Københavns Sundheds- og Omsorgsforvaltning

Sikkerhedsinstruks

2006

Indholdsfortegnelse

Bilags fortegnelse

Sikkerhedsinstruks for Københavns Sundheds- og Omsorgsforvaltning

Kapitel 1

Sikkerhedsinstruksens formål og område:

Denne sikkerhedsinstruks for Sundheds- Omsorgsforvaltningen er udarbejdet af Forvaltningens IT-sikkerhedsleder i henhold til IT-sikkerhedsregulativets § 16, stk. 1 og er godkendt af Borgmesteren for Sundheds- og Omsorgsforvaltningen i henhold til IT-sikkerhedsregulativets § 16, stk. 2.

Formålet med instruksen er at uddybe IT-sikkerhedsregulativets bestemmelser og give en mere detaljeret beskrivelse af IT-sikkerhedsorganisationen og IT-sikkerhedsbestemmelserne i Sundheds- og Omsorgsforvaltningen.

IT-sikkerhedsinstruksen gælder enhver form for databehandling der foretages i Sundheds- og Omsorgsforvaltningen, herunder behandling af personoplysninger der foretages helt eller delvis med brug af IT samt for behandling af personoplysninger, der er eller vil blive indeholdt i et register.

IT-sikkerhedsinstruksen gælder også for selvejende og private institutioner samt andre, der har driftsoverenskomst med Sundheds- og Omsorgsforvaltningen eller som Sundheds- og Omsorgsforvaltningen udfører behandlinger for.

IT-sikkerhedsinstruksen skal kendes af alle medarbejdere i Sundheds- og Omsorgsforvaltningen, der direkte eller indirekte arbejder med databehandling samt ledere herfor, men er ikke offentlig tilgængelig. Sikkerhedsinstruksen ligger på KKnet, desuden gøres medarbejderen bekendt med henvisningen i brev i forbindelse med brugeroprettelsen.

IT-sikkerhedsinstruksen gælder for alle medarbejdere og grupper af medarbejdere, der direkte eller indirekte arbejder med databehandling i Sundheds- og Omsorgsforvaltningen, samt ledere herfor.

IT-sikkerhedsinstruksen skal ses i sammenhæng med relevante sikkerhedsbestemmelser i lovgivningen og Københavns Kommunes og Sundheds- og Omsorgsforvaltningens regler, se bilag 1

Man skal være opmærksom på IT-sikkerhedsforskrifterne, der indeholder regler om sikkerhedsforanstaltninger for Sundheds- og Omsorgsforvaltningens IT-anlæg.

IT-sikkerhedsinstruksen skal gennemgås mindst én gang hvert år med henblik på, at instruksen til stadighed er fyldestgørende og afspejler de faktiske forhold i Sundheds- og Omsorgsforvaltningen.

Bilagene til instruksen revideres løbende efter behov.

IT-sikkerhedsorganisationen i Sundheds- og Omsorgsforvaltningen fremgår af bilag 2 og navne på den udpegede IT-sikkerhedsleder, IT-ansvarlige, systemansvarlige og disses stedfortrædere er vist i bilag 3 og 4.

Kapitel 2

IT - Sikkerhedsorganisation

Dette kapitel indeholder oplysning om IT – Sikkerhedsorganisationen samt de opgaver, rettigheder og pligter som forskellige funktioner giver, herunder den enkelte medarbejder.

Medarbejdere rettigheder og pligter

I forbindelse med tildeling af adgang til IT-systemerne modtager medarbejderen pjecen "PC – vejledning for brugere". Ligesom der i ledsagebrevet gøres opmærksom på, medarbejderens pligt til at vedligeholde data og at behandle oplysninger om borgerne med fortrolighed.

Medarbejderens adgang til IT-systemer og behandling af persondata forudsætter, at der foreligger et tjenstligt behov og at opgaven falder inden for den enkelte medarbejders arbejdsopgaver.

