes arbejdsrelaterede brug af bl.a. mobile enheder, internet, e-mail, programmer og onlinetjenester.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Ansvar for at it-aktiver anvendes til arbejdsrela-terede formål	Forvaltningens digitaliserings-enhed og de enkelte ansatte	Forvaltningen som har ansvar for det pågældende it-aktiv	ØKF (Koncern IT)	-

Medarbejdere kan dog anvende kommunens informationsaktiver til private formål, hvis kommunen har tilladt en sådan brug, og hvis privat anvendelse ikke strider mod gældende lovgivning og kommunens informationssikkerhedsregler.

For så vidt angår medarbejdernes privat brug af kommunens aktiver, skal der fastsættes nærmere regler for acceptabel brug af brug af internet, programmer og onlinetjenester samt opbevaring af oplysninger på kommunens drev. Hvis der opstår behov for det, kan der i en fællesadministrativ forretningsgang også fastsættes nærmere regler for medarbejdernes brug af egne mobile enheder i arbejdsrelaterede sammenhænge.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Ansvar for at privat brug af informationsaktiver alene sker anerkendte og lovlige formål	Forvaltningers digitaliserings-enhed og de enkelte ansatte	Forvaltningen som har ansvar for det pågældende it-aktiv	ØKF (Koncern IT)	-

3.4. Tilbagelevering og ombytning af aktiver

Udleveret udstyr afleveres og rettigheder deaktiveres, senest når ansættelse- eller andet kontraktforhold ophører mellem medarbejder/leverandør/bruger og kommunen.

Udleveret udstyr skal senest ved ansættelses-/kontrakt-/aftaleforholdets ophør indsamles af nærmeste leder eller af en nærmere anvist person/funktion. Dette gælder ligeledes udstyr, der ombyttes og er omfattet af den obligatoriske serviceaftale mellem forvaltningerne og Koncern IT.

Ved akut ophør må data på arbejdsstationer, mobilt it-udstyr og e-mailkonti ikke slettes, men skal arkiveres med passende sikkerhedsforanstaltninger (efter gældende praksis) for eventuelle videre undersøgelser.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Tilbagelevering af udstyr	Nærmeste leder eller den kontraktansvarlige	Forvaltningens direktion	-	-

3.5. Klassifikation af data

Kommunens klassifikation af information og data følger dansk lovgivning, herunder navnlig databeskyttelsesforordningen, forvaltningsloven og offentlighedsloven. Hertil kan der anvendes begreber, der alene knytter sig til kommunens egen klassificering.

I relation til informationssikkerhed klassificeres kommunens oplysninger som følger:

- Almindelige personoplysninger: For definition af almindelige personoplysninger henvises til forretningscirkulære om persondatabeskyttelse – de registreredes rettigheder
- Fortrolige og følsomme personoplysninger: For definition af almindelige personoplysninger henvises til forretningscirkulære om persondatabeskyttelse – de registreredes rettigheder
- Værdidata: Omfatter oplysninger, der er beskyttelsesværdige fordi de har en væsentlig økonomisk eller forvaltningsmæssig værdi for kommunen eller andres omdømme (f.eks. staten og private virksomheder).
- Åbne data: Oplysninger, der ikke er omfattet af ovenstående

Et eventuelt behov for at beskytte data i de forskellige kategorier kan være begrundet i,

1. at oplysninger ikke kommer til uvedkommendes kendskab (fortrolighed),
2. at oplysninger ikke uretmæssigt ændres (integritet) eller
3. at oplysningerne er tilgængelige for kommunen eller andre (tilgængelighed).

Hvor beskyttelsesbehov for personoplysninger som udgangspunkt ikke ændrer sig over tid, kan beskyttelsesbehovet for værdidata potentielt ændres sig. Det kunne f.eks. være mødemateriale, der er fortroligt frem til afholdelsen af et specifikt møde, hvorefter det kunne blive offentligt tilgængeligt. Behovet for tilknyttede sikkerhedsforanstaltninger kan derfor potentielt ændres sig i takt med beskyttelsesbehovet for oplysninger ændrer sig.

I kommunen gælder der i almindelighed samme regler for beskyttelse af værdidata og for beskyttelse af fortrolige og følsomme personoplysninger.

3.6. Opbevaringsperiode for data (sletning og arkivering)

Værdidata og personoplysninger skal opbevares og sikres indtil det ikke længere er nødvendigt for kommunen at have oplysningerne.

Personoplysninger (både almindelige, fortrolige og følsomme) skal slettes eller gøres anonyme, når det ikke længere er nødvendigt for kommunen at have oplysningerne. Det er de enkelte forvaltningers ansvars at vurdere, hvor længe det er nødvendigt at opbevare oplysningerne ud fra de formål, som oplysningerne oprindelig blev indsamlet til. Der henvises i øvrigt til reglerne om opbevaring, sletning og legitime formål i navnlig databeskyttelsesforordningens artikel 5.

Værdidata, om ikke omfatter personoplysninger, skal som udgangspunkt ikke slettes. Efter en konkret vurdering kan det imidlertid være nødvendigt slette sådanne oplysninger, hvis disse oplysninger ikke er nødvendige for kommunen eller andre, og hvis opbevaringen af data i sig selv kan udgøre en sikkerhedsrisiko for kommunen eller andre.

Åbne data kan men skal ikke nødvendigvis slettes, når det ikke længere er nødvendigt for kommunen at have oplysningerne.

Arkivering af oplysninger efter arkivlovens regler herom, kan sidestilles med sletning.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Sletning af data	Forvaltningen	Forvaltningens direktion	Databeskyttelses-rådgiveren	-

4. SIKKERHEDSOMRÅDE 4 - ADGANGSSTYRING, BRUGERRETTEDE POLITIKKER MM.

4.1. Funktionsadskillelse

Modstridende funktioner skal, hvis det er teknisk muligt, altid adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af data og øvrige aktiver i kommunen.

Hvis det ikke er muligt at understøtte en teknisk funktionsadskillelse, skal der etableres passende tekniske organisatoriske foranstaltninger med henblik på at forebygge muligt misbrug. Sådanne kompenserende foranstaltninger kan være brug af f.eks. kontrol af logs eller instrukser om at bestemte opgaver skal udføres af to personer i forening. De kompenserende foranstaltninger skal modsvare graden af risiko for misbrug.

I kravet om funktionsadskillelse ligger også et krav om, at en medarbejder ikke kan tildele systemadgang og -rettigheder til sig selv, men at sådanne rettigheder skal tildeles af vedkommendes leder eller den udpegede autorisationsansvarlige.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Teknisk funktions-adskillelse	Den anskaffende enhed	Forvaltningens direktion	Forvaltningens digitaliseringsenhed og eventuelt Koncern IT	-

4.2. Adgang til netværk og netværkstjenester

Brugere i kommunen skal kun have adgang til de netværk, netværkstjenester, systemer m.m., som de specifikt er autoriserede til at anvende.

Al adgang til kommunens it-systemer, servere, netværk og pc'er, der indeholder personoplysninger eller værdidata, skal være betinget af konkrete autorisationer. Dette gør sig gældende for alle brugere, herunder medarbejdere, eksterne samarbejdspartnere og automatiserede løsninger (RPA). Som udgangspunkt skal adgange altid gives via kommunens løsning til tildeling af autorisationer.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Adgang til relevante systemer	Nærmeste leder eller kontraktansvarlige	Forvaltningens direktion	Koncern IT	-

4.2.1 Autorisationsansvarlige

Den autorisationsansvarlige har ansvaret for at bestille rettigheder, som den ansvarlige leder for brugeren vurderer, at der er et arbejdsrelateret behov for.

