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

Københavns Kommune

Kultur- og Fritidsforvaltningen

Bilag 9c

IT-sikkerhedsdokumenter

1 INDHOLD

1. INTERNE ORGANISATORISKE FORHOLD

De interne organisatoriske forhold er fastsat i "Regulativ for it-sikkerhed i Københavns Kommune". Beskrivelsen omfatter alle forvaltningerne. F.eks. beskrives ansvar/opgaverne for direktion, It-sikkerhedsfunktion, systemejer, den Driftsansvarlige, Brugeradministrationen, Autorisationsansvarlige, ledere og medarbejdere.

1.1 ORGANISERING AF AFTALER MED EKSTERNE SAMARBEJDSPARTNERE

Ved indgåelse af aftaler med eksterne samarbejdspartnere er systemejeren ansvarlig for at sikre at samarbejdspartneren underskriver en tavshedspligtserklæring, hvis samarbejdspartneren som led i samarbejdet får adgang til kommunens netværk.

Ved indgåelse af aftaler med eksterne samarbejdspartnere, der indebærer, at samarbejdspartneren skal foretage databehandling på kommunens vegne, skal der for større systemer indgås en databehandleraftale, hvis indhold er i overensstemmelse med en af IT-sikkerhedsfunktionen udarbejdet skabelon. Databehandleraftalen sikrer at den eksterne samarbejdspartner ved hvilke regler han skal overholde og at han har tavshedspligt. IT-sikkerhedsfunktionen kan dog godkende at der anvendes andre databehandleraftaler.

Udveksling af person- og værdioplysninger i form af udtræk fra et system til et andet skal ske i henhold til retningslinjer udarbejdet af systemejeren.

1.2 STYRING AF AKTIVER

De væsentlige aktiver hos kommunen er grupperet i kategorier, således at ansvar for disse aktiver kan decentraliseres.

- IT-systemaktiver og informationer. F.eks. driftssystemer, forretningssystemer, m.m.
- Slutbruger aktiver. F.eks. udstyr til arbejdspladser
- Mobilt IT-udstyr. F.eks. telefoner, Smartphones, tablets, mm.
- Infrastruktur og netværk. F.eks. Netværk, kabling, mm.
- Servere. Dette omfatter elementer til serverdrift såsom hardware, SAN, UPS, mm.
- Print/multifunktionsenheder. Omfatter printere, fax, kopi, scan, mm.

1.2.1 Ansvar for IT-aktiver

- Alle væsentlige IT-systemer skal dokumenteres i kommunens systemfortegnelse FISKK hvilket er systemejernes ansvar.

- Systemejerne for kritiske systemer er ansvarlige for at der sker ajourføring af driftsplaner og godkendelse af disse.
- Ansvar for administrering og ajourføring af IT-aktiver ligger hos den forretningsenhed, der varetager driften af de pågældendes It-aktiver.

1.1.1.1. Fortegnelse over IT-aktiver

- I samarbejde med forvaltningerne definerer Koncern Service hvilke typer af IT-aktiver, der anses for hhv. kritiske og væsentlige.
- Som led i risikovurderingen skal IT-sikkerhedsfunktionen sikre, at der til enhver tid findes en ajourført fortegnelse over alle væsentlige IT- og informationsaktiver.
- Koncern Service har ansvaret for at der føres lister over væsentlige IT-aktiver.
- Der skal tages stilling til arkivering og eventuel sletning af oplysninger.
- Placering af kritiske IT-aktiver skal registreres, herunder placering i sikre områder.

1.1.1.2. Ejerskab til information

Kommunen ejer alle ikke private informationer, som lagres i kommunens IT-systemer, herunder på medarbejdernes IT-udstyr, og forbeholder sig ret til inden for lovens grænser frit at anvende disse informationer.

1.3 KLASSIFIKATION AF INFORMATION OG DATA

Klassifikationen af data hos kommunen tager udgangspunkt de lovmæssige krav der er gældende for personoplysninger og Justitsministeriets Bekendtgørelse om IT-sikkerhed nr. 528. Der er ydermere foretaget en klassifikation af data i forhold til interne oplysninger, hvoraf nogle vil blive vurderet som fortrolige.

1.3.1 Klassifikation af informationer og data

Personoplysninger, fortrolige/følsomme. Omfatter etnisk tilhørsforhold, religion, sociale forhold, straffeforhold, helbredsoplysninger m.m.

Personoplysninger, almindelige. Kan indeholde identificerbare oplysninger: Det være sig navn, adresse, e-post, telefonnumre, mm.

Værdioplysninger. Oplysninger der har en væsentlig økonomisk eller forvaltningsmæssige værdi for kommunen, og hvor offentliggørelse vil forårsage væsentlige skade på Københavns Kommunens forvaltning, omdømme eller økonomi. Det gælder f.eks. visse økonomidata, data om IT-infrastruktur, fortrolige forretningsplaner eller udbudsmateriale.

Interne data. Omfatter oplysninger der ikke er person- eller værdioplysninger, men kun er tiltænkt internt brug i Københavns Kommune, og hvor offentliggørelse kun vil forårsage ubetydelig skade på Københavns Kommunes forvaltning, omdømme eller kun ubetydelig økonomisk effekt, som f.eks. vagtplaner og interne notater.

Åbne data. Omfatter alt hvad der ikke er omfattet af ovenstående f.eks. Som f.eks. alle oplysninger, der er egnet til almen offentliggørelse, åbne dagsordner, borger og erhvervsinformation.

1.4 MEDARBEJDERSIKKERHED

1.1.2. Ansættelse af medarbejdere

Alle medarbejdere skal senest på tiltrædelsestidspunktet og som en del af ansættelsesaftalen erklære at være bekendt med, at de er underlagt IT-sikkerhedshåndbogen og reglerne om tavshedspligt, jf. forvaltningslovens § 27 og straffelovens § 152 og §§ 152 c-152 f. Ansvaret herfor påhviler medarbejderens nærmeste overordnede.

1.1.3. Under ansættelsesforholdet

- Den nærmeste leder er ansvarlig for, at medarbejderen er informeret om sine opgaver og ansvar i forhold til IT-sikkerheden, inden der gives adgang til kommunens it-systemer.
- Alle medarbejdere får ved adgang til kommunens netværk et elektronisk brev om kommunens IT-sikkerhedsregler og et link til kommunens IT-sikkerhedshåndbog som de har pligt til at læse.

1.1.4. Ved ansættelsesforholdets ophør

- Medarbejderens nærmeste leder sikrer, at medarbejderen senest ved ansættelsesforholdets ophør afleverer IT-udstyr og lignende, som tilhører kommunen.
- Medarbejderens nærmeste leder skal orientere medarbejderen om at tavshedspligten stadig gælder efter ansættelsesforholdets ophør.
- Det skal sikres at inddragelse af medarbejderes adgangsrettigheder sker i henhold til en af Koncernservice godkendt procedure.

1.1.4.1. Akut ophør af medarbejder

- Det skal sikres, at rettigheder og adgange til systemer og data bliver deaktiveret hurtigst muligt efter gældende procedure.
- Ved akut ophør må data på arbejdsstationer, mobilt IT-udstyr og e-mail konti ikke slettes, men skal arkiveres for eventuelle videre undersøgelser.

