Forretningscirkulære for informationssikkerhed
Opdateret og godkendt, december 2020

FORRETNINGS-CIRKULÆRE FOR INFORMATIONS-SIKKERHED

INDLEDNING

Forretningscirkulære for informationssikkerhed fastsætter de nærmere regler for informationssikkerheden i Københavns Kommune.

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

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.

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

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

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

Figur 1: Regelhierarki for Københavns Kommune.

INDHOLD

INFORMATIONSSIKKERHED

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

Tabel 1: Sikkerhedsområder fra ISO27001

#	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 it-systemer ISO 27001 område 14
9	Leverandørforhold ISO 27001 område 15
10	Styring af informationssikkerhedsnedbrud samt informationssikkerhedsaspekter 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 været suppleret af bindende forretningsgange, sikkerhedsstandarder 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 i forhold til informationssikkerhed. Denne beskrives ud fra følgende aktører: "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 aktiviteten.

Ansvarlig

Den aktør, som over for den pågældende borgmester og Økonomiudvalget har det endelige ansvar for, at aktiviteten udføres.

Rådgivende

De(n) aktør(er), som de(n) udførende skal rådføre sig med i forhold til 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, om aktiviteten udføres i samarbejde med de(n) rådgivende.

Informeret

De(n) aktør(er), som de(n) udførende skal informere om fremdrift i udførelsen af aktiviteten og/eller resultatet af aktiviteten.

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.

Tabel 2: Ansvars- og rollefordeling ift. "Organisering af informationssikkerhed"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forretningscirkulære for organisering af informationssikkerhed*

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' henvises der navnlig til infrastrukturelementer, it-systemer, computere, mobile enheder, printere, scannere og data, jf. afsnit 3.1. Når data er omfattet af informationsbegrebet, har det desuden den betydning, at særligt værdioplysninger og personoplysninger om borgere og ansatte skal sikres. Dermed skal hensynet til borgerne og de ansatte også inddrages i kommunens fastlæggelse af et passende informationssikkerhedsniveau.

Med 'passende' sigtes der endvidere til, at hver forvaltning ud fra 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.

Tabel 3: Ansvars- og rollefordeling ift. "Generelt for informationssikkerhed i kommunen"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Fastsættelse af et passende teknisk og organisatorisk informationsniveau	Forvaltningen	Forvaltnings-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, regler for persondatabeskyttelse og regler om tavshedspligt, jf. de til enhver tid gældende bestemmelser i forvaltningsloven og straffeloven. Nye medarbejderes identitet skal i øvrigt kunne fastslås.

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. Desuden skal nye medarbejderes identitet kunne fastslås, før en ansættelse må finde sted.

For øvrige krav til ansættelse henvises til forretningscirkulære – løn og personale.

Tabel 4: Ansvars- og rollefordeling ift. "Ved ansættelsen"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Instruktion af nye medarbejdere om informations-sikkerhedsregler	Nærmeste leder	Forvaltnings-direktion	Forvaltningens digitaliserings-enhed og evt. Koncern IT	Forvaltningens digitaliserings-enhed
Informere om tavshedspligt	Nærmeste leder	Forvaltnings-direktion	Forvaltningens forvaltningsretlige funktion	-
Fastslå ny medarbejders identitet	Nærmeste leder	Forvaltnings-direktion	-	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forretningscirkulære – løn og personale*
- *Ledelsesrettet informationsmateriale om informationssikkerhed og databeskyttelse*

2.2. Under ansættelsen

Alle medarbejdere i Københavns Kommune med adgang til kommunens it-systemer, enheder og data skal til enhver tid 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 og skal løbende gennemgå relevant uddannelse på området.

Tabel 5: Ansvars- og rollefordeling ift. "Under ansættelsen"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Ledelsesrettet informationsmateriale om informationssikkerhed og databeskyttelse*

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 enhver tid gældende bestemmelser i forvaltningsloven og straffeloven.

Tabel 6: Ansvars- og rollefordeling ift. "Ved ansættelsesforholdets ophør"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Ledelsesrettet informationsmateriale om informationssikkerhed og databeskyttelse*

3. SIKKERHEDSOMRÅDE 3 - STYRING AF AKTIVER

3.1. Fortegnelse over informationsaktiver

Kommunen skal føre en ajourført fortegnelse over alle væsentlige informationsaktiver.

Alle forvaltninger skal have et overblik over forvaltningens informationsaktiver med henblik på at kunne opretholde et passende informationssikkerhedsniveau.

Økonomiforvaltningen skal desuden, 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
- Hjælpeværktøjer, jf. definitionen i forretningscirkulære for it-anskaffelser.
- Computere, herunder bærbare pc'er.
- Mobile enheder, f.eks. telefoner, smartphones og tablets.
- Andre væsentlige it-aktiver, f.eks. printere og scannere.
- Data, navnlig personoplysninger.

Kommunens informationsaktiver inkluderer desuden aktiver, som opbevares og driftes i interne, eksterne samt cloud-miljøer.

Forvaltningerne skal tage stilling til, hvilke af forvaltningens informationsaktiver, som må anses som særligt kritiske for opretholdelsen af et passende informationssikkerhedsniveau. Informationssikkerhedsniveauet har betydning for tilgængeligheden af de enkelte forvaltningers informationsaktiver. Den fysiske placering af disse informationsaktiver skal registreres og behandles som beskrevet i afsnit 5.1. Forvaltningen skal desuden forholde sig til, hvilke oplysninger som er særligt kritiske for forretningen. Disse oplysninger klassificeres som værdioplysninger, jf. afsnit 3.5.

For så vidt angår registrering af personoplysninger, behandlingsprocesser og datastrømme henvises til forretningscirkulære for persondatabeskyttelse - dokumentation og compliance.

Tabel 7: Ansvars- og rollefordeling ift. "Fortegnelse over informationsaktiver"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Fortegnelse over forvaltningens væsentlige informationsaktiver	Forvaltning	Forvaltnings-direktion	Koncern IT	-
Fortegnelse over kommunens væsentlige informationsaktiver	Koncern IT	ØKF-direktion	-	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forretningscirkulære for organisering af informationssikkerhed*
- *Forretningscirkulære for it-anskaffelser*
- *Forretningscirkulære for persondatabeskyttelse – dokumentation og compliance*

3.2. Ansvar for informationsaktiver

Ansvar for kommunens informationsaktiver skal være klart defineret.

Det skal fremgå af kommunens fortegnelser, hvilken forvaltning, der har ansvaret for de pågældende informationsaktiver, som Københavns Kommune ejer.

Kommunen ejer al ikke-privat data, som lagres i kommunens informationsaktiver, herunder på medarbejdernes it-udstyr, og forbeholder sig ret til at anvende denne data inden for lovens rammer.

Tabel 8: Ansvars- og rollefordeling ift. "Ansvar for informationsaktiver"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Klar definition af ejerskab af og ansvar for informations-aktiver	Forvaltningens digitaliserings-enhed	Forvaltnings-direktion	Koncern IT	-

3.3. Medarbejdernes brug af informationsaktiver

3.3.1. Arbejdsbetinget brug af informationsaktiver

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

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

Tabel 9: Ansvars- og rollefordeling ift. "Arbejdsbetinget brug af informationsaktiver"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Sikring af at informationsaktiver anvendes til arbejdsbetinget formål	Forvaltningens digitaliserings-enhed og de enkelte ansatte	Forvaltnings-direktion	Koncern IT	-
Fastsættelse af regler for arbejdsbetinget brug af informationsaktiver	Koncern IT	ØKF-direktion	-	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes retningslinjer og vejledninger på området*
- *Forvaltningsspecifikke forretningsgange og regler*

3.3.2. Privat brug af informationsaktiver

Medarbejdere kan 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 private brug af kommunens aktiver, skal der fastsættes nærmere regler for acceptabel anvendelse af internet, programmer og online-tjenester samt opbevaring af oplysninger på kommunens lagringsmedier.