Oplysninger som medarbejderen får kendskab til er omfattet af tavshedspligten, og må kun anvendes i tjenstlig sammenhæng.

Alle opslag i systemerne skal være tjenstligt begrundet og ske i overensstemmelse med systemets formål.

Ingen kan beordres til at foretage opslag som ikke er tjenstligt begrundet.
Et eventuelt samtykke berettiger ikke i sig selv til at foretage opslag på oplysninger.

Det er ikke tilladt for medarbejderen at slå op i systemerne og søge oplysninger om sig selv, ligesom medarbejderen heller ikke må søge oplysninger om familie, venner, kolleger og tilsvarende uden en tjenstlig begrundelse.

Overtrædelse af sikkerhedsbestemmelserne og misbrug af autorisationerne betragtes som tjenstlig forseelse, som følges op med passende sanktioner i forhold til den konstaterede overtrædelse. Sanktionerne kan være lige fra en skriftlig påtale til øjeblikkelig bortvisning.

Medarbejderen får adgang til de enkelte systemer ved en personlig autorisation, med brugerident. (user-id) og kendeord (password), som tildeles af sikkerhedslederen eller stedfortræderen for sikkerhedslederen efter

skriftlig indstilling fra en af de underskrift berettede medarbejdere i enheden. De underskrift berettigede medarbejdere er udpeget af enhedens leder.

Brugerident. (user-id) er entydig i forbindelse med alle autorisationer til databehandling i Sundheds- og Omsorgsforvaltningen.

Autorisationsproceduren beskrives nærmere i afsnittet om autorisationer.

Medarbejderens kendeord (password) er personligt og fortroligt. Det må ikke benyttes eller kendes af andre end medarbejderen selv.

Opstår der mistanke om at kendeord, (password) ikke længere er fortroligt, skal der omgående rettes henvendelse til sikkerhedslederen eller dennes stedfortrædere via den nærmeste leder, og kendeord (password) skal straks udskiftes.

Regler for opbygning af kendeord fremgår af vejledning for CICS – brugere, denne udleveres til de medarbejdere, der autoriseres til ZI – systemet. Desuden er der udarbejdet brugervejledninger for opbygning af kendeord til en række andre systemer, det er systemer, der ikke autoriseres til via CICS.

Når medarbejderen autoriseres som bruger til systemerne, tildeles medarbejderen et kendeord (password), som kun kan bruges en gang (engangskendeord) og medarbejderen skal straks udskifte det med et personligt og fortroligt kendeord.

Hvis medarbejderen har glemt sit kendeord (password), og er sat inaktiv i et system eller gyldighedsperioden er udløbet og medarbejderen derfor skal have nyt, skal medarbejderen tildeles et nyt engangskendeord (password). Dette kan på nuværende tidspunkt udføres af Sundheds- og Omsorgsforvaltningens IT-brugerservice og i visse tilfælde af den nærmeste leder. Alternativt kan engangskendeordet tildeles af sikkerhedslederen eller dennes stedfortræder.

Kendeord (password) indtastes i et ikke læsbart felt.

Kendeord (password) skal udskiftes senest efter 90 dage. De fleste systemer giver selv advarsler, når fristen er ved at udløbe.

Medarbejderen kan selv udskifte sit kendeord (password) når som helst. Et tidligere anvendt kendeord (password) må ikke benyttes igen.

Hvis medarbejderen ikke har været logget på et system i mere end 90 dage, inaktiveres systemet. Dette sker for de fleste systemers vedkommende automatisk. Medarbejderen skal henvende sig til sin nærmeste leder for at blive aktiveret til systemet igen.

Hvis der sker fejl under indtastning af brugerident. og kendeord (password), vises en fejlmeddelelse. Efter 3 mislykkede forsøg på at logge ind på systemet, sætter systemet automatisk medarbejderen inaktiv i systemet. For at få adgang til systemet igen, skal medarbejderen henvende sig til sin nærmeste leder.