1.5 FYSISK SIKKERHED

Kommunen skal sikre sig, at der er etableret en passende fysisk sikkerhed omkring området og kritiske områder, såsom databehandlingssteder og andre steder, hvor der kunne ligge personfølsomme oplysninger eller værdioplysninger. Eksempler er områder med borgeradgange, arkiver, serverrum, netværksudstyr og lignende. Kommunen bruger følgende kategorier af sikre områder, som er defineret i det følgende:

1. Sikre områder
2. Kontrollerede områder
3. Åbne områder med borgeradgang og ubemandede områder.

1.1.5. Sikre områder

1.1.5.1. Generelt om sikre områder

- Krydsfelter, serverrum og andre steder, hvor netværksudstyr er placeret, anses altid som sikre områder.
- Den lokale ledelse kan i samarbejde med IT-sikkerhedsfunktionen træffe beslutning om inddragelse af andre områder som sikre områder.
- Den driftsansvarlige skal føre en fortegnelse over sikre områder. Det skal fremgå af fortegnelsen om det er den driftsansvarlige, eksterne eller den lokale ledelse der er ansvarlige for området.
- Sikre områder skal være afgrænset og beskyttet i henhold til en risikovurdering, der omfatter de informationsaktiver der opbevares i området.
- Den driftsansvarlige skal i samarbejde med IT-sikkerhedsfunktionen fastsætte minimumsretningslinjer for fysisk sikring herunder eventuelle retningslinjer for godkendelse af personale med adgang til sikre områder.
- Den driftsansvarlige er ansvarlig for at vurdere behovet for sikringstiltag såsom alarmsystemer, beskyttelse mod brand og vandskader, UPS, køling eller andre sikringstiltag.
- Der skal være etableret branddøre til store server-rum.
- Passende indbrudsalarmer skal være etableret som minimum til større installationer
- Den Driftsansvarlige skal revidere listen med sikre områder mindst hvert 4. år.

1.1.5.2. Fysisk adgangskontrol

- Der skal være etableret passende adgangskontroller til store server-rum, således at kun autoriserede personer kan få adgang.
- Den driftsansvarlige skal sikre at der sker logning af hvem der har været inde i store server-rum og hvornår de har været inde.
- Den Driftsansvarlige skal sikre at alle eksterne personer med adgang til store server-rum er registreret og der skal ske en periodisk revurdering af om der fortsat er behov for at disse eksterne personer har adgang.

1.1.5.3. Beskyttelse mod eksterne trusler

- Brandfarligt materiale skal placeres i forsvarlig afstand fra sikre områder.

- Sikkerhedskopier og andre typer af arkiver skal være beskyttet mod eksterne trusler såsom brand og oversvømmelser.
- Der skal være etableret klimaanlæg og løbende overvågning af serverrum i forhold til temperatur og fugt.
- Der skal være etableret brandslukningsmekanismer i serverrum.
- Der skal foreligge opdaterede servicerapporter, hvor sikringsmekanismerne er blevet testet og godkendt af eksterne parter.

1.1.5.4. Arbejde i sikrede områder – større serverrum

- Den driftsansvarlige fastsætter retningslinjer for arbejde i større serverrum.

1.1.6. Kontrollerede områder

- I visse mindre sikre områder - som offentligheden dog ikke normalt skal have adgang til - er der kun begrænsede krav IT-sikkerheden, disse områder betegnes "kontrollerede områder"
- Den driftsansvarlige eller den lokale ledelse træffer beslutning om, hvilke områder, som offentligheden ikke normalt skal have adgang til, og som dermed skal anses som kontrollerede områder.
- Den driftsansvarlige eller den lokale ledelse kan - i samarbejde med IT-sikkerhedsfunktionen - fastsætte retningslinjer for sikkerheden på sådanne kontrollerede områder.
- For kontrollerede områder bør der være etableret passende fysisk adgangskontrol (f.eks. aflåsning).

1.1.6.1. Overvågning af områder til af- og pålæsning

- Adgang til og fra af- og pålæsningsområdet i Koncernservice skal være sikret på passende vis med fysiske og logiske adgangskontroller.
- Ved fysisk transport af ind- og uddata skal der afhængigt af oplysningernes karakter, anvendes en betryggende transportform. Vurderingen heraf skal foretages af systemejeren for det system, som ind- og uddataene hidrører fra og efter inddragelse af IT-sikkerhedsfunktionen.

1.1.7. Områder med borgeradgange og ubemandede områder

- Den lokale ledelse i de enkelte forvaltninger er ansvarlig for at sikre områderne på passende vis
- Den lokale ledelse i forvaltningen er ansvarlig for at sikre at eventuel tv-overvågning overholder de gældende krav omkring persondatabeskyttelse, IT-sikkerhedsfunktionen skal konsulteres ved oprettelse af ny tv-overvågning på offentligt tilgængelige steder, se også afsnit 2.5.10.2 Tv-overvågning

1.1.8. Beskyttelse af udstyr

- IT-udstyr skal være placeres så skader og uautoriseret adgang minimeres.
- Væsentligt IT-udstyr skal beskyttes mod tyveri.
- IT-sikkerhedsfunktionen kan stille krav om tv-overvågning af særligt kritisk iT-udstyr eller udstyr af høj værdi.

- IT-systemer og infrastruktur skal være beskyttet mod lyn og overspændinger.
- IT-udstyr, der benyttes til behandling af personoplysninger eller værdioplysninger, skal placeres på en sådan måde, at det er beskyttet mod adgang fra uvedkommende.
- Printere, der benyttes til udskrivning af personoplysninger eller værdioplysninger, skal placeres i kontrollerede områder, hvortil der ikke er offentlig adgang, eller det skal sikres, at det kun er muligt at udskrive dokumenter ved medarbejderens tilstedeværelse.
- Den Driftsansvarlige i henholdsvis Koncernservice, Børne- og Ungdomsforvaltningen og Brandvæsenet skal fastsætte regler for, hvilket IT-udstyr, der skal tyverisikres gennem mærkning.

1.1.8.1. Forsyningssikkerhed

- Ved større forretningskritiske serverrum m.m. skal der være etableret nødstrømsanlæg til korttidsbrug og kontrollerede nedlukninger.
- På disse lokationer skal der være etableret plan for brugen af nødstrømsanlæg og det skal periodisk afprøves og kontrolleres.
- Der skal være etableret alternative kommunikationsforbindelser til kritiske forretningssystemer.

1.1.8.2. Sikring af kabler og udstyr

- Den Driftsansvarlige i henholdsvis Koncernservice, Børne- og Ungdomsforvaltningen og Brandvæsenet skal sørge for beskyttelse af kabler til datakommunikation mod uautoriserede indgreb og skader. Faste kabler og udstyr bør mærkes klart og entydigt.
- Den Driftsansvarlige skal sikre at der findes overordnet dokumentation for kabelføring og at den bliver opdateret, når den faste kabelføring ændres.
- Den driftsansvarlige skal periodisk kontrollere netværket for uautoriseret it-udstyr og om nødvendigt kontakte den ansvarlige.

1.1.8.3. Fjernelse af virksomhedens informationsaktiver og sikker bortskaffelse

- Bortskaffelse af IT-udstyr, som indeholder personoplysninger eller værdioplysninger skal i det omfang det er muligt ske ved destruktion.
- Ved salg, genbrug eller bortskaffelse af IT-udstyr herunder pc'er og eksterne harddiske skal alle data lagrede på udstyret slettes på en sådan måde, at data ikke kan gendannes.
- Koncernservice kan dispensere herfra. Ansvaret for sletning og bortskaffelse påhviler den driftsansvarlige i Koncernservice.

1.6 STYRING AF KOMMUNIKATION OG DRIFT

1.1.9. Driftsafviklingsprocedurer

1.1.9.1. Driftsafviklingsprocedurer

- Der skal sikres at driftsprocedurer for infrastruktur og forretningssystemer løbende bliver ajourførte og er tilgængelig for driftspersonale.