Tabel 10: Ansvars- og rollefordeling ift. "Privat brug af informationsaktiver"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Sikring af at privat anvendelse af informationsaktiver sker efter anerkendte og lovlige formål	Forvaltningers digitaliserings-enhed og de enkelte ansatte	Forvaltnings-direktion	Koncern IT	-
Udarbejdelse af regler for privat brug af informationsaktiver	Koncern IT	ØKF-direktion	-	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes retningslinjer og vejledninger på området*

3.4. Tilbagelevering og ombytning af aktiver

Udleveret udstyr afleveres, og autorisationer deaktiveres, senest når ansættelses- 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 for eventuelle videre undersøgelser.

Tabel 11: Ansvars- og rollefordeling ift. "Tilbagelevering og ombytning af aktiver"

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

3.5. Klassifikation af data

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

I Københavns Kommune klassificeres kommunens oplysninger som følger:

- Almindelige personoplysninger: Omfatter almindelige personhenførbare oplysninger, som hverken kan klassificeres som fortrolige eller følsomme.
- Følsomme personoplysninger: Omfatter personoplysninger af følsom personhenførbar karakter, og som kræver en snævrere ramme for behandling end almindelige personoplysninger.
- Fortrolige personoplysninger: Omfatter personoplysninger der må anses som fortrolige, hvis det vurderes, at oplysningen ikke bør komme til offentlighedens kendskab. Følsomme personoplysninger er altid fortrolige, men fortrolige personoplysninger er ikke altid følsomme. Herunder gælder eksempelvis CPR-numre, som er en almindelig personoplysning, som skal behandles fortroligt.
- Værdioplysninger: Omfatter fortrolige oplysninger, der er beskyttelsesværdige, fordi de har en kritisk økonomisk eller forretningsmæssig værdi for kommunen eller har betydning for kommunens/andres omdømme (f.eks. staten og private virksomheder).

- Andre oplysninger: interne, åbne og offentlige oplysninger. Omfatter oplysninger der ikke har kritisk forretningsmæssig værdi, som uden væsentlige konsekvenser kan deles med omverdenen eller ikke kan kategoriseres under nogen af ovenstående kategorier.

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 værdioplysninger potentielt ændre sig. Det kunne f.eks. være mødemateriale, der er fortroligt frem til afholdelsen af et specifikt møde, hvorefter det bliver offentligt tilgængeligt. Dermed ændrer oplysningerne sig fra at høre under kategorien 'værdioplysninger' til at høre under kategorien 'andre oplysninger'. Behovet for tilknyttede sikkerhedsforanstaltninger kan altså potentielt ændre sig i takt med, at beskyttelsesbehovet for oplysninger ændrer sig.

I Københavns Kommune er det besluttet at have samme sikkerhedsniveau for værdioplysninger som for almindelige, følsomme og fortrolige personoplysninger. Sikkerhedsniveauet skal fastlægges ud fra en risikobaseret tilgang.

Tabel 12: Københavns Kommunes dataklassifikationssystem (ikke udtømmende)

Københavns Kommunes dataklassifikationssystem	
Kategori	**Eksempler**
Almindelige personoplysninger	Navn, adresse, ansættelsesforhold, digitale fodspor, forbrugsoplysninger, ejerforhold (f.eks. bolig og bil), foto/video (som udgangspunkt), GPS-lokationer, IP-adresse, matrikelnummer, uddannelse, og CV.
Følsomme personoplysninger	Race og etnisk tilhørsforhold, politisk overbevisning, religiøs overbevisning, filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, genetiske data, biometriske data, helbredsoplysninger, seksuelle forhold og orientering
Fortrolige personoplysninger	CPR-numre, børneattester, straffeattester og oplysninger, som efter omstændighederne skal behandles som fortrolige, herunder indkomst- og formueforhold, arbejds-, uddannelses- og ansættelsesmæssige forhold, interne familieforhold, sociale problemer mm.
Værdioplysninger	Udbudsmateriale, kontraktbestemmelser, fortrolige økonomiske forhold, patentoplysninger, systemdokumentation, infrastrukturbeskrivelser mm.
Andre oplysninger	Interne, åbne og/eller offentlige oplysninger som mødereferater fra styregruppemøder, dagsordener, politikker, strategier, arbejdsnoter uden forretningskritisk indhold og kontaktoplysninger.

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:
- *Forretningscirkulære for persondatabeskyttelse – dokumentation og compliance*
- *Forretningscirkulære for persondatabeskyttelse – registreredes rettigheder*
- *Københavns Kommunes retningslinjer og vejledninger på området*

3.6. Mærkning af informationer

Der skal fastsættes procedurer til mærkning af informationer i kommunens it-systemer i overensstemmelse med det dataklassifikationssystem, som kommunen har vedtaget.

Det skal aktivt sikres, at informationer er korrekt mærkede ift. det fastlagte dataklassifikationssystem med henblik på at leve op til gældende regler for bl.a. sletning, arkivering og journalisering. Disse procedurer skal fastsættes for it-systemer, som behandler mere end én datatype, f.eks. værdioplysninger og følsomme personoplysninger.

Tabel 13: Ansvars- og rollefordeling ift. "Mærkning af data"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Mærkning af informationer i fagspecifikke it-systemer	Ansvarlig forvaltning	Forvaltnings-direktion	Koncern IT	-
Mærkning af informationer i generiske administrative it-systemer	ØKF	ØKF-direktion	-	Forvaltningerne

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forvaltningsspecifikke forretningsgange og regler*

3.7. Opbevaringsperiode for data (sletning og arkivering)

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

Personoplysninger (både almindelige, følsomme og fortrolige) skal slettes eller gøres anonyme, når det ikke længere er nødvendigt for kommunen at have oplysningerne. Det er de enkelte forvaltningers ansvar at vurdere, hvor længe det er nødvendigt at opbevare oplysningerne ud fra de formål, som oplysningerne oprindelig blev indsamlet til. Dermed skal forvaltningerne eksempelvis forholde sig til opbevaringsperioden for data i forbindelse med anskaffelsen af nye it-systemer.

Værdioplysninger, som 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.

Andre oplysninger behøver ikke blive slettet indenfor en fastsat periode, men skal dog slettes, hvis data er forældet eller kan medføre misforståelser, fejlagtig behandling eller på anden måde være til skade for kommunen, medarbejdere, borgere eller erhvervsliv.

Overførsel af oplysninger efter arkivlovens regler herom kan sidestilles med sletning.

Tabel 14: Ansvars- og rollefordeling ift. "Opbevaringsperiode for data (sletning og arkivering)

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Sletning af oplysninger	Forvaltningen	Forvaltnings-direktion	Databeskyttelses-rådgiveren	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes retningslinjer og vejledninger på området*

4. SIKKERHEDSOMRÅDE 4 - ADGANGSSTYRING, BRUGERRETTEDE POLITIKKER MM.

4.1. Brugeradministration

Brugeradministrationen varetages af en centralt placeret brugerstyringsfunktion, som tildeler autorisationer på baggrund af bestilling(er) fra den autorisationsansvarlige.