Opgaven med bestilling af rettigheder varetages af en autorisationsansvarlig. Den autorisationsansvarlige skal – i samarbejde med lederen af det relevante fagområde – sikre, at de tildelte rettigheder alene afspejler det arbejdsrelaterede behov.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Bestilling af rettigheder	Den autorisations-ansvarlige	Brugerens nærmeste leder	Koncern IT	-

4.2.2 Autorisationer til eksterne samarbejdspartnere

Eksterne samarbejdspartnere, som har brug for adgang til et it-system af hensyn til drifts-, udviklings- og vedligeholdelsesopgaver, skal autoriseres hertil.

Autorisation af eksterne samarbejdspartnere må kun finde sted, såfremt en entydig identifikation af den pågældende medarbejder kan finde sted. Dette kan eventuelt ske i form af cpr-nummer-identifikation. Autorisation skal altid ske på baggrund af en anmodning fra en autorisationsansvarlig i samarbejde med den ansvarlige for aftaleindgåelsen (alternativt en medarbejder, som har fået uddelegeret ansvaret), der sørger for at indhente de fornødne oplysninger i forbindelse med bestillingen.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Bestilling af rettigheder	Den autorisations-ansvarlige	Den kontrakt-ansvarlige	Koncern IT	-

4.2.3 Brugeroprettelser

Til brug for autorisation skal der til systemer udarbejdes dokumentation for den løbende tildeling af rettigheder samt retningslinjer, der blandt andet skal beskrive hvilke medarbejdergrupper, som beskriver kriterier for tildelingen af adgang til it-systemet.

Der skal til stadighed foreligge retvisende og opdateret dokumentation for, hvem der konkret er tildelt rettigheder i henhold til udarbejdede og ledelse godkendte retningslinjer. Retningslinjerne for autorisationer skal som minimum indeholde beskrivelser af, hvilke roller og rettigheder, der kan tildeles brugere, og efter hvilke kriterier rettighederne skal tildeles.

Følgende kriterier gælder endvidere altid for brugeroprettelser:

- brugere skal ved oprettelse tildeles et unikt brugernavn
- brugernavnet er personligt og må ikke overdrages til andre
- de enkelte brugernavne skal genereres i kommunens dertil indrettede system
- ved oprettelse eller nulstilling af adgangskode skal brugeren tildeles en midlertidig adgangskode, som skal ændres ved første anvendelse
- midlertidige adgangskoder skal opfylde de gældende krav til adgangskoder

- udlevering af midlertidige adgangskoder skal ske på en sikker måde
- adgangskoder som udleveres over internettet eller andre åbne netværk skal krypteres
- brugeren kan som udgangspunkt ikke tildeles lokaladministratorrettigheder på arbejds-pc'er.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Udarbejdelse af retnings-linjer for oprettelse af brugere	Bruger-administrationen	Bruger-administrationen i samarbejde med den forvaltning som er ansvarlig for systemet	Koncern IT	-

4.2.4 Ændring af brugerrettigheder

Hvis en brugers arbejdsopgaver ændrer sig på en sådan måde, at behovet for autorisationer ændrer sig, skal den nærmeste leder sikre, at brugeren kun har autorisationer, der er et arbejdsmæssigt behov for.

Ved organisatoriske omplaceringer eller ved andre ændringer i arbejdsopgaver skal den leder, som fremover, har det ledelsesmæssige ansvar for den pågældende bruger sikre, at de nødvendige ændringer af brugerrettigheder bestilles.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Bestilling af ændrede bruger-rettigheder	Den autorisations-ansvarlige	Brugerens nærmeste (nye) leder	Koncern IT	-

4.2.5.Nedlæggelse af brugerrettigheder

Ophører ansættelsesforholdet skal brugerrettighederne nedlægges, og ved orlov, længerevarende sygdom eller andet fravær skal brugerens adgangsrettigheder deaktiveres.

Brugerens nærmeste leder skal sikre, at brugerrettighederne nedlægges eller deaktiveres, hvis ansættelsesforholdet ophører eller hvis brugeren i en længere periode ikke kan eller skal varetage de opgaver, hvor til brugerrettighederne knytter sig.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Nedlæggelse af bruger-rettigheder	Den autorisations-ansvarlige	Brugerens nærmeste leder	Koncern IT	-

4.2.6 Styring af privilegerede adgangsrettigheder

Privilegerede rettigheder til it-systemer skal være dokumenterede og brugen skal registreres ved logning.

Med 'privilegerede rettigheder' forstås udvidede brugerrettigheder til et system, herunder systemadministratorrettigheder. Tildeling af sådanne privilegerede rettigheder skal til enhver tid

være dokumenterede og må kun anvendes i begrænset omfang. Dertil kommer, at der altid skal føres log over anvendelsen af privilegerede rettigheder.

Logning skal i øvrigt ske i overensstemmelse med reglerne i afsnit 6.5.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Dokumentation for tildeling, brug og kontrol af privilegerede rettigheder	Brugerens nærmeste leder	Forvaltningens direktion	Koncern IT	-

4.2.7 Privilegerede administrative adgange til it-infrastrukturen

Privilegerede administrative adgange til it-infrastrukturkomponenter mv. skal være dokumenterede og brugen heraf skal så vidt muligt registreres.

Med 'privilegerede administrative adgange til it-infrastrukturkomponenter mv.' forstås muligheden for at have adgang til nødvendig systemkonfiguration, installation, backup, reset mv. af centrale services og styringsprodukter i infrastrukturen. Sådanne udvidede adgange skal til enhver tid være dokumenterede og må kun anvendes, når det er strengt nødvendigt for at sikre en stabil og sikker drift af it-infrastrukturen. Anvendelsen af privilegerede administrative adgange bør logges i det omfang, at dette er en teknisk mulighed.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Dokumentation for tildeling, brug og kontrol af privilegerede administrative adgange	Brugerens nærmeste leder	Forvaltningens direktion	Koncern IT	-

4.2.8 Tilsyn med autorisationer

Der skal mindst hver sjette måned føres tilsyn med om tildelte autorisationer afspejler medarbejdernes arbejdsmæssige behov.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Tilsyn med autorisationer	Nærmeste leder	Forvaltningens direktion	Koncern IT	-

4.3. To-faktor-autentifikation og adgangskoder

4.3.1 To-faktor-autentifikation

Enhver adgang til kommunens it-systemer og administrative netværk må som udgangspunkt kun foregå ved brug af to-faktor-login.

Adgangen til kommunens administrative netværk og it-systemer, herunder kommunens data, skal ske ved, at brugeren identificerer sig ved brug af to forskellige faktorer:

1. noget som brugeren ved (brugernavn i kombination med kodeord)
2. noget som brugeren har (f.eks. enheder som er "kendt" af Koncern IT's MDM-løsning, opkalds- og sms-løsninger, godkender-applikationer samt hardware-tokens)

Kommunen anvender ikke biometri som en egentlig faktor for adgang til it-systemer, men biometri kan efter omstændigheder anvendes til at logge på enheder, som allerede er kendt af kommunen, jf. punkt 1 og 2.