Medarbejderen skal altid logge af systemet, hvis PC eller andet udstyr skal udlånes til en kollega i tjenestelig øjemed. Medarbejderen må ikke overlade en "åben" skærm til andre.

Hver medarbejder har sammen med sin nærmeste leder ansvar for at have de korrekte autorisationer til systemerne. Medarbejderen må kun have de autorisationer, der er tjenstligt behov for.

Mindst én gang hvert halve år skal medarbejderen, sammen med sin nærmeste leder, gennemgå sine autorisationer. Den nærmeste leder er ansvarlig for den nødvendige administrative ajourføring herfor.

Hver medarbejder skal være opmærksom på at sikkerheden i forbindelse med anvendelsen af systemerne overholdes og skal kontakte sin nærmeste leder eller sikkerhedslederen (eller dennes stedfortrædere) i tilfælde af mistanke om, at reglerne overtrædes eller sikkerheden på anden måde kompromitteres.

Borgmesteren
Borgmesteren udpeger Forvaltningens IT-sikkerhedsleder og stedfortrædere for denne.

Den årlige beretning om IT - sikkerhedsarbejdets forløb afgives til Borgmesteren. Sundheds- og Omsorgsudvalget orienteres om årsberetningen.

Hvis Sundheds- og Omsorgsforvaltningen ønsker at afvige fra Sikkerhedsregulativets bestemmelser, skal dette godkendes af Borgmesteren på baggrund af en skriftlig begrundet anmodning fra IT-sikkerhedslederen.

Denne sikkerhedsinstruks skal være godkendt af Borgmesteren for Sundheds- og Omsorgsforvaltningen.

Direktionen
Forvaltningens Direktion er generelt ansvarlig for at Forvaltningen overholder alle IT-sikkerhedsregler.

Det påhviler hver enkelt medarbejders leder at sørge for, at medarbejderen får den fornødne instruktion i behandling af Sundheds- og Omsorgsforvaltningens data og gøres bekendt med de til en hver tid gældende sikkerhedsregler.

Det er Sundheds- og Omsorgsforvaltningens Direktion, der skal sikre, at der udarbejdes en risikoanalyse og en risikovurdering og derfra tilrettelægge IT-sikkerhedsniveauet og IT-sikkerhedspolitikken.

Risikoanalyse og risikovurdering skal udarbejdes for hele Sundheds- og Omsorgsforvaltningens IT-anvendelse, herunder de anvendte IT-systemer og IT-driftsmiljøet.

IT-sikkerhedsniveauet og IT-sikkerhedspolitikken skal godkendes af Sundheds- og Omsorgsudvalget.

Der skal foreligge en oversigt over samtlige IT-systemer Sundheds- og Omsorgsforvaltningen er systemansvarlige for, se bilag 5.

Sundheds- og Omsorgsforvaltningens Direktion skal sikre, at der udarbejdes skriftlige aftaler i forbindelse med IT-driftsopgaver, der udføres for Sundheds- og Omsorgsforvaltningens eksterne databehandlere.

Eksterne databehandlere skal ved en årlig erklæring fra en ekstern revisor dokumentere, at der er truffet de tekniske og organisatoriske sikkerhedsbestemmelser, der er fastsat i sikkerhedsreglerne.

Direktionen skal følge op på sikkerhedsmæssige hændelser.

Direktionen skal sikre vedligeholdelsen af risikoanalyser og IT-sikkerhedspolitikken og skal sikre sammenhæng mellem Sundheds- og Omsorgsforvaltningens og Kommunens IT-sikkerhedspolitik og IT-strategi.

Det er Sundheds- og Omsorgsforvaltningens Direktion, der udpeger systemansvarlige og IT-ansvarlige.

Ved udpegning skal det påses at der ikke sker sammenfald mellem kontrollerende og udførende funktioner, dvs. mellem IT-sikkerhedsleder, systemansvarlig og IT-ansvarlige. Dette betyder at en medarbejder kun kan udpeges til én af disse funktioner.

Systemansvarlige og IT-ansvarlige skal udpeges blandt ledende medarbejdere.