- Driftsprocedurer skal omfatte beskrivelse af eventuel integration og driftsmæssige bindinger til andre systemer.
- Driftsprocedurer skal indeholde procedurer for fejlhåndtering og systemdokumentation der beskriver ind/uddata.
- Driftsprocedurer skal omfatte beskrivelser af reetableringsproces
- Driftsprocedurer skal beskrive muligheder og opsætning af kontrolspor og øvrig systemteknisk logning.

1.1.9.2. Ændringsstyring

Det skal sikres at ændringer ikke forringer indbyggede integritetskontroller.

- Alle påvirkede systemer, databaser og udstyr skal identificeres i forbindelse med ændringer.
- Ændringer skal være formelt godkendte på møder i Change Advisory Board inden implementering.
- Systemejer for større systemer er – i samarbejde med den driftsansvarlige - ansvarlige for at vurdere behovet for tekniske test og brugerinvolvering inden implementering.
- Ved større ændringer til IT-systemer, skal interne kontroller testes for at sikre, at disse ikke forringes ved implementeringen.
- Test skal være med til at afdække utilsigtede afledte virkninger på Københavns Kommunes daglige drift og sikkerhed.
- Mulige konsekvenser af ændringer skal vurderes
- Der skal tages stilling til behovet for fallback.
- Der skal sikres et kontrolspor for gennemførte ændringer på systemerne.

1.1.10. Håndtering af eksterne samarbejdspartnere

- Det skal sikres at eksterne samarbejdspartnere efterlever Københavns Kommunes krav til sikkerhed og stabilitet og tilgængelighed.
- Kontrakter og SLA'er (Service level-agreement) med eksterne samarbejdspartnere bør indeholde beskrivelser af logiske og fysiske sikkerhedstiltag.
- Kommunen skal kunne gennemføre audit eller kontrol med outsourcede aktiviteter såsom logning af adgang og ændringer til systemer.
- Ansvar for identifikation af sikkerhedshændelser og IT-beredskab skal være defineret i kontraktuelle aftaler med eksterne samarbejdspartnere.
    - Det skal sikres at eksterne samarbejdspartnere som minimum efterlever Københavns kommunes regler for ændringsstyring omfattende: teknologiske, hardwaremæssige, organisatoriske og IT-systemmæssige ændringer.

1.1.11. Kapacitetsstyring

- IT-infrastrukturen skal løbende overvåges i forhold til ressourceforbrug.
- Der skal være defineret tærskelværdier med alarmering hvis disse overskrides ved fejl på f.eks. CPU, disk, eller ved andre lign. performanceproblemer.

- Der skal løbende tages stilling til behovet for kapacitetsændringer såsom indkøb af nyt hardware, mm.
- Krav til kapacitetsstyring skal tage udgangspunkt i forretningens krav til svartider og tilgængelighed.

1.1.12. Skadevoldende programmer og ondsindet kode

1.1.12.1. Scope

- Alle servere, arbejdsstationer, bærbare pc'er og andet mobilt IT-udstyr, netværksenheder og andre relevante enheder, skal være beskyttet mod ondsindet kode, såsom virus, malware, mm.
- Netværksindgange og e-mail trafik til og fra kommunen skal være beskyttet mod ondsindet kode.
- Det skal være muligt at blokere ondsindede websider eller e-mails, således at disse ikke kan tilgås.

1.1.12.2. Hvad skal scannes

IT-sikkerhedsfunktionen kan fastsætte retningslinjer for hvilke typer af data, der skal scannes. Det omfatter som minimum følgende:

- Kritiske system filer
- Master boot records
- Specifikke filer såsom pdf'er, eksekverbare filer, makroer, scripts, ondsindede links i e-mails, mm.
- Indgående/udgående netværkstrafik
- Alle vedhæftede filer i e-mail systemer skal scannes inden de åbnes.
- Mobile medier såsom USB enheder, eksterne drev og CD/Dvd'er.
- Java applets og browser-relaterede trusler.

1.1.12.3. Review

- Der skal gennemføres periodisk review af antivirus/malware løsninger for at sikre, at alle enheder er aktive og beskyttet med seneste signaturer.
- Et periodisk review i form af stikprøve eller scanninger af systemer skal gennemføres og resultatet dokumenteres.
- Håndtering af kritiske observationer der ikke automatisk kan håndteres af antivirus/malware løsningen skal dokumenteres med handlingsplan.
- Automatisk karantæne skal være aktiveret med henblik på efterfølgende undersøgelser.

1.1.13. Backup

Kommunen tager backup af alle væsentlige informationsaktiver i henhold til de forretnings- og driftsmæssige krav hos Københavns Kommune.

- Der skal udarbejdes en overordnet strategi for backup i KK og strategien har til formål at sikre, at der til enhver tid kan gennemføres gendannelse af systemer og data, samt at backup tilbydes som en standardiseret ydelse over for kommunens systemejere.

- Krav til backupkonfigurationer for alle systemer og data, skal være dokumenteret i backupplaner omfattende hyppighed og på hvilke medier de bliver arkiveret.
- Backupplaner skal tage udgangspunkt i de forretningsmæssige krav til tilgængelighed og acceptabel periode for datatab.
- IT-systemer (kilden) og backupmedier (kopien) skal være fysisk adskilte, og placeringen af backupmedier skal være beskyttet med passende fysiske og logiske adgangskontroller.
- Arkiverede backupmedier hos Københavns Kommune, skal placeres i data- og brandsikret rum, skabe eller bokse.
- Fjernarkivering af backupmedier som f.eks. langtidslagring skal ske i en anden fysisk enhed hos kommunen eller hos autoriserede samarbejdspartnere og der skal signes af på udlevering/aflevering af backupmedier til fjernarkivering.
- Fjernarkiverede backupmedier skal være beskyttet med passende fysiske og logiske adgangskontroller.
- Backup skal minimum testes en gang årligt med henblik på at validere integriteten af backupmedierne og at systemer og data kan genskabes inden for de aftale tidsrammer.
- Ændringer til backupkonfigurationer eller backupløsninger skal formelt godkendes og dokumenteres.
- I forbindelse med større idriftsættelser eller andre betydende ændringer, skal der gennemføres backup af systemopsætninger.
- Automatiserede backupjobs som f.eks. kørsler og batchjobs skal løbende overvåges for identifikation af fejlede kørsler.
- Systemejerne for kritiske systemer skal sikre, at der kan gennemføres en restoretest hos enten KS serverdrift eller hos ekstern leverandør, hvis systemet driftes eksternt.

1.1.14. Netværkssikkerhed

- Der skal forefindes beskrevne procedurer for logisk adgang til kritisk netværksudstyr som f.eks. switche, routere og firewalls.
- Administration der ikke foretages fra Københavns Kommunes netværk, skal ske med en sikker og krypteret forbindelse med automatisk timeout funktion efter inaktiv periode.
- Netværksinfrastrukturen skal designes med henblik på at minimere sikkerhedsrisici f.eks. segregering/VLAN, DMZ zoner, mm.
- Der skal tages backup af kritiske netværksudstyr i forbindelse med opdateringer og som minimum hver 4. uge.
- Installation og konfiguration af nyt netværksudstyr skal omfatte konfiguration af basale sikkerhedsparametre.
- Kritisk netværksudstyr skal løbende overvåges for driftsmæssige problemer eller for sikkerhedshændelser såsom DDOS, port scanninger eller uautoriserede adgangsforsøg.