Al brugeradministration i Københavns Kommune, herunder adgangsstyring og rolle- og rettighedsstyring, varetages af brugerstyringsfunktionen i Koncern IT (med undtagelse af brugeradministrationen på det pædagogiske område). Ansvaret for tildeling og nulstilling af adgangskoder i specifikke systemer kan dog uddelegeres efter dispensation.

Brugeradministrationen på det pædagogiske område varetages af BUF.

Tabel 15: Ansvars- og rollefordeling ift. "Brugeradministration"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Tildeling af autorisationer	Brugerstyringsfunktionen i Koncern IT	ØKF-direktion	-	-
Tildeling af autorisationer på det pædagogiske område	BUF IT-drift	BUF-direktion	-	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes retningslinjer og vejledninger på området*

4.1.1. Autorisationsansvarlige

Den autorisationsansvarlige varetager bestillingen af autorisationer, som den ansvarlige leder for brugeren vurderer, at der er et arbejdsbetinget behov for.

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

Tabel 16: Ansvars- og rollefordeling ift. "Autorisationsansvarlige"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Bestilling af autorisationer	Den autorisations-ansvarlige	Nærmeste leder	Koncern IT	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes retningslinjer og vejledninger på området*

4.1.2. Brugeroprettelser

Til brug for autorisation skal der til it-systemer udarbejdes dokumentation for den løbende tildeling af autorisationer samt retningslinjer, der bl.a. beskriver kriterierne for tildeling af adgange i det pågældende it-system.

Teknisk systemejer skal til stadighed kunne forelægge retvisende og opdateret dokumentation for, hvem der i det givne it-system er tildelt autorisationer i henhold til udarbejdede og ledelsesgodkendte retningslinjer. Disse retningslinjer, som udarbejdes af den forretningsmæssige systemejer, skal som minimum indeholde beskrivelser af, hvilke roller og rettigheder, der kan tildeles brugere, og efter hvilke kriterier rettighederne skal tildeles.

Brugerstyringsfunktionen i Koncern IT fastsætter de generelle retningslinjer for tildeling af autorisationer i it-systemer i Københavns Kommune.

Følgende kriterier gælder 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 it-system,
- deaktiverede eller udløbne bruger-ID må ikke genudstedes til andre end den bruger, som oprindeligt fik det udstedt,
- 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, og
- brugeren kan som udgangspunkt ikke tildeles lokaladministratorrettigheder på arbejds-pc'er.

Tabel 17: Ansvars- og rollefordeling ift. "Brugeroprettelser"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Forelægge dokumentation for tildeling af autorisationer i det givne it-system	Teknisk systemejer	Forvaltnings-direktion	Koncern IT	-
Udarbejde retningslinjer for roller og rettigheder i det givne it-system	Forretningsmæssig systemejer	Forvaltnings-direktion	Koncern IT	-
Udarbejdelse af generelle retningslinjer for tildeling af autorisationer	Brugerstyrings-funktionen i Koncern IT	Brugerstyrings-funktionen i Koncern IT i samarbejde med den forvaltning som er ansvarlig for it-systemet	-	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes retningslinjer og vejledninger på området*

4.1.3. Ændring af brugers autorisationer

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 arbejdsbetinget 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 brugers autorisationer bestilles.

Tabel 18: Ansvars- og rollefordeling ift. "Ændring af brugers autorisationer"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Bestilling af ændrede brugerautorisationer	Den autorisations-ansvarlige	Nærmeste (nye) leder	Koncern IT	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes retningslinjer og vejledninger på området*

4.1.4. Nedlæggelse af brugers autorisationer

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

Brugerens nærmeste leder skal sikre, at brugers autorisationer nedlægges eller deaktiveres, hvis ansættelsesforholdet ophører, eller hvis brugeren i en længere periode ikke kan eller skal varetage de opgaver, hvortil autorisationerne knytter sig.

Tabel 19: Ansvars- og rollefordeling ift. "Nedlæggelse af brugers autorisationer"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes retningslinjer og vejledninger på området*

4.1.5. 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, hvis en entydig identifikation af den pågældende medarbejder kan finde sted. Denne identifikation skal som udgangspunkt foretages ved verificering af medarbejderens CPR-nummer, men kan om nødvendigt ske med pas eller kørekort. Autorisationen skal altid ske på baggrund af en anmodning fra en autorisationsansvarlig i samarbejde med den ansvarlige for aftaleindgåelsen, der sørger for at indhente de nødvendige oplysninger i forbindelse med bestillingen.

Såfremt der er tale om en ekstern samarbejdspartner udenfor EU/EØS, kan det være nødvendigt at forholde sig til kommunens gældende regler for overførsel af personoplysninger til tredje lande.

Tabel 20: Ansvars- og rollefordeling ift. "Autorisationer til eksterne samarbejdspartnere"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Bestilling af autorisationer til eksterne samarbejdspartnere	Den autorisations-ansvarlige	Den kontrakt-ansvarlige	Koncern IT	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes retningslinjer og vejledninger på området*

4.1.6. 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 it-system, herunder systemadministratorrettigheder. Tildeling af sådanne privilegerede rettigheder skal ske ud fra en risikovurdering, skal til enhver tid være dokumenteret og må kun anvendes i begrænset omfang.

Logning af privilegerede rettigheder skal ske i overensstemmelse med reglerne i afsnit 6.6. Kravet om logning af privilegerede rettigheder kan ikke fraviges.

Tabel 21: Ansvars- og rollefordeling ift. "Styring af privilegerede adgangsrettigheder"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes retningslinjer og vejledninger på området*

4.1.7. 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 gives ud fra en risikovurdering, 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 skal altid kunne logges. Hvis det ikke er muligt at etablere teknisk logning, skal logningen foretages manuelt, eller andre foranstaltninger skal istandsættes.

Tabel 22: Ansvars- og rollefordeling ift. "Privilegerede administrative adgange til it-infrastrukturen"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes retningslinjer og vejledninger på området*

4.1.8. Tilsyn med autorisationer

Medarbejderens nærmeste leder skal ud fra en risikobaseret tilgang føre periodiske tilsyn med, at tildelte autorisationer i it-systemer afspejler medarbejderens arbejdsmæssige behov.

For it-systemer, der behandler personoplysninger, skal der dog som udgangspunkt føres tilsyn med, om tildelte autorisationer afspejler medarbejdernes arbejdsmæssige behov, mindst hver sjette måned.

Tilsyn med autorisationer vedrører også eksterne konsulenters autorisationer. Vær her opmærksom på særlige kontraktuelle bestemmelser for det enkelte it-system.

Tabel 23: Ansvars- og rollefordeling ift. "Tilsyn med autorisationer"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forretningscirkulære for ledelsestilsyn*

4.1.9. Integration til brugerstyringsløsning

It-systemer med adgangsstyring, som håndterer person- eller værdioplysninger, skal integreres med kommunens til enhver tid anvendte brugerstyringsløsning til bestilling af autorisationer.

Hvis integration til den gældende brugerstyringsløsning fravælges, skal fravalget dokumenteres og forelægges for Økonomiforvaltningen, som efter koordinering med It-kredsen, kan meddele dispensation herfra.

Integrationen til kommunens anvendte brugerstyringsløsning sikrer, at muligheden for automatiserede ledelsestilsyn med autorisationer altid foreligger. Hvis et it-system ikke integreres til kommunens anvendte brugerstyringsløsning, skal tilsyn med autorisationer gennemføres på anden vis, om nødvendigt manuelt.