Det kan efter omstændighederne være forsvarligt at fravige kravet om to-faktor-login, hvis der er tale om en ekstern it-løsning, som separeret for kommunens øvrige systemer og netværk. Det kunne f.eks. være i forhold til it-løsninger anvendt på skoler eller andre borgervendte løsninger, hvor der ikke logges på med et medarbejder-login. Det er dog en forudsætning, at sådanne løsninger ikke indeholder værdidata, fortrolige eller følsomme personoplysninger.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Implementering af to-faktor-login	Den anskaffende enhed	Forvaltningens direktion	Koncern IT	-

4.3.2 Adgangskoder

Adgangen til kommunens informationsaktiver må kun ske ved forsvarlig brug af adgangskoder.

Adgang til kommunens informationsaktiver, jf. afsnit 3.1., må kun ske ved forsvarlig brug af adgangskoder, hvorved der forstås, at sådanne koder er personlige og strengt fortrolige og ikke må udlånes til andre.

Der gælder i øvrigt følgende krav til adgangskoder:

- under hensyn til karakteren af det pågældende system/komponent, f.eks. karakteren af indeholdte oplysninger og systemets funktioner, skal adgangskoder til enhver tid være af passende længde og kompleksitet (styrke)
- der kan etableres tekniske foranstaltninger med henblik på at sikre en passende styrke af adgangskoder
- adgang til systemer skal blokeres senest efter 5 mislykkede login-forsøg og håndhæves i mindst 30 min., medmindre det efter en konkret vurdering findes sikkerhedsmæssigt forsvarligt at acceptere flere mislykkede login-forsøg
- adgangskoder skal skiftes ved mistanke om kompromittering, dog mindst en gang årligt.

Alle arbejdsstationer skal have en skærmlås, der aktiveres automatisk ved inaktivitet med krav om indtastning af adgangskode. Tidsrummet for inaktivitet afhænger af karakteren af oplysninger i det pågældende system og systemets funktioner i øvrigt.

Hvis adgangskoden kompromitteres, eller der opstår mistanke herom, er det medarbejderens ansvar straks at ændre kodeordet og underrette Koncern IT herom.

Muligheden for at gemme passwords i browsere eller andre applikationer skal deaktiveres. Koncern IT kan dog tillade, at passwords bliver gemt i single sign on-løsninger.

Standardadgangskoder fra systemleverandører skal ændres i forbindelse med installation af nye it-systemer.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Implementering af principper for adgangskoder	Den anskaffende enhed	Forvaltningens direktion	Koncern IT	-

4.3.3 Alternativer til adgangskoder

Der kan anvendes alternativer til adgangskoder, hvis den pågældende løsning har mindst den samme grad af sikkerhed som brug af adgangskoder.

Indtastning af adgangskode kan erstattes af brug af id-kort eller lignende autentifikationsmekanisme med et tilsvarende eller højere sikkerhedsniveau.

Ligeledes kan det efter en konkret vurdering være forsvarligt at anvende løsninger baseret på biometri.

Hvis et alternativt til adgangskoder ikke indgår i en it-anskaffelse, og derfor inddrages i it-anskaffelsesvurderingen og er omfattet af en ibrugtagningstilladelse, indebærer ibrugtagningen af så sådan løsning, at der skal foretages en fornyet vurdering af Koncern IT, jf. Forretningscirkulære for organisering af informationssikkerhed og Forretningscirkulære for it-anskaffelser.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Implementering af alternativer til adgangskoder	Den anskaffende enhed	Forvaltningens direktion	Koncern IT	-

4.4. Brugerrettede instrukser

Brugere med adgang til kommunens systemer, netværk, applikationer, mobile enheder m.m. skal følge kommunens instruks om anvendelse.

Efter en risikobaseret betragtning har forvaltningerne ansvar for at instruere medarbejdere med henblik på at sikre kommunens systemer, netværk, applikationer, mobile enheder m.m. (informationsaktiver).

Kommunens it-brugere skal følge såvel generelle som forvaltningsspecifikke instrukser om anvendelsen af sådanne informationsaktiver både internt i kommunen og i det offentlige rum.

Instrukser kan evt. meddeles som fællesadministrative eller forvaltningsspecifikke forretningsgange.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Forvaltningsspecifikke instrukser	Den enkelte forvaltning	Den enkelte forvaltning	Koncern IT	Medarbejdere i den enkelte forvaltning
Generelle instrukser	ØKF	ØKF	Koncern IT	Forvaltningerne

4.4.1. Kommunikation med borgere, virksomheder og myndigheder

Kommunens kommunikation med borgere, virksomheder og andre myndigheder skal ske på en sikker måde, således at der særligt sikres, at oplysninger ikke kommer til uvedkommendes kendskab.

Der skal i en fællesadministrativ forretningsgang fastsættes nærmere regler om kommunikation med borgere, virksomheder og myndigheder. I den forbindelse skal relevant lovgivning iagttages, herunder navnlig regler om beskyttelse af personoplysninger. Forretningsgangen skal som minimum omfatte regler om sikker kommunikation via e-mail, blanketløsninger og sociale medier.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Implementering af sikre kommunikationsl-øsninger	Den anskaffende enhed	Forvaltningens direktion	Koncern IT	-
Udarbejdelse af forretningsgang om sikker kommunikation	Koncern IT	ØKF	Databeskyttelses-rådgiveren	Forvaltningerne
Implementering af instruks om sikker kommunikation	Forvaltningen	Forvaltningens direktion	Koncern IT	

4.4.2 Brug af mobilt udstyr, eksterne lagringsmedier og fjernarbejdspladser

> *Personoplysninger må kun opbevares på mobile enheder og andre eksterne lagringsmedier (enheder), hvis der er etableret passende teknisk beskyttelse, og hvis brugeren er instrueret i korrekt anvendelse.*

Opbevaring af værdi- eller personoplysninger på eksterne lagringsmedier udgør en sikkerhedsrisiko. Sikkerhedsrisikoen skal håndteres gennem passende tekniske sikkerhedsforanstaltninger og gennem instruktion af brugerne af mediet.

Mobilt udstyr *med potentiel dataadgang*, f.eks. telefoner, tablets og computere, er personligt og må ikke deles med andre. Mobile enheder skal låses, når de forlades, og sikres med kode eller tilsvarende sikkerhedsforanstaltning, f.eks. adgangsspærring baseret på biometri.

Sikring af mobile enheder og løsninger *med potentiel dataadgang* skal ske efter fælles standarder, herunder i forhold til to-faktor-login, kryptering, adgangsstyring og nødprocedure for fjernelse af person- og værdidata ved bortkomst. Hvis dette ikke er teknisk muligt, skal der iværksættes passende tekniske og organisatoriske kompenserende foranstaltninger.

Opbevaring af værdidata samt fortrolige og følsomme personoplysninger på eksterne lagringsmedier *uden dataadgang*, f.eks. usb-nøgler, cd'er, dvd'er, eksterne harddiske, hukommelseskort og lignende skal sikres, f.eks. i aflåste bokse eller ved kryptering af indhold.