1.1.14.1. Netværkstjenester og opkobling af netværksudstyr

- Netværket skal periodisk scannes efter uautoriserede netværkstjenester omfattende usikre protokoller og software tjenester, såsom torrent klienter, Eksterne fildelingstjenester, FTP, telnet, uautoriserede webservere, mm.
- Tilføjelser eller undtagelser til regler for al netværkstrafik på Københavns Kommunes interne netværk, skal godkendes i form af en change request.
- Administration af netværksenheder må kun foretages fra specifikke IP adresser eller ske via en sikker forbindelse som er krypteret f.eks. SSL, https eller lign.
- Netværksudstyr, samt overvågning af disse, skal konfigureres efter definerede standarder der omfatter brugen af best practices for sikkerhedskonfigurationer. F.eks. deaktivering af services, porte, konsoladgange, ukrypterede forbindelser, mm.
- Al adgang til det administrative netværk skal valideres med AD oprettet netværksbrugernavn og password.
- Alt netværksudstyr med borgeradgange skal afvikles på et publikumsnetværk som er fysisk og logisk adskilt fra det administrative netværk. Det er dog muligt at få adgang til det administrative netværk, hvis der benyttes netværk hvor sikkerhedsforanstaltningerne skriftligt er godkendt af den driftsansvarlige.

1.1.14.2. Trådløse netværk

- Alle eksterne der får adgang til Københavns Kommunes publikumsnetværk eller gæstenetværk skal præsenteres for en startside med krav om accept af vilkår for brug.

1.1.15. Håndtering af databærende medier

- Bortskaffelse af USB-nøgler, cd'er, dvd'er, hukommelseskort og lign. kan kun ske ved destruktion efter en af den driftsansvarlige godkendt procedure.
- Systemdokumentation såsom vejledninger, topologitegninger, konfigurationsdokumenter og anden systemdokumentation skal beskyttes og må ikke placeres på ikke beskyttede eksterne databærende medier.

1.1.16. Informationsudveksling

- Der skal være etableret sikringsforanstaltninger til opdagelse af og beskyttelse mod misbrug, fejlforsendelser og manipulation af data.
- Der må ikke efterlades printet personfølsomme oplysninger eller værdioplysninger på offentlige områder såsom åbne kontorlandskaber eller i printerrum.
- Det skal sikres at personfølsomme oplysninger eller værdioplysninger ved Transport bliver sikret på passende vis. F.eks. beskyttet emballage, aflåste bokse eller ved kryptering af indhold.

1.1.17. Elektronisk handel og betaling

- Den systemansvarlige for systemer der hvori der indgår elektronisk handel eller elektronisk betaling er ansvarlig for at sikre at den elektroniske handel/elektroniske betaling foregår i overensstemmelse med best practice.

1.1.18. Logning og overvågning

Generelle regler

Omfang af logning på brugeraktiviteter skal være baseret på en risikovurdering, således at der kun logges for relevante og nødvendige hændelser. Logning omfatter systemer og brugeradgange i forhold til lovgivningen beskrevet i Bekendtgørelse om IT-sikkerhed nr. 528 kapitel 3 § 15 og Københavns kommunes kasse og regnskabsregulativ.

Hvis et system ikke behandler personfølsomme oplysninger eller værdioplysninger, kan kravet om logning fraviges.

1.6.1.1 Brugerlogning

- IT-systemer hvor personoplysninger behandles, skal omfattes af logning, med mindre de er undtaget fra logning i Justitsministeriets Bekendtgørelse om IT-sikkerhed nr. 528 § 19. Logdata skal f.eks. indeholde dato for systemanvendelse og specificering af systemer, log-on og log-off.
- Fejlede og succesfulde adgangsforsøg
- Logning af brugen af udvidede rettigheder på kritiske systemer
- Logning af data indeholdende personfølsomme oplysninger skal opbevares i 6 måneder, hvorefter logdata skal slettes. Undtagelser hvor logdata skal opbevares i op til 5 år, skal være dokumenteret.
- IT-systemer, hvor data der er omfattet af Københavns kommunes kasse og regnskabsregulativ opbevares, skal logge i henhold til denne.

1.6.1.2 Systemlogning

- Installation og brugen af systemværktøjer på kritiske systemer
- Brugen af kritiske transaktionstyper, herunder læsning og ændring af data.
- Konfigurationsændringer
- Benyttede netværksprotokoller
- Aktivering/deaktivering af systemkontroller såsom antivirus, firewall og andre logiske sikringskontroller.

1.6.1.3 *Opfølgning på logning*

- Der skal løbende følges op på logdata med henblik på at identificere uhensigtsmæssigheder f.eks. overskridelser af tærskelværdier, forsøg på uretmæssig adgang til kritiske data, uventede ændringer 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.

1.6.1.4 Fejllogs

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

1.6.1.5 Administratorlogs

- Hvis et system indeholder personfølsomme data eller værdi data skal aktiviteter udført af systemadministratorer og andre med særlige rettigheder logges. Hvor det er teknisk muligt skal der være etableret funktionsadskillelse, således at systemadministratorer ikke selv kan ændre loginformationer.

1.6.1.6 Beskyttelse af logdata

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

1.1.18.1. IT-sikkerhedsrapporter

Kommunen gennemfører periodiske udtræk fra systemer for f.eks. at kontrollere adgange til data og systemer.

- Anmodninger om udtræk i form af IT-sikkerhedsrapporter, skal godkendes af it-sikkerhedsfunktionen.
- IT-sikkerhedsrapporter skal udarbejdes enten i forbindelse med de generelle kontroller af medarbejderes adgange eller ved begrundet mistanke om misbrug, mm.
- Udtrækkene skal altid opbevares på sikker vis, således at uvedkommende ikke kan få adgang til oplysningerne.
- Udtrækkene skal destrueres så snart forholdet er endeligt afklaret og der ikke længere er behov for at arkivere disse.

1.1.18.2. Tv-overvågning

Tv-overvågning må som udgangspunkt alene iværksættes i kriminalitetsforebyggende øjemed. Offentlige myndigheders adgang til at iværksætte tv-overvågning er først og fremmest reguleret af persondatalovens regler samt i lov om Tv-overvågning. Efter § 2a i lov om Tv-overvågning kan en kommune med henblik på at fremme trygheden foretage tv-overvågning af offentlig gade, vej, plads eller lignende område, som benyttes til almindelig færdsel, og som ligger i nær tilknytning til et område, der allerede tv-overvåges. I praksis betyder "nær tilknytning" inden for en radius af 500 m. fra allerede etableret Tv-overvågning, som ikke behøver at være iværksat af kommunen. Politidirektøren i København skal høres, inden Tv-overvågningen iværksættes. De relevante regler i persondataloven er navnlig de grundlæggende principper om god databehandlingsskik, saglighed og proportionalitet i § 5 og de enkelte regler for behandling af personoplysninger i §§ 6-8.

- Ved Tv-overvågning af steder eller lokaler, hvor der er almindelig adgang, eller af arbejdspladser, skal der oplyses om overvågningen ved skiltning eller anden tydelig information.
- Alle ansatte på stedet skal oplyses om formålet med Tv-overvågningen og om, i hvilke tilfælde optagelserne vil blive gennemgået og videregivet til politiet.
- Billedoptagelser fra Tv-overvågning i kriminalitetsforebyggende øjemed skal slettes senest 30 dage efter, at de er optaget med mindre de indgår i en verserende politisag.
- Der skal træffes de nødvendige fysiske og tekniske foranstaltninger imod, at billedoptagelser fra et overvågningskamera kommer til uvedkommendes kendskab eller misbruges.
- Billedoptagelser fra Tv-overvågning i kriminalitetsforebyggende øjemed må kun videregives, hvis personen på optagelsen har givet sit udtrykkelige samtykke eller videregivelse sker til politiet i kriminalitetsopklarende øjemed.