Tabel 24: Ansvars- og rollefordeling ift. "Integration til brugerstyringsløsning"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Integration brugerstyrings-løsning	Den enhed som har ansvar for it-systemet	Forvaltnings-direktion	Forvaltningens digitaliseringsenhed og Koncern IT	-

4.2. Adgangsstyring

For at få adgang til kommunens netværk, netværkstjenester, it-systemer mm., skal brugerens identitet verificeres.

Al adgang til kommunens it-systemer, servere, netværk og pc'er, der indeholder person- eller værdioplysninger, skal være betinget af konkrete verificeringer af brugerens identitet, så det sikres at der kun gives retmæssige adgange. Dette gør sig gældende for alle brugere, herunder medarbejdere, eksterne samarbejdspartnere og automatiserede løsninger (RPA). Adgange skal gives via kommunens løsninger til tildeling og styring af adgange.

Brugen af systemprogrammer, der kan omgå systemkontroller og applikationskontroller, skal begrænses og styres effektivt.

Tabel 25: Ansvars- og rollefordeling ift. "Adgangsstyring"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Gældende sikkerhedsstandard(er) på området*
- *Københavns Kommunes retningslinjer og vejledninger på området*

4.2.1. Multifaktor-autentifikation

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

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

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 enkeltstående faktor for adgang til ressourcer, men biometri kan efter omstændighederne 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 multifaktor-login, hvis der er tale om en ekstern it-løsning, som ikke er forbundet med kommunens øvrige it-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 følsomme eller fortrolige personoplysninger eller værdioplysninger, og at fravigelsen beror på en ledelsesgodkendt risikovurdering og en konsekvensanalyse.

Tabel 26: Ansvars- og rollefordeling ift. "Multifaktor-autentifikation"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Implementering af multifaktor-login	Den enhed som har ansvar for it-systemet	Forvaltnings-direktion	Koncern IT	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Gældende sikkerhedsstandard(er) på området*

4.2.2. 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 desuden følgende krav til adgangskoder:

- under hensyn til karakteren af det pågældende it-system/komponent, f.eks. karakteren af indeholdte oplysninger og it-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 loginforsøg og håndhæves i mindst 30 min., medmindre det efter en konkret vurdering findes sikkerhedsmæssigt forsvarligt at acceptere flere mislykkede loginforsøg, og
- adgangskoder skal skiftes ved mistanke om kompromittering, dog mindst én 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 de oplysninger, der behandles på arbejdsstationen.

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

Tabel 27: Ansvars- og rollefordeling ift. "Adgangskoder"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Implementering af principper for adgangskoder	Den enhed som har ansvar for it-systemet	Forvaltnings-direktion	Koncern IT	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes retningslinjer og vejledninger på området*

4.2.3. 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, der med rimelig sikkerhed gør det muligt at verificere brugeren af det alternative identifikationsmiddel.

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

Hvis et alternativt til adgangskoder udvikles til et it-system, efter it-systemet er implementeret og har fået en ibrugtagningstilladelse, skal Koncern IT foretage en ny vurdering, jf. forretningscirkulære for organisering af informationssikkerhed og forretningscirkulære for it-anskaffelser.

Tabel 28: Ansvars- og rollefordeling ift. "Alternativer til adgangskoder"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Implementering af alternativer til adgangskoder	Den enhed som har ansvar for it-systemet	Forvaltnings-direktion	Koncern IT	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forretningscirkulære for organisering af informationssikkerhed*
- *Forretningscirkulære for it-anskaffelser*
- *Københavns Kommunes retningslinjer og vejledninger på området*

4.2.4. Tilkobling til national, digital identitetsinfrastruktur

Alle it-systemer, som er tilkoblet Danmarks nationale, digitale identitetsinfrastruktur, skal følge gældende standarder for adgangsstyring.

Københavns Kommune gør brug af en række digitale løsninger, som er tilkoblet den nationale, digitale identitetsinfrastruktur, som benytter den nationale løsning for adgangsstyring. Det gælder for alle de af kommunens it-systemer, der er tilkoblet den nationale, digitale identitetsinfrastruktur, at der skal fastsættes et passende sikringsniveau ud fra en konkret risikovurdering. For vejledning hertil henvises til den til enhver tid gældende nationale standard for identiteters sikringsniveauer.

Tabel 29: Rolle- og ansvarsfordeling ift. "Tilkobling til national, digital identitetsinfrastruktur".

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Fastsættelse af sikringsniveau ud fra risikovurdering	Forvaltning	Forvaltnings-direktion	Koncern IT	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Gældende sikkerhedsstandard(er) på området*

4.3. Rolle- og rettighedsstyring

It-brugere i kommunen skal kun have de roller og rettigheder, som er relevante for, at de kan udføre deres arbejdsopgaver.

Roller og rettigheder i og til kommunens it-systemer, servere, netværk, pc'er og andre informationsaktiver, hvori person- eller værdioplysninger behandles, skal styres, så brugere med it-adgang kun har de roller og rettigheder, som er nødvendige, for at de kan udføre deres opgaver. Dette gør sig gældende for alle brugere, herunder medarbejdere, eksterne samarbejdspartnere og automatiserede løsninger (RPA). Roller og rettigheder skal styres og gives via kommunens løsninger til rolle- og rettighedsstyring.

Tabel 30: Ansvars- og rollefordeling ift. "Rolle- og rettighedsstyring"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Tildeling af autorisationer	Den autorisations-ansvarlige	Forvaltnings-direktion	Koncern IT	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Gældende sikkerhedsstandard(er) på området*
- *Københavns Kommunes retningslinjer og vejledninger på området*

4.3.1. Funktionsadskillelse

Modstridende funktioner skal som udgangspunkt (og 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 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 -autorisationer til sig selv, men at sådanne autorisationer skal tildeles af brugerstyringsfunktionen i Koncern IT via vedkommendes leder eller den udpegede autorisationsansvarlige.

Tabel 31: Ansvars- og rollefordeling ift. "Funktionsadskillelse"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Teknisk funktions-adskillelse	Forvaltning	Forvaltnings-direktion	Forvaltningens digitaliseringsenhed og evt. Koncern IT	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forvaltningsspecifikke forretningsgange og regler*

4.4. Brugerrettede instrukser

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

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

Tabel 32: Ansvars- og rollefordeling ift. "Brugerrettede instrukser"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Udarbejdelse af forvaltningsspecifikke instrukser	Den enkelte forvaltning	Forvaltnings-direktion	Koncern IT	Medarbejdere i den enkelte forvaltning
Udarbejdelse af generelle instrukser	ØKF	ØKF-direktion	Koncern IT	Forvaltningerne

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Fællesadministrative eller forvaltningsspecifikke forretningsgange på området*

4.4.1. Kommunikation med borgere, virksomheder og myndigheder

Kommunens kommunikation med borgere, virksomheder og andre myndigheder skal ske på en sikker måde, så 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.

Tabel 33: Ansvars- og rollefordeling ift. "Kommunikation med borgere, virksomheder og myndigheder"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Fællesadministrativ forretningsgang for sikker kommunikation (skal udarbejdes)*
- *Københavns Kommunes retningslinjer og vejledninger på området*

4.4.2. Brug af mobile enheder, flytbare lagringsmedier og fjernarbejdspladser

Personoplysninger må kun opbevares på mobile enheder og flytbare lagringsmedier, hvis der er etableret passende teknisk beskyttelse, og hvis brugeren er instrueret i korrekt anvendelse.