Ved opbevaring af værdidata og personoplysninger på mobile enheder (*med og uden potentiel dataadgang*) skal det ligeledes sikres, at eventuelle krav om opbevaringsfrister og logning overholdes. Sådanne enheder må øvrigt heller ikke forlades i offentlige rum.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Sikring af og instruks om opbevaring af data på mobile enheder	Forvaltningen	Forvaltningens direktion	Koncern IT	-

5. SIKKERHEDSOMRÅDE 5 - FYSISK SIKKERHED OG MILJØSIKRING

5.1. Fysisk sikkerhed

Der skal etableres en passende fysisk sikkerhed generelt og særligt på kritiske områder, f.eks. databehandlingssteder og andre steder, der indeholder persondata eller værdioplysninger.

Københavns Kommunes fysiske lokationer kan opdeles i følgende områder:

- Sikre områder: områder med begrænset adgang for kommunale medarbejdere. Krydsfelter, serverrum og andre steder, hvor netværksudstyr er placeret, anses altid som sikre områder.
- Kontrollerede områder: lukkede administrationsområder med adgang for kun kommunale medarbejdere eller autoriserede eksterne samarbejdspartnere.
- Åbne administrationsområder: områder med begrænsede krav til sikkerheden, men som offentligheden ikke skal have adgang til (f.eks. Rådhuset).
- Modtagelsesområder: områder hvor borgere mødes med kommunale medarbejdere (f.eks. borger-, kultur- og jobcentre, sociale aktivitetstilbud, børnefamilieenheder og voksenenheder, genoptræningsenheder mv.).
- Delvist åbne områder: områder hvor visse borgere har fri adgang, og som ikke nødvendigvis er under opsyn (f.eks. plejehjem og institutioner).
- Åbne områder: områder med fri borgeradgang, og som ikke nødvendigvis er under opsyn (f.eks. biblioteker og sportshaller).

Der skal inden for hver forvaltning fastsættes nærmere regler for sikring af forvaltningens lokationer med henblik på sikring af kommunens informationsaktiver.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Udarbejdelse af regler for fysisk sikring af informationsaktiver	Forvaltningen	Forvaltningens direktion	Koncern IT	Enheder i den pågældende forvaltning

5.2. Sikre og kontrollerede områder

Sikre og kontrollerede områder skal være afskærmede fra offentligheden, og der skal være etableret en passende fysisk adgangskontrol.

Der skal være etableret passende adgangskontrol til store serverrum, således at kun autoriserede personer kan få adgang. Sikre områder skal være afgrænsede og beskyttede i henhold til en risikovurdering, der omfatter de informationsaktiver, der opbevares i området. For kontrollerede områder bør der være etableret passende fysisk adgangskontrol (f.eks. aflåsning).

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Sikring af sikrede og kontrollerede områder	Forvaltningen	Forvaltningens direktion	Koncern IT	-

I områder, der bl.a. anvendes til af- og pålæsning, og hvor uautoriserede personer har adgang, skal en passende sikkerhed etableres. Disse områder skal så vidt muligt adskilles fra områder med behandling af information/data.

Adgang til og fra af- og pålæsningsområder skal være sikret med passende sikringsforanstaltninger.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Sikring af af- og pålæsnings-områder	Forvaltningen	Forvaltningens direktion	Koncern IT	-

5.3. Åbne administrationsområder og modtagelsesområder

Områder, hvor der behandles fortrolige informationer mv., og som ligger i umiddelbar tilknytning til områder, hvor borgere frit kan færdes, skal sikres på passende vis.

Der bør i sådanne områder være et særligt fokus på,

- at pc'ere låses, når de forlades
- at computerskærme placeres eller dækkes, så de ikke er synlige for uvedkommende
- at fysiske dokumenter, som anvendes, ikke kan læses af uvedkommende
- at fysiske dokumenter i øvrigt kan opbevares i aflåste skabe eller skuffer
- at lokaler, hvori der opbevares fortrolige informationer mv. så vidt muligt låses, når de ikke er bemandede.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Sikring af åbne administrations-områder og modtagelses-områder	Forvaltningen	Forvaltningens direktion	Koncern IT	-

5.4. Åbne og delvist åbne områder

Områder med borgeradgange og ubemandede områder skal sikres på passende vis.

Sikringsforanstaltningerne skal vurderes og implementeres under hensyn til typerne af person- og værdidata, mængden af data og graden af kontakt med f.eks. borgere eller øvrige tredjeparter.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Sikring af åbne og delvist åbne områder	Forvaltningen	Forvaltningens direktion	Koncern IT	-

5.5. Tv- og videoovervågning

Tv- og videoovervågning må som udgangspunkt alene iværksættes i særlige tilfælde af kriminalitetsforebyggende og tryghedsskabende initiativer.

Ved tv- og videoovervågning af arbejdspladser, steder eller lokaler, hvor der er almindelig adgang, skal der oplyses om overvågningen ved skiltning eller anden tydelig information. Alle ansatte på stedet skal oplyses om formålet med tv- og videoovervågningen og om i hvilke tilfælde,

optagelserne vil blive gennemgået og videregivet til politiet. Billedoptagelser fra tv- og videoovervågning i kriminalitetsforebyggende og tryghedsskabende øjemed skal slettes senest 30 dage efter, at de er optaget, med mindre de indgår i en verserende politisag.

Der skal træffes de nødvendige fysiske og tekniske foranstaltninger mod, at billedoptagelser fra et overvågningskamera kommer til uvedkommendes kendskab eller misbruges. Kun et begrænset antal medarbejdere må have adgang til optagelserne. Billedoptagelser fra tv- og videoovervågning i kriminalitetsforebyggende øjemed må kun videregives, hvis personen på optagelsen har givet sit udtrykkelige samtykke hertil, eller hvis videregivelse sker til politiet i kriminalitetsopklarende øjemed.

Tv- og videoovervågning kan i medfør af tv-overvågningsloven iværksættes, såfremt overvågningen sker i forbindelse med særligt kriminalitetsforebyggende og tryghedsskabende initiativer.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Overholdelse af regler om tv-overvågning	Forvaltningen	Forvaltningens direktion	Forvaltningens DPO Business Partner	-

5.6. Beskyttelse af udstyr

It-udstyr skal være placeret på en sådan måde, at skader og uautoriseret adgang minimeres.

It-udstyr, der benyttes til behandling af persondata eller værdioplysninger, skal placeres på en sådan måde, at det er beskyttet mod adgang fra uvedkommende. Printere, der benyttes til udskrivning af personoplysninger eller værdioplysninger, skal placeres i kontrollerede områder, hvortil der ikke er offentlig adgang, eller det skal sikres, at det kun er muligt at udskrive dokumenter ved medarbejderens tilstedeværelse.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Placering af udstyr	Forvaltningen	Forvaltningens direktion	Koncern IT	-

5.7. Forsyningssikkerhed

Der skal være etableret foranstaltninger, anlæg m.m., således at relevant udstyr og infrastruktur er beskyttet mod strømsvigt og andre forstyrrelser.

I serverrum og på lignende lokationer, der rummer installationer som af den ansvarlige forvaltning er vurderet til at være af væsentlig betydning for kommunens drift, skal der være etableret nødstrømsanlæg til korttidsbrug og kontrollerede nedlukninger. På disse lokationer skal der ligeledes være etableret en plan for brugen af nødstrømsanlæg, der periodisk skal afprøves og kontrolleres.