1.7 ADGANGSSTYRING, BRUGERRETTEDE POLITIKKER MED MERE

1.1.19. Forretningsmæssige krav og ansvar

- Al adgang til kommunens IT-systemer, servere, netværk og pc'er, der indeholder person- eller værdioplysninger, skal være betinget af konkrete autorisationer.
- Nærmeste leder har ansvaret for tildelte autorisationer til medarbejderne.
- Systemejer meddeler Koncernservice (Brugeradministrationen og IT-sikkerhedsfunktionen) de nærmere retningslinjer for adgangsstyring til hvert enkelt IT-system.
- Retningslinjerne skal blandt andet beskrive, hvilke medarbejdergrupper der skal have adgang til IT-systemet, samt hvilke oplysninger og funktioner den enkelte medarbejder kan få adgang til, og kan endvidere indeholde en beskrivelse af eventuel mulighed for anvendelse af rolleprofiler.
- Rolleprofiler skal oprettes og vedligeholdes af systemejer i samarbejde med Brugeradministrationen i Koncernservice

1.1.20. Administration af brugeradgange

- Oprettelse og vedligeholdelse af medarbejdere i kommunens IT-systemer bliver gennemført af brugeradministrationen i Koncernservice.
- Medarbejdere i Brandvæsenet oprettes og vedligeholdes som udgangspunkt af Brugeradministrationen i Koncernservice, Brandvæsenet sikre efterfølgende selv relevante autorisationer til egne systemer efter egen forretningsgang. Koncernservice er ansvarlig for at der foreligger ajourførte procedurer for adgangsstyring og brugeradgang omfattende oprettelser, ændringer og sletning af interne og eksterne brugere. Den autorisationsansvarlige har ansvaret for, at der bestilles de rettigheder, som medarbejderne har behov for arbejdsmæssigt.

- Eksterne samarbejdspartnere, som har brug for adgang til et IT-system af hensyn til drifts-, udviklings- og vedligeholdelsesopgaver, skal autoriseres hertil.
- Autorisation af eksterne samarbejdspartnere må kun finde sted, såfremt en entydig identifikation af den pågældende medarbejder kan finde sted. Dette skal som udgangspunkt ske i form af cpr-nummer.
- Autorisation skal ske på baggrund af en anmodning fra en autorisationsansvarlig i samarbejde med den ansvarlige for aftaleindgåelsen, der sørger for at indhente de fornødne oplysninger i forbindelse med bestillingen.
- Slutbrugeren får som udgangspunkt ikke lokaladministratorrettigheder på arbejdspc'er.

1.1.20.1. Brugeroprettelser

- Hver medarbejder skal ved oprettelse tildeles et unikt brugernavn.
- Brugernavnet er personligt og må ikke overdrages til andre.
- De enkelte brugernavne skal genereres i kommunens IT-sikkerhedssystem.
- Ved oprettelse eller nulstilling af adgangskode skal medarbejderen tildeles en midlertidig adgangskode, som skal ændres ved første anvendelse.
- Udlevering af den midlertidige adgangskode skal ske på en sikker måde.
- Midlertidige adgangskoder skal opfylde de gældende krav til adgangskoder.
- Koncernservice er ansvarlig for at ajourføre procedurer for, hvordan en brugers identitet fastslås, før en ny adgangskode må udleveres, og for hvorledes udleveringen skal ske.
- Såfremt der skal foretages udlevering af adgangskoder over Internettet eller andre åbne netværk, skal denne udlevering sikres vha. kryptering.
- Standardadgangskoder fra systemleverandører skal ændres i forbindelse med installation af nye IT-systemer.
- Indtastning af adgangskode kan erstattes af brug af id-kort eller lignende autentifikationsmekanisme med et tilsvarende eller højere sikkerhedsniveau.

1.7.1.1 Periodisk review

- IT-sikkerhedsfunktionen sikrer at der foretages stikprøvekontrol af de tildelte autorisationer.
- IT-sikkerhedsfunktionen skal især sikre, at der sker kontrol af de medarbejdere, der har adgang til værdioplysninger eller fortrolige personoplysninger.

1.7.1.2 Ændring af brugerrettigheder

- Ved omplacering skal den nye leder sikre, at medarbejderen kun har de autorisationer, der er et arbejdsmæssigt behov for, og eventuelle ændringer af rettighederne bestilles hos brugeradministrationen.

1.7.1.3 Nedlæggelse af brugerrettigheder

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

1.7.1.4 Udvidede rettigheder

- Udvidede rettigheder til forretningssystemer og IT-systemer, skal være dokumenteret.
- Brugen af udvidede rettigheder til administration af brugeradgange skal registreres i form af logning.

1.7.1.5 Adgangskoder generelt (mobilt udstyr se dog afsnit 2.6.3.10)

- Adgangskoder skal indeholde mindst 8 tegn
- Adgangskoder til systemadministrator profiler skal så vidt muligt indeholde mindst 12 tegn
- Adgangskoder skal indeholde kombinationer fra følgende tre kategorier; store bogstaver, små bogstaver og tal.
- Der må ikke benyttes brugernavn, eget navn eller datoer som en del af adgangskoden,
- Adgangskoder skal skiftes efter højst 90 dage
- Adgang til systemer skal blokeres senest efter 5 mislykkedes login forsøg og håndhæves i mindst 30 min.
- Alle arbejdsstationer skal have en skærmlås, der aktiveres automatisk efter højest 15 minutters inaktivitet med krav om indtastning af password.
- Adgangskoder til administratoradgang skal opbevares i en forseglet kuvert i et aflåst pengeskab.
- IT-sikkerhedsfunktionen kan tillade at passwords bliver gemt i single sign on løsninger. Muligheden for at gemme passwords i browsere eller andre applikationer skal deaktiveres.

1.1.21. Brugerrettede politikker

1.1.21.1. Adgangskoder

- Adgangskoder er personlige og strengt fortrolige og må ikke udlånes til andre.
- Såfremt adgangskoden kompromitteres, eller der opstår mistanke herom, er det medarbejderens ansvar straks at ændre kodeordet og underrette IT-sikkerhedsfunktionen.
- Hvis flere medarbejdere benytter den samme arbejdsstation, skal den enkelte medarbejder logge på med egen adgangskode, før der udføres arbejdsopgaver, og logge af, inden den næste medarbejder overtager arbejdspladsen.
- Når en medarbejder forlader en tændt arbejdsstation, skal den adgangskodebeskyttede skærmlås aktiveres.

1.1.21.2. Københavns Kommunes rettigheder

- Af hensyn til Københavns Kommunes drifts- og sikkerhedsmæssige forhold kan alt, hvad der sker på kommunens IT-systemer, løbende blive registreret/logget.
- Registreringen giver ikke ledere m.v. en adgang til at tilgå oplysninger om medarbejdernes brug af internet m.v.
- Eventuel gennemgang af en medarbejders e-mails må kun ske, hvis det er nødvendigt for, at Københavns Kommune kan forfølge berettigede interesser, og hensynet til den ansatte ikke

overstiger disse interesser. De berettigede interesser kan f.eks. være hensynet til drift, sikkerhed, genetablering og dokumentation samt hensynet til kontrol af medarbejderes brug.