Opbevaring af person- og værdioplysninger på mobile enheder og flytbare lagringsmedier udgør en sikkerhedsrisiko. Sikkerhedsrisikoen skal håndteres gennem passende tekniske sikkerhedsforanstaltninger og gennem instruktion af brugerne af mediet.

Mobile enheder *med potentiel dataadgang*, f.eks. telefoner, tablets og computere, er som udgangspunkt personlige 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 multifaktor-login, kryptering, adgangsstyring og nødprocedure for fjernelse af person- og værdioplysninger ved bortkomst. Hvis dette ikke er teknisk muligt, skal der iværksættes passende tekniske og organisatoriske kompenserende foranstaltninger. Ved opbevaring af person- og værdioplysninger på mobile enheder med potentiel dataadgang skal det ligeledes sikres, at eventuelle krav om opbevaringsfrister og logning overholdes. Sådanne enheder må ikke forlades i offentlige rum, hvor udefrakommende kan tilgå dem.

Person- og værdioplysninger må som udgangspunkt ikke opbevares på flytbare lagringsmedier, herunder usb-nøgler, cd'er, dvd'er, eksterne harddiske, hukommelseskort og lignende. Der kan gøres undtagelser i tilfælde, hvor fysisk transport af oplysninger er en nødvendighed. Her skal oplysningerne sikres på forsvarlig vis, f.eks. i aflåste bokse eller ved kryptering af indhold (se afsnit 5.10).

Fjernarbejdspladser må ikke anvendes af andre end dem, som fjernarbejdspladsen er tiltænkt, eller af kommunens it-medarbejdere, hvis dette sker som led i udførelsen af en it-service, som f.eks. installation eller reparation. Fjernarbejdspladser skal stilles til rådighed for kommunen i forbindelse med it-sikkerhedskontroller, servicering mv. For at få adgang til kommunens interne netværk fra en fjernarbejdsplads, skal brugeren anvende en krypteret forbindelse. Der må ikke behandles eller opbevares personoplysninger eller værdioplysninger på it-udstyr, der ikke tilhører kommunen, medmindre der er indgået aftale herom, f.eks. en databehandleraftale.

Tabel 34: Ansvars- og rollefordeling ift. "Brug af mobilt udstyr, flytbare lagringsmedier og fjernarbejdspladser"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes retningslinjer og vejledninger på området*
- *Forvaltningsspecifikke forretningsgange og regler*

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 person- 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 hvor kun kommunale medarbejdere og autoriserede eksterne samarbejdspartnere har adgang.
- Åbne administrationsområder: områder med begrænsede krav til sikkerheden, men med områder 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).

Hver forvaltning fastsætter selv sikkerhedsniveauet for sine lokationer samt de nærmere sikkerhedsregler på lokationerne med henblik på sikring af kommunens informationsaktiver.

Tabel 35: Ansvars- og rollefordeling ift. "Fysisk sikkerhed"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forvaltningsspecifikke forretningsgange og regler*

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 server- og teknikrum, så 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 skal der være etableret passende fysisk adgangskontrol (f.eks. aflåsning). Der skal desuden føres fortegnelse over sikre og kontrollerede områder, hvori det bl.a. fremgår, om det er den pågældende forvaltning selv eller en ekstern leverandør, der er ansvarlig for sikringen af området.

Tabel 36: Ansvars- og rollefordeling ift. "Sikre og kontrollerede områder"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forvaltningsspecifikke forretningsgange og regler*

5.2.1. Af- og pålæsningsområder

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.

Tabel 37: Ansvars- og rollefordeling ift. "Af- og pålæsningsområder"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forvaltningsspecifikke forretningsgange og regler*

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 skal i sådanne områder være et særligt fokus på:

- at pc'er låses, når de forlades,
- at computerskærme placeres eller dækkes, så de ikke er synlige for uvedkommende,
- at udskrivningen af fysiske dokumenter med person- og værdioplysninger begrænses,
- at fysiske dokumenter, som anvendes, ikke kan læses af uvedkommende,
- at fysiske indgange (f.eks. USB-porte) på enheder sikres på passende vis,
- at fysiske dokumenter i øvrigt kan opbevares i aflåste skabe eller skuffer, og
- at lokaler, hvori der opbevares fortrolige informationer mv. så vidt muligt låses, når de ikke er bemandede.

Tabel 38: Ansvars- og rollefordeling ift. "Åbne administrationsområder og modtagelsesområder"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forvaltningsspecifikke forretningsgange og regler*

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 data, mængden af data og graden af kontakt med f.eks. borgere eller øvrige tredjeparter.

Tabel 39: Ansvars- og rollefordeling ift. "Åbne og delvist åbne områder"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forvaltningsspecifikke forretningsgange og regler*

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, medmindre 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, hvis overvågningen sker i forbindelse med særligt kriminalitetsforebyggende og tryghedsskabende initiativer.

Etablering af tv- og videoovervågning er at regne for en it-anskaffelse, hvorfor man her skal følge anskaffelsesprocessen, som fremgår af forretningscirkulære for it-anskaffelser.

Tabel 40: Ansvars- og rollefordeling ift. "Tv- og videoovervågning"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Overholdelse af regler om tv-overvågning	Forvaltningen	Forvaltnings-direktion	DPO Business Partner og Databeskyttelses-rådgiveren	-
Etablering af tv- og videoovervågning	Forvaltningen	Forvaltnings-direktion	Koncern IT	Koncern IT

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forretningscirkulære for it-anskaffelser*
- *Københavns Kommunes retningslinjer og vejledninger på området*

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 person- eller værdioplysninger, skal placeres, så det er beskyttet mod adgang fra uvedkommende. Printere, der benyttes til udskrivning af person- 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.

Tabel 41: Ansvars- og rollefordeling ift. "Beskyttelse af udstyr"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forvaltningsspecifikke forretningsgange og regler*

5.7. Forsyningssikkerhed

Der skal være etableret foranstaltninger, anlæg mm., så 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) kommunikationsforbindelser 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.

Tabel 42: Ansvars- og rollefordeling ift. "Forsyningssikkerhed"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forvaltningsspecifikke forretningsgange og regler*

5.8. Transmission af information

Transmission af person- og værdioplysninger i kabler og udstyr skal beskyttes mod uautoriserede indgreb.

Kommunens person- og værdioplysninger, som transmitteres i kabler og udstyr til datakommunikation, skal i relevant omfang beskyttes mod aflytning, uautoriserede indgreb og interferens. Faste kabler og udstyr skal mærkes klart og entydigt.

Tabel 43: Ansvars- og rollefordeling ift. "Transmission af data"

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

5.9. Bortskaffelse af it-udstyr

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

Bortskaffelse af usb-nøgler, cd'er, dvd'er, hukommelseskort og lignende må 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 al data lagret på udstyret slettes på en sådan måde, at data ikke kan gendannes, jf. de til enhver tid gældende forretningsgange herom.

Tabel 44: Ansvars- og rollefordeling ift. "Bortskaffelse af it-udstyr"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forvaltningsspecifikke forretningsgange og regler*

5.10. Transport af information

Medier, der indeholder information, skal beskyttes mod uautoriseret adgang, misbrug eller ødelæggelse under transport.