Derudover skal der være etableret alternative (redundante) kommunikations-forbindelser til it-systemer med væsentlig betydning for Københavns Kommune.

Væsentlige it-systemer og infrastruktur skal være beskyttet mod fysiske og vejrrelaterede forhold som eksempelvis oversvømmelser, lyn og overspændinger.

Væsentligt it-udstyr skal ligeledes beskyttes mod tyveri.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Etablering af beskyttelse mod strømsvigt	Forvaltningen	Forvaltningens direktion	Koncern IT	-

5.8. Transmission af data

Transmission af fortrolige og forretningskritiske data i kabler og udstyr skal beskyttes mod uautoriserede indgreb.

I det omfang kommunens fortrolige og forretningskritiske data (fortrolige/følsomme personoplysninger, værdidata og andre fortrolige oplysninger), som transmitteres i kabler og udstyr til datakommunikation skal i relevant omfang beskyttes mod aflytning, uautoriserede indgreb og interferens.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Beskyttelse af transmission af data	Forvaltningen	Forvaltningens direktion	Koncern IT	-

5.9. Bortskaffelse af it-udstyr

Bortskaffelse af it-udstyr, som indeholder personoplysninger eller værdioplysninger, skal i videst muligt omfang ske ved destruktion eller der skal ske effektiv sletning.

Bortskaffelse af usb-nøgler, cd'er, dvd'er, hukommelseskort og lignende kan kun ske ved destruktion efter de til enhver tid gældende forretningsgange herom.

Ved salg, genbrug eller bortskaffelse af andet it-udstyr, herunder pc'er og eksterne harddiske, skal data lagret på udstyret slettes på en sådan måde, at data ikke kan gendannes, jf. de til enhver tid gældende forretningsgange herom.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Destruktion af udstyr eller effektiv sletning	Forvaltningen	Forvaltningens direktion	Koncern IT	-

6. SIKKERHEDSOMRÅDE 6 - DRIFTSIKKERHED

6.1. Driftsafviklingsprocedurer

Driftsprocedurer for infrastruktur og it-systemer skal dokumenteres og ajourføres løbende. Driftsprocedurer skal være tilgængelige for de brugere, der har behov for dem.

Driftsprocedurer skal indeholde en beskrivelse af de driftsmæssige bindinger, herunder integrationer og transport af data fra og til andre systemer og infrastrukturkomponenter. De skal ligeledes indeholde procedure for fejlhåndtering og reetableringsproces. Driftsprocedurer skal derudover indeholde beskrivelse af kontrolspor og systemteknisk logning.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Udarbejdelse af driftsprocedurer	Teknisk systemejer	Direktionen for den forvaltning, som er ansvarlig for systemet	Koncern IT	-

6.2. Kapacitetsstyring

Der skal være løbende overvågning af infrastruktur og understøttende systemer med henblik på at styre ressourceforbruget.

Der skal være defineret tærskelværdier ved fejl på f.eks. CPU, disk, eller ved andre lignende performanceproblemer. Hvis tærskelværdierne overskrides, skal der ske alarmering til den ansvarlige og udførende enhed.

Der skal løbende tages stilling til behovet for kapacitetsændringer såsom indkøb af nyt hardware, sletning af data, afvikling af applikationer, systemer, miljøer m.m.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Overvågning af infrastruktur	Koncern IT/PIT	ØKF/BUF	-	-

6.3. Skadevoldende programmer og ondsindet kode

Ud fra en risikobaseret tilgang skal kommunens informationsaktiver i videst muligt omfang være beskyttet mod skadevoldende programmer og ondsindet kode.

Det skal være muligt at blokere skadevoldende programmer og ondsindet kode, så dette ikke aktiveres på kommunens informationsaktiver, jf. punkt 3.1. Det gælder således for alle arbejdsstationer, bærbare pc'er og andet mobilt it-udstyr, servere og andre enheder, der stiller services til rådighed samt datatransportbærende enheder.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Beskyttelse mod ondsindet kode mv.	Den forvaltning som er ansvarlig for det pågældende informationsaktiv	Forvaltningens direktion	Forvaltningens digitaliseringsenhed og Koncern IT	-

6.4. Backup

Der skal tages backup af alle væsentlige informationsaktiver i henhold til kommunens behov for at kunne opretholde en sikker drift.

Der skal til enhver tid kunne gennemføres gendannelse af systemer og data, der har væsentlig betydning for kommunens myndighedsudøvelse og drift. Backup skal tilbydes af Koncern IT som en standardiseret ydelse over for kommunens systemejere. Krav til backup-konfigurationer for alle systemer og data skal være dokumenteret i backup-planer, der beskriver hyppighed, og hvor backups kan tilgås. Backup skal testes periodisk, dog minimum halvårligt, med henblik på at validere, dels indholdet af backup'en, dels at systemer og data kan genskabes inden for de aftalte tidsrammer.

Backup-planer skal tage udgangspunkt i kommunens krav til tilgængelighed og acceptabel periode for tab af adgang til data. I forbindelse med større idriftsættelser eller andre betydende ændringer, skal der gennemføres backup af systemopsætninger. Automatiserede backup-jobs, som f.eks. kørsler og batch-jobs, skal løbende overvåges for identifikation af fejlede kørsler.

It-systemer (kilden) og opbevaring af backups (kopien) skal være fysisk adskilte, og placeringen/opbevaringen af backups skal være beskyttet med passende sikringsforanstaltninger.

Der skal kunne gennemføres en restore-test hos enten Koncern IT eller hos ekstern leverandør, hvis systemet driftes eksternt.

Ændringer til backup-konfigurationer eller backup-løsninger efter ibrugtagning skal være dokumenteret og skal godkendes af den ansvarlige enhed.

I det omfang en backup indeholder personoplysninger skal det ved en eventuel indlæsning af backup'en (restore) sikres, at personoplysninger – som er slettet siden seneste backup – på ny slettes.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Backup af væsentligt informationsaktiver	Den forvaltning som er ansvarlig for det pågældende informationsaktiv	Forvaltningens direktion	Forvaltningens digitaliseringsenhed og Koncern IT	-

6.5. Logning og overvågning

6.5.1 Logning generelt

Logning foretages i forhold til såvel brugere som systemer. Logning af brugeraktiviteter skal være baseret på en risikovurdering, således at der kun logges for relevante og nødvendige hændelser.

Hvis et system ikke behandler personoplysninger eller værdidata, kan kravet om logning fraviges. Af hensyn til Københavns Kommunes drifts- og sikkerhedsmæssige forhold er udgangspunktet, at al brug af kommunens it-systemer løbende skal registreres (logges).

Logning skal foretages på en måde, så det efterfølgende er muligt at (gen)etablere brugerens handlinger, samt tolke og forstå loggens indhold. Logdata skal i videst muligt omfang sikres, så integriteten af loggen til enhver tid er bevaret.

Logfaciliteter og loginformation skal være beskyttet, således at risikoen for uautoriseret adgang eller manipulation af indholdet reduceres.

Logfaciliteterne skal være sikret både fysisk og virtuelt mod beskadigelse, fortabelse og manipulation mm.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Overordnet ansvar for at der er etableret logning	Den forvaltning som er ansvarlig for det pågældende informationsaktiv	Forvaltningens direktion	Forvaltningens digitaliseringsenhed og Koncern IT	-

6.5.2 Brugerlogning

It-systemer, der behandler person- og værdioplysninger, skal til enhver tid kunne fremvise logs for brugeradfærd.