- Medarbejderne skal på forhånd - på en klar og utvetydig måde - være informeret om eventuel gennemgang af den enkelte medarbejders e-mails.
- Ved en gennemgang af en medarbejders e-mails må arbejdsgiveren ikke læse medarbejderens private e-mails.

1.1.21.3. Accepteret brug af e-mail

- Medarbejdere skal anvende e-mailsystemer til arbejdsmæssige forhold og i det omfang det ikke generer den arbejdsrelaterede anvendelse, må e-mailsystemet godt anvendes til private formål.
- Kommunens IT-sikkerhedspolitik skal overholdes ved brug af kommunens e-mailsystemer.
- E-mails der indeholder fortrolige, personfølsomme skal altid krypteres, hvis de sendes udenfor Københavns Kommunes netværk. Dette skal ske som ”sikker e-mail”.
- Såfremt modtageren ikke kan modtage sikker e-mail, kan der ikke anvendes e-mails til korrespondancer, der indeholder værdioplysninger, fortrolige personoplysninger eller andre beskyttelsesværdige personoplysninger som f.eks. cpr-nr.
- Hvis en medarbejder markerer private e-mails med teksten ”privat” i emnefeltet og gemmer e-mails i en folder navngivet med ”privat” er kommunens ansatte forpligtiget til i videst muligt omfang ikke at gøre sig bekendt med indholdet.
- Det er ikke tilladt automatisk at videresende medarbejderens e-mail til en privat eller ekstern e-mailadresse.

1.1.21.4. Afsendelse af sikker e-mail

- Kommunen skal afsende digital post via "Doc2mail", her kan medarbejderen let se, om modtageren har en digital postkasse. Hvis det ikke er tilfældet sender systemet automatisk et fysisk brev.
- Hvis kommunen skal sende en sikker e-mail til en modtager, er det en forudsætning, at postsystemet ’kender’ modtagerens certifikat.
- Har en enhed i kommunen modtaget en sikker e-post fra modtageren, vil kravet om kendskab til modtagers certifikat være opfyldt, idet certifikatet automatisk bliver gemt i systemet
- Hvis postsystemet ikke ”kender” modtagerens certifikat, skal dette fremskaffes, førend der kan afsendes sikker post.

1.1.21.5. Intern e-mailkorrespondance

- Det kræver ikke kryptering at sende mails inden for Københavns Kommunes interne netværk.
- En intern mailbruger kan identificeres ved, at e-mailadressen ender med ”kk.dk”.

1.1.21.6. Accepteret brug af internet

- Privat brug af internettet må finde sted i det omfang, det er foreneligt med medarbejderens varetagelse af sit daglige arbejde i kommunen og i øvrigt ikke strider mod lovgivningen, Københavns kommunens IT-politik og kommunens værdigrundlag.

- Medarbejdere må ikke anvende kommunens IT-udstyr til bevidst at opsøge anstødelige eller ulovlige hjemmesider, som f.eks. racistiske eller børnepornografiske hjemmesider.
- Det er kun tilladt arbejdsmæssigt at bruge sociale netværkstjenester som er godkendt af Koncernservice.
- Der må ikke via de godkendte sociale netværkstjenester udveksles fortrolige oplysninger, herunder person- og værdioplysninger vedrørende kommunens forhold eller sager.
- *Særligt om en kommunal afdelings oprettelse af profiler på Facebook eller andre sociale netværkstjenester:*
- Det anbefales at afdelingerne undgår at offentliggøre medarbejdernes personoplysninger på Facebook eller andre sociale netværkstjenester ellers skal der foreligge skriftligt samtykke fra medarbejderen.
- Afdelinger, der vælger at lægge personoplysninger vedrørende medarbejdere ud på Facebook eller andre sociale medier, bliver dataansvarlig for de oplysninger, som de vælger at lægge ind på deres profil og skal følge persondatalovens regler.

1.1.21.7. Accepteret brug af programmer og tjenester

- Det er ikke tilladt at installere eller benytte ikke godkendte programmer eller tjenester.

1.1.21.8. Accepteret brug af trådløse netværk

- Det er som udgangspunkt kun tilladt at koble netværksudstyr indkøbt via Koncernservice på det administrative netværk.
- Medarbejdere der tilgår fremmede trådløse netværk f.eks. i lufthavne, toge og hoteller, skal anvende IT-sikkerhedsløsninger som er godkendt af den driftsansvarlige.

1.1.21.9. Accepteret brug af mobilt IT-udstyr

Dette afsnit omfatter ikke bærbare Pc'er.

- Håndholdt udstyr, som er stillet til rådighed af kommunen, må ikke anvendes af andre end den medarbejder, hvortil udstyret er udleveret.
- Mobiltelefoner og andre håndholdte enheder skal kunne stilles til rådighed for kommunens teknikere i forbindelse med support og vedligehold.
- Den driftsansvarlige skal fastsætte retningslinjer for om medarbejderne selv må installere programmer eller acceptere licensvilkår for applikationer.
- Den driftsansvarlige skal fastsætte retningslinjer for anvendelsen af krypteringsmekanismer.
- Den driftsansvarlige skal fastsætte retningslinjer for som beskriver om Kommunens håndholdte udstyr må forbindes direkte til IT-systemer, der ikke ejes eller administreres af Københavns Kommune.
- Personfølsomme oplysninger eller værdioplysninger må som udgangspunkt ikke lagres på mobiltelefoner og andre håndholdte enheder.

- Håndholdt udstyr skal opbevares på forsvarlig og sikker vis og til enhver tid under medarbejderens kontrol.
- Ved bortkomst af håndholdt udstyr, skal medarbejderen melde en sådan bortkomst til Koncernservice.

1.1.21.10. Sikkerhedskrav for brug af mobilt IT-udstyr

- Mobilt IT-udstyr omfatter smartphones, tablets og PDA'er med synkronisering til Exchange eller anden dataadgang til Københavns Kommunes IT-systemer, som ansvarsmæssigt er underlagt den driftsansvarlige hos Koncernservice.

1.7.2 Tekniske minimumstiltag

- PIN koder skal som minimum indeholde 4 tegn.
- Enheden skal spærres efter højst 5 forkerte adgangsforsøg.
- Enheden skal være udstyret med adgangskodebeskyttet skærmlås, der automatisk aktiveres efter højst 1 minuts inaktivitet.
- Skærmlåsen tilstræbes at være konfigureret således, at brugeren ikke kan slå funktionen fra, når det er teknisk muligt at sætte systemet op til det.
- Enhederne skal være beskyttet med kryptering, medmindre koncernservice beslutter andet.
- Håndholdt udstyr skal være underlagt en centralt administreret løsning, der sikrer, at enheden kan spærres og data slettes, i tilfælde af at enheden mistes eller stjæles.
- Lagrede adgangskoder til kommunens netværk skal sikres på passende vis. Dette omfatter også certifikater.
- Der skal etableres automatisk timeout funktion på dataforbindelse der er inaktive i en længere periode.

1.1.22. Netværksadgange

Den driftsansvarlige skal udarbejde forretningsgange for:

- Brug af netværkstjenester
- Autentifikationskrav
- Identifikation af netværksudstyr
- Beskyttelse af netværksenheder: logiske porte og fysiske konfigurations porte.
- Opdeling af netværk f.eks. i form af segregering.

1.1.23. Styring af systemadgange

- Kontrol med afviste adgangsforsøg skal etableres ved login til kommunens netværk eller i forbindelse med login til IT-systemer, der behandler værdioplysninger eller fortrolige eller følsomme personoplysninger, således at forgæves forsøg på login automatisk bliver registreret i en log.