Hvis person- og værdioplysninger skal transporteres fysisk, f.eks. via flytbare lagringsmedier eller i papirformat, skal oplysningerne sikres på betryggende vis. Oplysningerne skal være tilstrækkeligt beskyttet mod fysisk skade, herunder miljømæssige forhold som varme, fugt og elektromagnetiske felter, og, hvis muligt, gennem kryptering, for at sikre, at uvedkommende ikke kan tilgå oplysningerne. Når kryptering ikke er mulig, skal afsender overveje øvrige sikringsforanstaltninger, f.eks. aflåste bokse. Fysisk transport af person- og værdioplysninger skal finde sted gennem anvendelse af pålidelige og ledelsesgodkendte transportører og kurerer, og indgående og udgående fysiske medier skal registreres.

Fysisk transport af medier med person- og værdioplysninger skal være godkendt på et relevant ledelsesniveau.

Tabel 45: Ansvars- og rollefordeling ift. "Transport af information"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Transport af information	Forvaltningen	Forvaltnings-direktion	Koncern IT og DPO Business Partner	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forvaltningsspecifikke forretningsgange og regler*

6. SIKKERHEDSOMRÅDE 6 - DRIFTSIKKERHED

6.1. Driftsafviklingsprocedurer

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

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

Tabel 46: Ansvars- og rollefordeling ift. "Driftsafviklingsprocedurer"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Udarbejdelse af driftsprocedurer	Teknisk systemejer	Forvaltnings-direktion	Koncern IT	-

6.2. Kapacitetsstyring

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

Der skal være defineret tærskelværdier ved fejl på f.eks. CPU, disk, netværk 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, it-systemer, miljøer mm.

Tabel 47: Ansvars- og rollefordeling ift. "Kapacitetsstyring"

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

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 flytbare lagringsmedier.

Der skal gennemføres periodisk review af sikringsløsningerne for at sikre, at alle enheder er aktive og beskyttet med seneste signaturer. Håndtering af kritiske observationer, der ikke automatisk kan håndteres af den pågældende antivirus/malware-løsning, skal dokumenteres med handleplan.

Tabel 48: Ansvars- og rollefordeling ift. "Skadevoldende programmer og ondsindet kode"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes retningslinjer og vejledninger på området*

6.4. Teknisk sårbarhedsstyring

Der skal løbende indhentes informationer om tekniske sårbarheder i kommunens it-systemer, netværk og infrastruktur. Kommunens eksponering for sådanne sårbarheder skal evalueres, og der skal iværksættes passende foranstaltninger for at håndtere den tilhørende risiko.

Kommunen skal have etableret processer, som tager hånd om den tekniske sårbarhedsstyring af kommunens it-systemer, netværk og infrastruktur. Herunder gælder bl.a., at kommunen skal have etableret processer for sårbarhedsovervågning, patching, aktivsporing mm. Når tekniske sårbarheder opdages, skal alvorligheden og relevansen for Københavns Kommune vurderes, og passende handleplaner skal udarbejdes, prioriteres og implementeres ud fra en risikovurdering.

Tabel 49: Ansvar- og rollefordeling ift. "Teknisk sårbarhedsstyring"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Udarbejdelse af procedurer og løbende overvågning	Den forvaltning som er ansvarlig for det pågældende informationsaktiv	Forvaltnings-direktion	-	Forvaltningerne

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes retningslinjer og vejledninger på området*

6.5. 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 it-systemer og data, der har væsentlig betydning for kommunens myndighedsudøvelse og drift. Krav til backup-konfigurationer for alle it-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 backuppen, dels at it-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 it-systemer og 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.

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

Personoplysninger, som befinder sig i backuppen, følger de gængse opbevaringsregler for personoplysninger og skal slettes indenfor den fastsatte ramme for opbevaring af personoplysninger. I forbindelse med gendannelse af personoplysninger ved indlæsning af backuppen (restore) skal integriteten, dvs. rigtigheden, af de gendannede oplysninger sikres. Der skal føres logs over gendannelsen af personoplysninger, og disse logs skal som minimum omfatte navnet på den ansvarlige for gendannelsen samt en beskrivelse af de gendannede oplysninger.

Tabel 50: Ansvars- og rollefordeling ift. "Backup"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes retningslinjer og vejledninger på området*

6.6. Logning og monitorering

6.6.1. Logning generelt

Logning foretages i forhold til såvel brugere som it-systemer. Logning af aktiviteter skal være baseret på en risikovurdering, så der kun logges for relevante og nødvendige hændelser.

Af hensyn til Københavns Kommunes drifts- og sikkerhedsmæssige forhold er udgangspunktet, at al brug af kommunens it-systemer løbende skal registreres (logges). Hvis et it-system ikke behandler person- eller værdioplysninger, vil kravet om logning være mindre omfangsrigt.

Logning skal foretages på en måde, så det efterfølgende er muligt at (gen)etablere de foretagne 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, så risikoen for uautoriseret adgang eller manipulation af indholdet reduceres.

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

Logdata indeholdende person- og værdioplysninger 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.

Tabel 51: Ansvars- og rollefordeling ift. "Logning generelt"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Gældende sikkerhedsstandard(er) på området*

6.6.2. Logning af brugeradfærd

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

De nærmere bestemmelser for brugerlogning kan findes i den til enhver tid gældende standard, kommunen benytter sig af.

Tabel 52: Ansvars- og rollefordeling ift. "Logning af brugeradfærd"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Gældende sikkerhedsstandard(er) på området*

6.6.3. Logning af systemadministrators adfærd

I it-systemer med person- eller værdioplysninger skal aktiviteter, som udføres af systemadministratorer og andre med særlige rettigheder, logges.

Hvor det er teknisk muligt, skal der være etableret funktionsadskillelse, så systemadministratorer ikke selv kan ændre loginformationer. Se i øvrigt afsnit 4.3.1.

Tabel 53: Ansvars- og rollefordeling ift. "Logning af systemadministrators adfærd"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Gældende sikkerhedsstandard(er) på området*

6.6.4. Integration til SIEM

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

Tabel 54: Ansvars- og rollefordeling ift. "Integration til SIEM"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Gældende sikkerhedsstandard(er) på området*

6.6.5. Systemlogning

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

De nærmere bestemmelser for systemlogning kan findes i den til enhver tid gældende standard, kommunen benytter sig af.

Tabel 55: Ansvars- og rollefordeling ift. "Systemlogning"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Gældende sikkerhedsstandard(er) på området*

6.6.6. Opfølgning på systemlog

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.

Tabel 56: Ansvars- og rollefordeling ift. "Opfølgning på systemlog"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Gældende sikkerhedsstandard(er) på området*
- *Forvaltningsspecifikke forretningsgange og regler*

6.6.7. Monitorering

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

Københavns Kommune skal af sikkerhedshensyn monitorere og logge kommunens egne netværk og it-systemer og brugernes adfærd i disse.

Den ansvarlige enhed for et it-system er ansvarlig for, at der gennemføres periodiske udtræk fra it-systemets log for f.eks. at kontrollere adgange og behandling af data.

Tabel 57: Ansvars- og rollefordeling ift. "Monitorering"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Monitorering af it-systemer	Den enhed som har ansvar for it-systemet	Forvaltnings-direktion	Forvaltningens digitaliseringsenhed og Koncern IT	-
Monitorering af netværk	Koncern IT	KIT-direktion	-	-

6.6.8. Mistanke om misbrug

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 et udtræk af logfiler. Udtræk og andre logfiler må kun benyttes til kontrol af medarbejderes adfærd, internetbrug eller øvrige brug af it-systemer, hvis kommunens personalejuridiske funktion konkret har tilkendegivet, at der er et lovligt grundlag for at anvende den pågældende log i kontroløjemed. Udtrækkene skal altid opbevares på sikker vis, så 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.