Logdata skal som minimum indeholde logs på følgende områder:

- anvendelsen af data
- tidspunkt for systemanvendelse
- identifikation af brugeren (brugerid) på den udførende medarbejder
- den eller de borgere, som opslaget eller opslagene drejer sig om (den eller de registrerede)
- de konkrete data eller søgninger, der er behandlet i den sammenhæng, loggen beskriver
- logning af brugen af udvidede rettigheder.

Logning af data indeholdende personoplysninger skal opbevares i 6 måneder, hvorefter logdata skal slettes. Undtagelser, hvor logdata skal opbevares i op til 5 år, skal være dokumenteret med en begrundet angivelse af behovet for den længere opbevaring.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Etablering af log om brugeradfærd	Den enhed som har ansvar for it-systemet	Forvaltningens direktion	Forvaltningens digitaliseringsenhed og Koncern IT	-

I systemer med værdidata samt fortrolige og følsomme personoplysninger skal aktiviteter, som udføres af systemadministratorer og andre med særlige rettigheder, logges.

Hvis et system indeholder værdidata, fortrolige eller følsomme personoplysninger, skal aktiviteter udført af systemadministratorer og andre med særlige rettigheder logges. Hvor det er teknisk muligt, skal der være etableret funktionsadskillelse, således at systemadministratorer ikke selv kan ændre loginformationer. Se i øvrigt afsnit 4.1.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Etablering af log om systemadministrators adfærd	Den enhed som har ansvar for it-systemet	Forvaltningens direktion	Forvaltningens digitaliseringsenhed og Koncern IT	-

6.5.3 Logning og overvågning af brugerlog

Der skal løbende følges op på logdata i systemer med henblik på at identificere uhensigtsmæssigheder og misbrug af rettigheder i forhold til navnlig person- eller værdioplysninger.

Af sikkerhedshensyn overvåger kommunen egne it-systemer og brugernes adfærd i disse. Den ansvarlige enhed for et system er ansvarlig for, at der skal gennemføres periodiske udtræk fra systemer for f.eks. at kontrollere adgange til data og systemet.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Opfølgning på brugerlog	Den enhed som har ansvar for it-systemet	Forvaltningens direktion	Forvaltningens digitaliseringsenhed og Koncern IT	-

Det skal altid vurderes, om systemer med person- eller værdioplysninger skal indgå i kommunens til enhver tid anvendte SIEM-løsning. Hvis ikke systemet indgår i denne løsning, skal fravalget dokumenteres og godkendes forvaltningens ledelse.

Dette skal ske både gennem sikre arbejdsgange og ved brug af kommunens SIEM-løsning, hvor det er teknisk muligt. Alternativt til brug af SIEM kan man udføre stikprøvekontroller af loggen.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Kobling til SIEM	Den enhed som har ansvar for it-systemet	Forvaltningens direktion	Forvaltningens digitaliseringsenhed og Koncern IT	-

Eventuel gennemgang af en specifikt udpeget medarbejders adfærd i kommunens it-systemer må kun ske, hvis det er nødvendigt for, at Københavns Kommune kan forfølge berettigede interesser, og hensynet til den ansatte ikke overstiger disse interesser.

Adgang til medarbejderes brugeradfærd og anvendelse af kommunens it-systemer gives, hvis kommunen forfølger berettigede interesser, f.eks. hensynet til drift, sikkerhed (herunder sikkerhedsbrud), genetablering og dokumentation samt hensynet til kontrol af anvendelse af data.

Ved begrundet mistanke om misbrug mm. kan der bestilles en udtræk af logfiler. Udtræk og andre logfiler må kun benyttes til kontrol af medarbejderes adfærd, internetbrug eller øvrige brug af systemer, hvis kommunens personalejuridiske funktion konkrete har tilkendegivet, at der er et lovligt grundlag for at anvende den pågældende log i kontroløjemed. Udtrækkene skal altid opbevares på sikker vis, således at uvedkommende ikke kan få adgang til oplysningerne. Udtrækkene skal destrueres, når det forhold, der begrundede udtrækket er endeligt afklaret, og hvis der i øvrigt ikke længere er behov for at opbevare udtrækket.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Berettiget kontrol på medarbejderniveau	Den enhed som har ansvar for it-systemet	Forvaltningens direktion	Forvaltningens digitaliseringsenhed, personalejuridisk funktion og Koncern IT	-

6.5.4 Systemlogning

I systemer indeholdende person- eller værdioplysninger skal ændringer i systemet logges.

Der skal på systemniveau som minimum logges for:

- kritiske systemændringer
- ændringer i rollebeskrivelser
- ændringer i rettighedsstyring.
- Fejllogs

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Etablering af systemlog	Den enhed som har ansvar for it-systemet	Forvaltningens direktion	Forvaltningens digitaliseringsenhed og Koncern IT	-

Der skal løbende følges op på logdata i systemloggen med henblik på at identificere uhensigtsmæssigheder i forhold til en effektiv drift af systemet.

Der følges op på områder som f.eks. overskridelser af tærskelværdier, forsøg på uretmæssig adgang til person- og værdioplysninger, uventede ændringer eller sletninger i data og til/frakobling af udstyr til systemer eller netværk.

Alarmer fra fysiske og logiske adgangskontrolsystemer, omfattende benyttede adgange, forsøg på adgang og aktivering/deaktivering af kontroller i disse systemer, skal håndteres.

Fejllogs skal regelmæssigt analyseres og gennemgås for at sikre, at alle fejl bliver rettet på tilfredsstillende vis. Korrigerende og kompenserende foranstaltninger, der kan påvirke beskyttelsen af data på systemerne, skal dokumenteres.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Opfølgning på systemlog	Den enhed som har ansvar for it-systemet	Forvaltningens direktion	Forvaltningens digitaliseringsenhed og Koncern IT	-

7. SIKKERHEDSOMRÅDE 7 - KOMMUNIKATIONSSIKKERHED (NETVÆRKSSIKKERHED)

7.1. Styring af netværkssikkerhed

Der skal være nedskrevne procedurer for såvel intern som ekstern adgang til kritisk netværksudstyr.

Der skal forefindes beskrevne procedurer for logisk adgang til kritisk netværksudstyr som f.eks. switches, routere og firewalls. Se også punkt 4.3.7 om privilegerede administrative adgange til it-infrastrukturen.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Udarbejdelse af procedurer for adgang til netværksudstyr	Den enhed som er ansvarlig for netværksudstyret	Forvaltningens direktion	Koncern IT	-

Netværksinfrastrukturen skal designes med henblik på at minimere sikkerhedsrisici, og ekstern adgang skal altid foregå via en sikker forbindelse.

Der skal være etableret sikringsforanstaltninger til opdagelse af og beskyttelse mod misbrug, fejlforsendelser og manipulation af data. Kritisk netværksudstyr skal således løbende overvåges for driftsmæssige problemer eller for sikkerhedshændelser såsom DDOS, port scanninger eller uautoriserede adgangsforsøg.