- Hvis der konstateres mere end 5 på hinanden følgende forgæves login-forsøg, skal der automatisk blokeres for yderligere forsøg.
- Blokeringen skal rapporteres til den driftsansvarlige
- Blokering for login kan ophæves af Koncernservice.
- Forbindelse til systemer hvor en bruger er logget ind, såsom VPN forbindelser, SSH, telnet, Remote Desktop og lign. skal beskyttes, således at der sker en automatisk afbrydelse, hvis forbindelsen har været inaktiv i mere end 15 min.
- Adgangskoder skal beskyttes.
- Ved brugen af systemværktøjer der kan omgå sikkerhedsmekanismer skal brugen være begrænset og dokumenteret

1.1.24. Fjernarbejdspladser

- 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.
- Personoplysninger eller værdioplysninger må ikke lagres på fjernarbejdspladsens harddisk medmindre dette er godkendt af IT-sikkerhedsfunktionen, og oplysningerne er krypterede.
- 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. databehandleraftale.
- Den driftsansvarlige skal sikre, at antivirusprogrammer og adgangskontrolsystemer er installerede på fjernarbejdspladser tillige med firewall eller anden tilsvarende sikkerhedsforanstaltning.
- Adgang til kommunens netværk må kun ske gennem sikkerhedsgodkendt IT-udstyr. Der kan fra fjernarbejdspladser fås adgang til de samme applikationer, som fra medarbejderens sædvanlige kontorarbejdsplads.
- Enhver adgang til kommunens IT-systemer og administrative netværk foretaget fra udstyr udenfor kommunens ejendom må som udgangspunkt kun foregå ved brug af to-faktor login eller anden tilsvarende sikkerhedsløsning.
- Bærbare computere må kun opkobles til kommunens administrative net via en sikret forbindelse f.eks. VPN eller VDI løsning.

1.8 ANSKAFFELSE, UDVIKLING OG VEDLIGEHOLDELSE AF INFORMATIONSSYSTEMER

Omfatter sikkerhedskrav i forbindelse med anskaffelse og udvikling af alle former for IT-systemer og programmel, som indeholder, udstiller eller behandler personfølsomme oplysninger og værdioplysninger. Sikkerhedskravene gælder både for systemer, der driftes af kommunen og af eksterne samarbejdspartnere. De overordnede krav og systemejerens generelle ansvarsområde er defineret i Regulativ for IT-sikkerhed i Københavns Kommune.

1.1.25. Sikkerhed i forhold til indkøb og nyudvikling af større systemer

Omfatter krav til sikkerhedsanalyse af systemer og programmel i forbindelse med udvikling.

- Sikkerhedsløsningen omkring anskaffede eller nyudviklede iT-systemer, skal godkendes af it-sikkerhedsfunktionen.
- Systemejeren er ansvarlig for at der sker dokumentation af iT-systemets funktionalitet, opbygning, anvendelse og sikkerhedsløsning omfattende nødvendige foranstaltninger til beskyttelse af iT-systemet
- Systemejeren er ansvarlig for at sikre at der foretages test inden migrering fra udvikling til produktion, for at sikre ønsket driftsniveau, iT-sikkerhedsniveau og brugbarhed.
- Systemejeren skal godkende afleveringstest fra leverandøren
- Logningsmuligheder i iT-systemet skal være dokumenteret
- Muligheden for styring af administratoradgange skal være dokumenteret. Herunder eventuelle skærpede krav til administratoradgangskoder.
- Krav til IT-kontroller og sikkerhedsrapporter, skal være dokumenteret og disse skal som minimum leve op til det niveau som IT-sikkerhedsfunktionen fastsætter under hensyntagen til krav fra den eksterne revision.
- Der bør være en enkel mulighed for at opfylde registreredes krav på indsigt efter reglerne i persondataloven.

1.1.25.1. Sikker udviklingsmetodik

- Ved udvikling bør sikkerhed tænkes ind i processen.
- Best practice for generelle sikkerhedskrav bør adresseres ved udvikling
- Ved udarbejdelse af kravspecifikation til nye systemer henvises til kommunens vejledning ”IT-sikkerhedskrav – Kravspecifikation Bilag 28”. (Det bør overvejes om der bør være krav til AD integration).

1.1.26. Korrekt informationsbehandling

1.8.1.1 Inddata og uddata

Informationsbehandling omfatter både IT-systemer og netværksudstyr der opbevarer, behandler eller transmitterer information. Informationsbehandling omfatter også fysiske systemer, medier og dokumenter.

- Adgangen til ind- og uddata, der indeholder personoplysninger eller værdioplysninger, skal begrænses til medarbejdere, der har et arbejdsbetinget behov herfor.
- Ind- og uddata skal til enhver tid opbevares således, at de ikke kommer til uvedkommendes kendskab, og som minimum ved aflåsning af lokalet eller enheden, når dette/denne forlades.
- I områder, som anvendes til betjening af borgere, og hvor der er offentlig adgang, skal ind- og uddata, som omfatter fortrolige eller følsomme personoplysninger eller værdioplysninger opbevares aflåst i skabe, skuffer eller lignende, når de ikke benyttes.
- Ind- og uddata skal destrueres på betryggende vis, f.eks. ved makulering, når der ikke længere er et sagligt behov for disse og senest 5 dage herefter.

1.1.27. Kryptografi

- Den driftsansvarlige skal anvise godkendte krypteringsløsninger eller etablere en generel og sikker krypteringsløsning og udarbejde et nøglehåndteringssystem, som understøtter anvendelsen af kryptografi
- IT-sikkerhedsfunktionen kan stille krav til krypteringsløsningerne.
- Nøgler og certifikater skal håndteres og beskyttes på passende vis.

1.1.28. Styring af systemfiler og programkildekode i større driftsmiljøer

1.1.28.1. Installation af systemer i driftsmiljø

- Der skal foretages test inden større opdateringer rulles ud i driftsmiljøet
- Der skal tages stilling til behovet for brugerinvolvering i testforløb
- Muligheden for tilbagerulning til tidligere versioner skal være dokumenteret.
- Alle opdateringer til driftsmiljøet skal være logget
- Hvis testdata indeholder personfølsomme oplysninger eller værdioplysninger, skal adgangen til testdata beskyttes.
- Overførsel af produktionsdata til testmiljø skal godkendes og dokumenteres.

1.1.28.2. Sikring af testdata

- Der skal være etableret separate testmiljøer for kritiske systemer
- Der skal tages stilling til behovet for anonymisering af testdata, hvis det indeholder personfølsomme data eller værdioplysninger.
- Der skal foretages en formel godkendelse af adgange til testmiljøer.

1.1.28.3. Styring af adgang til kildekode

- Kildekode til egenudviklede IT-systemer og IT-systemer, der er helt særlige for Kommunen, som ikke er standardsystemer, skal som udgangspunkt altid opbevares hos kommunen eller i et deponeringsinstitut.
- Kildekode må ikke opbevares i driftsmiljøet og fysisk/logisk adgang skal begrænses, kontrolleres og logges.

- Medarbejderes adgang til kildekode biblioteker skal være dokumenteret.

1.1.29. Sikkerhed i udviklings- og hjælpeprocesser

- Generelt skal al systemudvikling og ændringer foretaget hos kommunen eller af outsourcing partnere, gennemføres med de nødvendige IT-sikkerhedsforanstaltninger for at sikre at systemer ikke bliver ustabile eller der introduceres nye sårbarheder i disse.
- Forretningsgange for installation af systemer i driftsmiljøet skal være dokumenteret.
- Alle opdateringer til driftsmiljøet skal være registreret i logs
- Tidligere versioner af bruger- og styresystemer skal gemmes i tilfælde af behov for genindlæsning af disse.
- Det skal sikres at der er revisionshistorik på ændringer til kildekode og tidligere versioner af kildekode skal gemmes, således at tidligere versioner kan gendannes.