Tabel 58: Ansvars- og rollefordeling ift. "Mistanke om misbrug"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Berettiget kontrol på medarbejderniveau	Den enhed som har ansvar for it-systemet	Forvaltnings-direktion	Forvaltningens digitaliseringsenhed, personalejuridisk funktion 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 afsnit 4.1.7 om privilegerede administrative adgange til it-infrastrukturen.

Tabel 59: Ansvars- og rollefordeling ift. "Styring af netværkssikkerhed"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes retningslinjer og vejledninger på området*

7.2. Design af sikker netværksinfrastruktur

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 it-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.

Installation og konfiguration af nyt netværksudstyr skal omfatte konfiguration af basale sikkerhedsparametre.

Tabel 60: Ansvars- og rollefordeling ift. "Design af sikker netværksinfrastruktur"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Gældende sikkerhedsstandard(er) på området*

7.3. Opdeling i netværk

Kommunens netværk skal opdeles i separate netværksdomæner for at adskille administrative netværk med øvrige netværk.

Kommunens administrative netværk skal holdes fysisk og logisk adskilte fra publikumsnetværket, som borgere kan tilgå. Alt netværksudstyr med borgeradgang skal afvikles på publikumsnetværket for at sikre mod, at eksterne får utilsigtet adgang til kommunens administrative netværk.

Alle eksterne, som får adgang til Københavns Kommunes gæstenetværk eller publikumsnetværk, skal præsenteres for en startside med krav og accept af vilkår for brug.

Tabel 61: Ansvars- og rollefordeling ift. "Opdeling i netværk"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Opdeling i separate netværk	Koncern IT/BUF IT-drift	Direktion i ØKF/BUF	-	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes retningslinjer og vejledninger på området*

7.4. Udveksling af data

Der skal foreligge procedurer for udveksling af data for at sikre, at kommunens og borgernes data ikke kompromitteres.

Kommunen skal opretholde informationssikkerheden ved udveksling af data internt og med eksterne samarbejdspartnere. Når data overføres, skal det sikres, at modtageren ikke kan tilgå mere data end nødvendigt.

Gældende retningslinjer for intern udveksling af person- og værdioplysninger i Københavns Kommune skal iagttages. Se afsnit 9.1 for yderligere specificering om reglerne vedr. eksterne leverandørers behandling af kommunens data.

Tabel 62: Ansvars- og rollefordeling ift. "Udveksling af data"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Dokumentere forhold for dataudveksling	Forvaltningen	Forvaltnings-direktion	Koncern IT	-
Udarbejde retningslinjer for dataudveksling	Koncern IT	ØKF-direktion	Databeskyttelses-rådgiveren	Forvaltningerne

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes skabelon for databehandleraftaler*
- *Københavns Kommunes retningslinjer og vejledninger på området*

7.5. Kryptografi

Der skal være etableret løsninger til, at al datatransmission til og fra kommunens it-systemer og indenfor kommunens netværk er 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.

Tabel 63: Ansvars- og rollefordeling ift. "Kryptografi"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Gældende sikkerhedsstandard(er) på området*

7.6. Elektronisk handel og betaling

Informationer, der benyttes i forbindelse med elektronisk handel og betaling, skal 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.

Tabel 64: Ansvars- og rollefordeling ift. "Elektronisk handel og betaling"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes Kasse- og Regnskabsregulativ*
- *Gældende sikkerhedsstandard(er) på området*

7.7. Ind- og uddata

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

Inddata omfatter navnlig person- eller værdioplysninger, som opbevares i papirformat eller på elektroniske medier med henblik på indlæsning i kommunens it-systemer. Uddata omfatter navnlig person- eller værdioplysninger, som udskrives på papir eller kopieres over på flytbare lagringsmedier.

Adgangen til person- eller værdioplysninger 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 værdioplysninger, 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 anvendes en betryggende transportform (se afsnit 5.10).

Præsentation af data i fysisk form bør begrænses for at undgå uønsket offentliggørelse eller misbrug.

Tabel 65: Ansvars- og rollefordeling ift. "Ind- og uddata"

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

8. SIKKERHEDSOMRÅDE 8 - ANSKAFFELSE, UDVIKLING OG VEDLIGEHOLDELSE

8.1. Sikkerhed ift. indkøb og nyudvikling af it-systemer

It-systemer og hjælpeværktøjer, der anskaffes eller udvikles fra ny, skal overholde kommunens krav til sikkerhed og databeskyttelse.

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

I tilknytning til reglerne for sikkerhed, som er fastsat i dette forretningscirkulære, skal den anskaffende enhed ved anskaffelse, udvikling og ændring af it-systemer følge kommunens regler for persondatabeskyttelse (f.eks. om konsekvensanalyser og om understøttelse af de registreredes rettigheder, herunder fastsættelse af slettefrister) samt kommunens processer for it-anskaffelser. Der henvises i den forbindelse til forretningscirkulærerne for henholdsvis persondatabeskyttelse og it-anskaffelser og dertilhørende forretningsgange.

Tabel 66: Ansvars- og rollefordeling ift. "Sikkerhed ift. indkøb og nyudvikling af it-systemer"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forretningscirkulære for it-anskaffelser*
- *Forretningscirkulære for persondatabeskyttelse – dokumentation og compliance*
- *Forretningscirkulære for persondatabeskyttelse – registreredes rettigheder*
- *Fællesadministrativ forretningsgang for fælles it-anskaffelser*
- *Fællesadministrativ forretningsgang for fagspecifikke it-anskaffelser*

8.2. Ændringer af it-systemer

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

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

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

Tabel 67: Ansvars- og rollefordeling ift. "Ændringer af it-systemer"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Forelæggelse af ændringer for CAB	Teknisk systemejer	Forvaltnings-direktion	Koncern IT	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Gældende forretningsgange på området*

8.3. Styring af programkildekode i større driftsmiljøer

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

Medmindre der er tale Open Source-koder, må kildekoder 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 licensgiveren for kommunen og for andre kunder eller offentligheden, hvad enten licensgiveren er leverandør eller en tredjepart.

Det skal sikres, at der er revisionshistorik på ændringer til kildekode, og tidligere versioner af kildekode skal gemmes, så tidligere versioner kan gendannes.

Tabel 68: Ansvars- og rollefordeling ift. "Styring af programkildekode i større driftsmiljøer"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Opbevaring af kildekoder	Forvaltningens digitaliseringsenhed	Forvaltnings-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, medmindre det kan begrundes, dokumenteres og godkendes af den ansvarlige enheds ledelse, at der ikke er risiko for, at person- eller værdioplysninger mistes, ændres, at uvedkommende får adgang til det, eller at it-systemet eller andre it-systemer lider skade.

Tabel 69: Ansvars- og rollefordeling ift. "Adskillelse af udviklings- og testmiljøer fra produktionsmiljøer"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forretningscirkulære for it-anskaffelser*

8.5. Udførelse af test

Der må som udgangspunkt ikke testes i produktionsmiljøer.

Der må ikke testes i produktionsmiljøer, medmindre det på forhånd begrundes, dokumenteres og godkendes af den ansvarlige enheds direktion, at der ikke er risiko for, at kommunens data mistes, ændres, at uvedkommende får adgang til det, eller at it-systemet eller andre it-systemer lider skade.