Administration af systemer eller infrastrukturelementer, der ikke foretages fra Københavns Kommunes netværk, skal ske med en sikker og krypteret forbindelse med automatisk timeout-funktion efter inaktiv periode.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Design af sikker netværksinfrastruktur	Koncern IT/PIT	ØKF/BUF	-	-

7.2. Kryptografi

Der skal være etableret løsninger til, at transmission af værdidata samt fortrolige og følsomme oplysninger over det åbne internet kan ske krypteret.

Kryptering skal ske i overensstemmelse med anerkendte standarder for krypteringsløsninger. Heraf følger bl.a., at nøgler og certifikater skal håndteres og beskyttes på passende vis.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Etablering af løsninger til kryptering af transmission	Den enhed som har ansvar for it-systemet	Forvaltningens direktion	Koncern IT	-

Kommunens interne netværkstrafik skal krypteres med mindre der er truffet andre foranstaltninger, der sikrer det fysiske netværk, lokationer og installationer.

Om sikring af det fysiske netværk, lokationer og installationer se afsnit 5.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Sikring af intern netværkstrafik	Koncern IT	ØKF	-	-

7.3. Elektronisk handel og betaling

Informationer, der benyttes i forbindelse med elektronisk handel og betaling beskyttes for at forhindre ufuldstændig transmission, fejlforsendelser, uautoriseret ændring af meddelelser, uautoriseret offentliggørelse og uautoriseret kopiering eller retransmission af oplysninger.

Der skal altid anvendes sikre løsninger til elektronisk handel og betaling. Elektronisk handel og betaling skal i øvrigt altid foregå efter reglerne i kommunens kasse- og regnskabsregulativ.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Beskyttelse af informationer i forbindelse med elektronisk handel mv.	Den enhed som er ansvarlig for it-systemet	Forvaltningens direktion	Koncern IT	-

7.4. Ind- og uddata

Ind- og uddata skal til enhver tid opbevares således, at de ikke kommer til uvedkommendes kendskab.

Inddata omfatter navnlig personoplysninger og værdidata, som opbevares i papirformat eller på elektroniske medier med henblik på indlæsning i kommunens systemer. Uddata omfatter navnlig personoplysninger og værdidata, som udskrives i på papir eller kopieres over på bærbare lagringsmedier.

Adgangen til personoplysninger og værdidata skal begrænses til medarbejdere, der har et arbejdsbetinget behov herfor. Dette gælder også ved afsendelse og modtagelse. Data skal til enhver tid opbevares, så de ikke kommer til uvedkommendes kendskab.

I områder, der anvendes til betjening af borgere, og hvor der er offentlig adgang, skal medier/dokumenter, der indeholder fortrolige eller følsomme personoplysninger eller værdidata, opbevares aflåst i skabe, skuffer eller lignende, når de ikke benyttes.

Fysiske dokumenter skal destrueres på betryggende vis, når der ikke længere er et sagligt behov for opbevaring af disse. Ved fysisk transport af ind- og uddata skal der, afhængigt af oplysningernes karakter, anvendes en betryggende transportform.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Håndtering af ind- og uddata	Medarbejdere	Nærmeste leder	Forvaltningens DPO Business Partner og evt. Koncern IT	-

8. SIKKERHEDSOMRÅDE 8 - ANSKAFFELSE, UDVIKLING OG VEDLIGEHOLDELSE

8.1. Sikkerhed i forhold til indkøb og nyudvikling af systemer

Systemer og programmer, der anskaffes eller udvikles fra ny, skal overholde kommunens krav til sikkerhed og databeskyttelse.

Ved anskaffelse, udvikling og ændring af kommunens løsninger skal sikkerhed og databeskyttelse tænkes ind i processen.

I tilknytning til de i dette forretningscirkulære fastsatte regler om sikkerhed, skal den anskaffende enhed ved anskaffelse, udvikling og ændring af systemer iagttage kommunens kravbank, kommunens regler for persondatabeskyttelse (f.eks. om konsekvensanalyser og om understøttelse af de registreredes rettigheder) samt kommunens processer for it-anskaffelser. Der henvises i den forbindelse til forretningscirkulærerne for henholdsvis persondatabeskyttelse og it-anskaffelser.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Sikring af nye systemer og programmer	Den enhed som har ansvar for it-systemet	Forvaltningens direktion	Koncern IT	-

8.2. Ændringer af systemer mv.

Væsentlige ændringer af betydning for informationssikkerhed i systemer, netværk og øvrig infrastruktur, der implementeres i og/eller har en tilknytning til kommunens netværk og infrastruktur, skal godkendes af kommunens forum for it-ændringsønsker (Change Advisory Board – CAB) inden implementering.

Ændringer i kommunens systemer mv. skal være godkendt på møder i CAB inden implementering. Godkendelsen skal være dokumenteret, og alle påvirkede systemer, databaser og udstyr skal identificeres i forbindelse med gennemførelsen af ændringer. Ved større ændringer til it-systemer skal sikkerhedsforanstaltninger internt i systemet testes for at sikre, at disse ikke forringes ved implementeringen.

Test skal gennemføres for at afdække og håndtere uhensigtsmæssige følgevirkninger på Københavns Kommunes daglige drift og sikkerhed inden ændringerne implementeres i drift.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Forelæggelse af ændringer for CAB	Teknisk systemejer	Direktionen for den forvaltning, som er ansvarlig for systemet	Koncern IT	-

8.3. Styring af programkildekode i større driftsmiljøer

Med mindre der er tale om Open Source-kildekoder, skal kildekoder til egenudviklede it-systemer og til it-systemer, der er særligt for kommunen, opbevares hos kommunen eller i et deponeringsinstitut.

Med mindre der er tale open source-koder, må kildekoder må ikke opbevares i driftsmiljøet og fysisk/logisk adgang skal begrænses, kontrolleres og logges.

Med Open Source-kildekoder menes koder, som er stillet til rådighed af licensgi-veren for kommunen og for andre kunder eller offentligheden, hvad enten licensgiveren er leverandør eller en tredjepart.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Opbevaring af kildekoder	Forvaltningens digitaliseringsenhed	Forvaltningens direktion	Koncern IT	-

8.4. Adskillelse af udviklings- og testmiljøer fra produktionsmiljøer

Udviklings og testmiljøer skal have en passende adskillelse fra produktionsmiljøer for at nedsætte risikoen for uautoriseret adgang til og ændring af driftsmiljøet samt ikke godkendt anvendelse af data.

Udviklings- og testmiljøer skal være fuldstændigt adskilt fra produktionsmiljøer med mindre det kan begrundes, dokumenteres og godkendes af den ansvarlige enheds ledelse, at der ikke er risiko for, at værdidata eller personoplysninger mistes, ændres eller kommer til uvedkommendes kundskab, og at der ikke er risiko, at systemet eller andre systemer lider skade.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Adskillelse af udviklings- og testmiljøer fra produktionsmiljøer	Den enhed som har ansvar for it-systemet	Forvaltningens direktion	Koncern IT	-

8.5. Udførelse af test

Der må som udgangspunkt ikke testes i produktionsmiljøer.

Der må ikke testes i produktionsmiljøer med mindre det på forhånd begrundes, dokumenteres og godkendes af den ansvarlige enheds ledelse, at der ikke er risiko for, at værdidata eller personoplysninger mistes, ændres eller kommer til uvedkommendes kundskab, og at det dokumenteres, at der ikke er risiko, at systemet eller andre systemer lider skade.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Udførelse af test	Den enhed som har ansvar for it-systemet	Forvaltningens direktion	Koncern IT	-

8.6. Anvendelse af testdata

Der må ikke testes værdidata og personoplysninger som testdata.