1.1.29.1. Change procedurer

- I Koncernservice skal change procedurerne være iagttaget før udstyr og software sættes i produktion.

1.1.29.2. Teknisk gennemgang af programmer efter ændringer i operativsystemer

- Når operativsystemer ændres bør forretningskritiske programmer gennemses og testes.

1.1.30. Teknisk sårbarhedsstyring

- Den driftsansvarlige skal sikre at nye IT-systemer eller opdateringer bliver sikkerhedstestet inden de bliver idriftsat.
- Den driftsansvarlige skal holde sig informeret om sårbarheder og trusler i forbindelse med de anvendte platforme.
- Den driftsansvarlige skal løbende vurdere behovet for installation af rettelser, opdateringer og Service Packs til IT-systemer.
- Systemejeren skal løbende vurdere behovet for installation af rettelser/opdateringer til it-forretningssystemer.
- Den driftsansvarlige skal tage stilling til behovet for sikkerhedsanalyser af systemer og netværk såsom periodiske scanninger for sårbarheder. Eksempler er:
  - Periodiske sårbarhedsscanninger af infrastruktur
  - Periodiske penetrationstest af infrastruktur for at validere sårbarheder
    - Test af interneteksponerede enheder i infrastrukturen, såsom webapplikationer, såsom SQL injections, XSS, mm.
    - Når sårbarheder bliver opdaget, skal den driftsansvarlige vurdere alvorligheden og relevansen for Københavns Kommune. Passende handlingsplaner skal udarbejdes og prioriteres, samt implementeres hvor nødvendigt.

1.1.30.1. Teknisk sårbarheds management

- Alle patches og sikkerhedsopdateringer til styresystemer, brugersystemer og netværk skal formelt vurderes for relevans, herunder sikkerhedsmæssige implikationer.
- Fravælgelse af patches eller sikkerhedsopdateringer skal begrundes formelt.
- Der skal foretages en formel vurdering af udrulningstidspunkter for at minimerer driftsforstyrrelser.
- Stillingtagen til test i forbindelse med udrulning af patches skal overvejes og dokumenteres ved f.eks. en sårbarhedstest.
- For kritiske systemer bør brugen af testsystemer overvejes
- For kritiske systemer skal behovet for roll-back overvejes.
- Aktuelle patchniveauer for styresystemer, brugersystemer og netværk skal være centralt registreret, således at disse kan holdes op imod fastlagte minimumskrav til patchniveauer.
- Det skal sikres at patches der udføres af eksterne samarbejdspartnere overholder Københavns Kommunes krav til Patch Management.

1.9 STYRING AF IT-SIKKERHEDSHÆNDELSER

- Ved konstatering af brud eller formodning om brud på IT-sikkerhedsbestemmelserne **s**kal IT-sikkerhedsfunktionen underrettes herom. Hvis hændelsen har relation til et bestemt system skal systemejeren også underrettes.
- Medarbejdere der konstaterer IT-sikkerhedshændelser eller har en formodning herom, skal øjeblikkeligt notere alle vigtige detaljer såsom typen af brud, den opståede fejl, beskeder på skærmen og usædvanlige hændelser.
- IT-sikkerhedsfunktionen skal sikre, at der straks iværksættes de foranstaltninger, der er nødvendige for at korrigere de konstaterede fejl eller svagheder.
- IT-sikkerhedsfunktionen kan altid udbede sig en redegørelse fra involverede parter ved større IT-sikkerhedshændelser.
- IT-sikkerhedsfunktionen sikrer, at der sker opsamling og bearbejdning af oplysninger om IT-sikkerhedshændelser.
- IT-sikkerhedsfunktionen orienterer én gang årligt og inden udgangen af 1. kvartal Økonomiudvalget om konstaterede væsentlige IT-sikkerhedshændelser. Der redegøres i den forbindelse for udbedrende tiltag.
- Forvaltningerne holdes løbende orienteret om væsentlige sikkerhedshændelser, og indberetter en gang årligt og inden udgangen af 4. Kvartal fagudvalget og It-sikkerhedsfunktionen om konstaterede IT-sikkerhedshændelser.
- Koncernservice og eksterne samarbejdspartnere skal rapportere til IT-sikkerhedsfunktionen, såfremt der er konstateret hændelser af betydning for IT-sikkerheden og beskrive disse hændelser nærmere.

1.10 Beredskabsstyring

- IT-beredskabsprocessen som kommunen arbejder ud fra, tager afsæt i best practice for IT-beredskab. Business Impact Assessment og risikovurderinger skal sikre, at beredskabet er på et passende niveau. Københavns Kommunes IT-beredskab er del af det overordnede katastrofeberedskab som Brandvæsnet er ansvarlig for.
- Der skal forefindes en overordnet IT-beredskabsplan for Københavns Kommune.
- Koncernservice skal fastlægge de overordnede retningslinjer for udarbejdelse af IT-beredskabsplanerne.
- IT-beredskabsplanerne skal indeholde procedurer for iværksættelse af nødplaner, eskalering, reetablering af IT-systemer og begrænsning af skadevirkninger i tilfælde af større IT-nedbrud. Direktionen henholdsvis Revisionschefen, Borgerrådgiveren og Beredskabschefen har inden for eget område ansvaret for, at der bliver udarbejdet en IT-beredskabsplan som omfatter alle kritiske IT-systemer og processer.
- I tilfælde af større IT-nedbrud skal IT-beredskabsplanen aktiveres efter den fastlagte eskaleringsprocedure.
- Den driftsansvarlige har ansvaret for at indgå aftale om IT-beredskab, herunder den tekniske reetableringsplan med eksterne driftsleverandører og sikre, at disse bliver testet og vedligeholdt.
- Systemejeren for forretningskritiske systemer skal sikre, at der indgås aftale om IT-beredskab for eget IT-system.
- Direktionerne har ansvaret for at vurdere om der eventuelt skal tegnes en forsikring af det anvendte IT-udstyr m.v.
- Beredskabsplanen og ændringer til de sammenhængende IT-beredskabsplaner hos forvaltningsenhederne, skal revurderes mindst hvert 3. år.

1.11 Overensstemmelse med krav og politikker

- Medarbejdere må ikke gemme arbejdsrelaterede personfølsomme data lokalt på sin PC. Alle øvrige arbejdsrelaterede data må kun midlertidigt gemme lokalt, i ønsket om ikke at miste arbejdsrelaterede data.
- Medarbejdere må ikke publicere billeder af personer på nettet/intranettet, uden at de har givet skriftlig accept af dette.
- Medarbejdere der genbruger digitalt materiale så som software, lydfiler og billedfiler fra andres udgivelser, skal sikre sig at de ikke bryder den aktuelle lovgivning omkring ophavsrettigheder.

1.12 Sikkerhed i forbindelse med revision

- IT-revisioner skal altid planlægges med henblik på at minimere drifts– og sikkerhedsmæssige risici.
- IT-sikkerhedsfunktion skal formidle adgange til relevante systemer og data via lederen på det område der skal revideres.
- Al brug af revisionsværktøjer og adgange skal logges.

- Adgangsforhold til revisionen skal periodisk revurderes, med henblik på at deaktivere adgangsforhold efter endt brug og udleverede adgangskort skal inddrages efter endt revision.