Tabel 70: Ansvars- og rollefordeling ift. "Udførelse af test"

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

8.6. Anvendelse af testdata

Person- eller værdioplysninger må som udgangspunkt ikke bruges som testdata.

Person- eller værdioplysninger må ikke anvendes i tests, medmindre der foretages anonymisering af oplysningerne, eller det på forhånd begrundes, dokumenteres og godkendes af den ansvarlige enheds direktion, at der er taget passende sikkerhedsmæssige foranstaltninger, for at sikre, at der tages hensyn til den registreredes rettigheder, og at kommunens data ikke mistes, ændres, at uvedkommende ikke får adgang til data, eller at it-systemet eller andre it-systemer ikke lider skade. I et sådan tilfælde skal reglerne for tests og afprøvninger iagttages, som de står anført i forretningscirkulære for it-anskaffelser. 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.

Tabel 71: Ansvars- og rollefordeling ift. "Anvendelse af testdata"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forretningscirkulære for it-anskaffelser*

9. SIKKERHEDSOMRÅDE 9 - LEVERANDØRFORHOLD

9.1. Aftaler med leverandører

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, herunder cloududbydere, efterlever Københavns Kommunes krav til sikkerhed, persondatabeskyttelse, stabilitet og tilgængelighed.

Hvis samarbejdet med en leverandør forudsætter, at eksterne skal behandle personoplysninger på vegne af Københavns Kommune, gælder det, at enheden med ansvar for leverandørforholdet skal indgå en databehandleraftale. Ved behandling af øvrige datatyper skal leverandørens behandling på vegne af kommunen dokumenteres i kontrakten.

Se forretningscirkulære for persondatabeskyttelse – dokumentation og compliance for mere information om databehandleraftaler.

Tabel 72: Ansvars- og rollefordeling ift. "Aftaler med leverandører"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forretningscirkulære for persondatabeskyttelse – dokumentation og compliance*
- *Gældende skabeloner på de givne områder*

9.2. Ændringer af leverandørydelser

Ændringer af leverandørydelser skal styres under hensyntagen til, hvor kritiske de involverede forretningsinformationer, forretningssystemer og forretningsprocesser er, og til en revurdering af risici.

Ændring af leverandørydelser, herunder vedligeholdelse og forbedringer af eksisterende informationssikkerhedspolitikker, informationssikkerhedsprocedurer og informationssikkerhedskontroller, skal tage hensyn til kommunens sikkerhedsregler, så de givne ændringer ikke går ud over kommunens informationssikkerhed.

Hvis ændringer af leverandørydelser har en indflydelse på risikoniveauet for det givne it-system eller den givne proces, vil det være nødvendigt at genbesøge og opdatere den dertilhørende konsekvensanalyse. Se forretningscirkulære for persondatabeskyttelse – dokumentation og compliance for mere information om konsekvensanalysen.

Tabel 73: Ansvars- og rollefordeling ift. "Ændringer af leverandørydelser"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forretningscirkulære for persondatabeskyttelse – dokumentation og compliance*

10. SIKKERHEDSOMRÅDE 10 - STYRING AF INFORMATIONSSIKKERHEDS-HÆNDELSER OG BEREDSKAB

10.1. Informationssikkerhedshændelser

Kommunens procedure for indberetning af informationssikkerhedshændelser skal følges.

Koncern IT skal orienteres om såvel potentielle som reelle informationssikkerhedshændelser i henhold til kommunens forretningsgange herfor. Informationssikkerhedshændelser forstås som hændelser, som kan have kompromitterende betydning for kommunens informationssikkerhedsforhold, f.eks. installation af malware, overtrædelser af kommunens politikker eller brud på den fysiske sikkerhed.

Medarbejdere, der har mistanke om eller konstaterer sikkerhedsbrud, skal indmelde bruddet via en fast systemindgang og notere væsentlige detaljer om bruddet.

Den ansvarlige forvaltning og dennes driftsleverandør (herunder Koncern IT) er ansvarlig for håndtering af bruddet og for at iværksætte nødvendige foranstaltninger for at korrigere de konstaterede fejl og svagheder.

Et sikkerhedsbrud kan også forekomme i form af et persondatabrud, hvis personoplysninger er blevet kompromitteret. I et sådan tilfælde skal bruddet indberettes via samme faste systemindgang eller ved at kontakte ens DPO Business Partner. Se mere om håndtering af persondatabrud i forretningscirkulære for persondatabeskyttelse – dokumentation og compliance og den fællesadministrative forretningsgang for persondatabrud.

Tabel 74: Ansvars- og rollefordeling ift. "Informationssikkerhedshændelser"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Indberetning af informations-sikkerhedshændelser	Medarbejder	Forvaltnings-direktion	Forvaltningens digitaliserings enhed og Koncern IT	Koncern IT
Håndtering af informations-sikkerhedshændelser	Koncern IT	ØKF-direktion	-	Indberetter
Indberetning og håndtering af persondatabrud	Medarbejder	Nærmeste leder	DPO Business Partner	Forvaltnings-direktion, Databeskyttelses-rådgiveren og den forurettede

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forretningscirkulære for persondatabeskyttelse – dokumentation og compliance*
- *Fællesadministrativ forretningsgang for håndtering af persondatabrud*

10.2. Rapportering af informationssikkerhedshændelser

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

Afrapporteringen indeholder opsamling og bearbejdning af informationssikkerhedshændelser og persondatabrud for hele kommunen. Der redegøres i denne forbindelse ligeledes for, hvilke forbedrende tiltag, der er iværksat.

Tabel 75: Ansvars- og rollefordeling ift. "Rapportering af informationssikkerhedshændelser"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Afrapportering til Økonomiudvalget	Koncern IT	ØKF-direktion	-	Økonomi-udvalget
Afrapportering til forvaltningsdirektion	Forvaltningens digitaliseringsenhed	Forvaltningens digitaliseringsenhed	-	Forvaltnings-direktion

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Forretningscirkulære for organisering af informationssikkerhed*

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 ud fra en risikobetragtning og skal følge gældende forretningsgange.

Tabel 76: Ansvars- og rollefordeling ift. "Beredskabsstyring"

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

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- *Københavns Kommunes tværgående it-beredskabsplan*
- *Forvaltningsspecifikke beredskabsplaner*

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 med den fornødne viden
- At omfanget af risikovurderinger skal være proportionalt med det vurderede områdes betydning og det aktuelle trusselsbillede for Københavns Kommune
- 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.

Tabel 77: Ansvars- og rollefordeling ift. "Risikovurderinger af it-systemer og it-infrastruktur"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Udarbejdelse af risikovurderinger af it-systemer	Koncern IT	ØKF-direktion	-	-
Opfølgning på risikovurderinger	Forvaltningens digitaliseringsenhed	Forvaltnings-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 it-systemer og data via lederen på det pågældende område, og al brug af revisionsværktøjer og adgange skal registreres ved tilstrækkelig logning. Revisionens adgange skal inddrages, når adgangene ikke længere tjener et formål for revisionen.

Tabel 78: Ansvars- og rollefordeling ift. "It-revisioner"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Bistand til it-revisioner	Den enhed som har ansvar for det reviderede område	Forvaltnings-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.

Jf. ISO27001 skal politikkerne for informationssikkerhed gennemgås med jævne mellemrum. Dette forretningscirkulære revideres i henfør til den periodiske ajourføring af Informationssikkerhedsregulativet.

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, Økonomiudvalgets og It-kredsens beslutninger måtte indebære konsekvensrettelser i forretningscirkulæret.

Forretningscirkulære for informationssikkerhed