Værdidata og personoplysninger må ikke anvendes til test, med mindre der foretages anonymisering af oplysningerne. Ved en eventuel anonymisering af oplysninger skal det sikres, at det ikke på nogen måde er muligt at identificere de personer, som oplysningerne oprindeligt vedrørte.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Anvendelse af testdata	Den enhed som har ansvar for it-systemet	Forvaltningens direktion	Koncern IT	-

9. SIKKERHEDSOMRÅDE 9 - LEVERANDØRFORHOLD

Hvis der med eksterne leverandører og samarbejdspartnere indgås aftaler af betydning for kommunens it-drift eller informationssikkerhed, skal aftaleforholdet dokumenteres.

Hvis der med eksterne leverandører og samarbejdspartnere indgås aftaler om f.eks. levering af it-udstyr, it-drift, hosting, databehandling, rådgivning eller andre ydelser, der har betydning for kommunens it-drift eller informationssikkerhed, skal aftaleforholdet dokumenteres i relevant omfang gennem bl.a. driftsaftaler, SLA'er (Service Level Agreement), databehandleraftaler, tavshedspligtserklæringer samt kontrakter, der beskriver den leverede ydelse.

Det skal i den forbindelse sikres, at eksterne leverandører og samarbejdspartnere efterlever Københavns Kommunes krav til sikkerhed, persondatabeskyttelse, stabilitet og tilgængelighed.

Der henvises i øvrigt til Forretningscirkulære for persondatabeskyttelse – dokumentation og compliance i forhold til bl.a. databehandleraftaler.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Dokumentation af leverandørforhold	Den enhed som har ansvar for leverandørforholdet	Forvaltningens direktion	Forvaltningens digitaliseringsenhed, forvaltningens DPO Business Partner, Koncern IT	-

10. SIKKERHEDSOMRÅDE 10 - STYRING AF INFORMATIONSSIKKERHEDS-HÆNDELSER SAMT INFORMATIONSSIKKERHEDSASPEKTER MV.

10.1. Ansvar og procedurer

Kommunens procedurer for indberetning af hhv. persondatabrud og sikkerhedshændelser skal følges.

Koncern IT skal orienteres om såvel potentielle som reelle persondata- og sikkerhedsbrud i henhold til kommunens forretningsgang herfor.

Medarbejdere, der har mistanke om eller konstaterer sikkerhedsbrud, skal følge kommunens forretningsgang og herunder indmelde bruddet gennem den relevante it-løsning. Der skal straks herefter igangsættes foranstaltninger til korrigering af fejl eller svagheder.

Se i øvrigt Forretningsgang for håndtering af persondatabrud.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Indberetning af persondatabrud	Medarbejdere	Forvaltningens direktion	Forvaltningens DPO Business Partner	Koncern IT
Indberetning af sikkerhedshændel-ser	Medarbejdere	Forvaltningens direktion	Forvaltningens digitaliseringsenhed og Koncern IT	Koncern IT

10.2. Rapportering af informationssikkerhedshændelser

Der gennemføres løbende og med passende tidsintervaller afrapportering til relevante ledelseslag og Økonomiudvalget.

Afrapporteringen indeholder opsamling og bearbejdning af it-sikkerheds- og persondatahændelser for hele kommunen. Der redegøres i denne forbindelse ligeledes for hvilke forbedrende tiltag, der er iværksat.

Der henvises i øvrigt til Forretningscirkulære for organisering af informationssikkerhed.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Afrapportering til Økonomiudvalget	Koncern IT	ØKF	-	-
Afrapportering til forvaltningsledelsen	Forvaltningens digitaliseringsenhed	Forvaltningens direktion	-	-

10.3. Beredskabsstyring

Der skal forefindes en overordnet it-beredskabsplan med tilhørende delplaner/-politikker i forvaltningerne.

Københavns Kommunes it-beredskab er del af det overordnede kriseberedskab, som Hovedstadens Beredskab er ansvarlig for. It-beredskabsplanerne skal indeholde procedurer for iværksættelse af nødplaner, eskalering, reetablering af it-systemer og begrænsning af skadevirkninger i tilfælde af større it-nedbrud.

I tilfælde af større it-nedbrud skal it-beredskabsplanen aktiveres efter den fastlagte eskaleringsprocedure.

Kommunens it-beredskabsplan skal afspejle behovet for genopretning af kommunens drift inden for kerneområderne. Beredskabsplanen, herunder ændringer til de sammenhængende it-beredskabsplaner hos forvaltningsenhederne, skal testes og revurderes som det er beskrevet i de gældende forretningsgange.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Udarbejdelse af tværgående it-beredskabsplan	Koncern IT	ØKF	-	-
Udarbejdelse af forvaltningsspecifik it-beredskabsplan	Forvaltningens digitaliseringsenhed	Forvaltningens direktion	Koncern IT	-

10.4. Risikovurderinger af it-systemer og it-infrastruktur

Risikovurderinger skal foretages ved indførelse og ved væsentlige ændringer af it-systemer og it-infrastruktur.

Risikovurderinger skal være relevante og kvalificerede i forhold til det vurderede område. Heri ligger blandt andet:

- At vurderingerne i nødvendigt omfang skal tage afsæt i anerkendte, standardiserede og vedtagne principper for risikovurderinger, tilpasset det pågældende område og under hensyntagen til, at det i nødvendigt omfang skal være muligt at sammenholde og sammenligne risikoniveauet på tværs af forvaltninger
- At vurderingerne skal udføres af kvalificerede medarbejdere
- At omfanget af risikovurderinger skal være proportionalt med det vurderede områdes betydning
- At den foretagne risikovurdering dokumenteres
- At risikovurderinger foretages med den fornødne frekvens, og at det i relevant omfang er muligt at følge risikoudviklingen over tid.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Udarbejdelse af risikovurderinger af it-systemer	Koncern IT	ØKF	-	-
Opfølgning på risikovurderinger	Forvaltningens digitaliseringsenhed	Forvaltningens direktion	Koncern IT	

10.5. It-revisioner

It-revisioner skal altid planlægges med henblik på at minimere drifts- og sikkerhedsmæssige risici.

Kommunen skal give adgang til relevante systemer og data via lederen på det område, der skal revideres, og al brug af revisionsværktøjer og adgange skal registreres ved logning.

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Bistand til it-revisioner	Den enhed som har ansvar for det reviderede område	Forvaltningens direktion	Koncern IT	-

ÆNDRING OG AJOURFØRING

Økonomiforvaltningen har overfor Økonomiudvalget ansvar for vedligeholdelse og ajourføring af dette forretningscirkulære gennem inddragelse af kommunens relevante tværgående fora, hvori alle forvaltninger er repræsenteret.

Indholdsmæssige ændringer

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

Underliggende fællesadministrative forretningsgange udarbejdes og besluttes af Økonomiforvaltningen efter forelæggelse for It-kredsen.

Underliggende forvaltningsspecifikke forretningsgange udarbejdes af den enkelte forvaltning og forelægges den enkelte forvaltnings direktion til godkendelse.

Redaktionelle ændringer

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

Forretningscirkulære for informationssikkerhed