Direktionens IT-sikkerhedsopgaver er i det daglige uddelegeret til Informatikstaben

I tilfælde af alvorlige IT-sikkerhedsbrud skal Informatikchefen i Sundheds- og Omsorgsforvaltningen orienteres. Desuden skal Økonomiudvalget orienteres om sagen. Denne underretning sker senest ved den årlige beretning om IT-sikkerheden i Sundheds- og Omsorgsforvaltningen. Såfremt sagen skønnes at have betydning for revisionen, skal Revisionsdirektoratet underrettes. Denne underretning foretages af IT-sikkerhedslederen.

IT - Sikkerhedslederen

Borgmesteren for Sundheds- og Omsorgsforvaltningen udpeger IT-sikkerhedsleder og stedfortræder for sikkerhedslederen for Sundheds- og Omsorgsforvaltningens område.

IT-sikkerhedslederen fører tilsyn med at de til enhver tid gældende sikkerhedsbestemmelser i Sundheds- og Omsorgsforvaltningen og om disse overholdes.

IT-sikkerhedslederen udarbejder Sundheds- og Omsorgsforvaltningens IT-sikkerhedsinstruks og gennemgår/reviderer denne én gang årligt.

Overborgmesteren kan afkræve IT-sikkerhedslederen enhver oplysning af betydning for arbejdet i henhold til IT-sikkerhedsregulativet.

Såfremt der konstateres eller foreligger begrundet mistanke om misbrug, omgåelse af sikkerhedsbestemmelserne eller forsøg herpå, skal IT-sikkerhedslederen omgående foretage en nærmere undersøgelse og efter sin vurdering af sagens alvor orientere Sundhedsborgmesteren og Sundheds- og Omsorgsforvaltningens Direktion.

Administrationscentrets Personaleenhed og Sundheds- og Omsorgsforvaltningens Økonomistab skal efter omstændighederne inddrages i behandlingen af sikkerhedsbruddet.

Sanktionerne i forbindelse med sikkerhedsbruddet vurderes af Administrationscentrets Personaleenhed og medarbejderens chef, eventuelt inddrages Direktionen i sagen.

IT-sikkerhedslederen kan afkræve ethvert led inden for ansvarsområdet enhver oplysning af betydning for tilsyn og kontrol med IT-sikkerhedsbestemmelsernes overholdelse og skal herunder have adgang til lokaler hvor teknisk udstyr befinder sig.

IT-sikkerhedslederen kan også afkræve enhver anden IT-sikkerhedsleder i Københavns Kommune oplysninger af betydning for tilsyn og kontrol med sikkerhedsbestemmelserne inden for eget ansvarsområde.

IT-sikkerhedslederen udarbejder Sundheds- og Omsorgsforvaltningens bidrag til årsberetningen om sikkerhedsarbejdets forløb.

Sammen med de systemansvarlige og de IT-ansvarlige udarbejder IT-sikkerhedslederen autorisationsprocedurer for de forskellige systemer.

IT-sikkerhedslederen giver medarbejderne de nødvendige adgange (autoriserer) til systemerne efter indstilling fra de respektive nærmeste ledere eller fra de medarbejdere lederen har udpeget.

Autorisationsproceduren beskrives nærmere i kapitlet vedrørende autorisationer.

IT-sikkerhedslederen kontrollerer medarbejdernes autorisationer og kan på eget initiativ inddrage tildelte autorisationer.

IT-sikkerhedslederen kontrollerer systemernes sikkerhedslog, det er udelukkende IT - sikkerhedslederen og dennes stedfortræder, der må anmode om en sikkerhedsrapporter og logudskrift, ligesom sikkerhedsrapporter og logudskrift sendes til IT – sikkerhedslederen eller dennes stedfortræder.

IT-sikkerhedslederen skal sikre, at medarbejderne bliver gjort bekendt med sikkerhedsbestemmelserne og at disse regler er tilgængelige i Københavns Kommunens og Sundheds- og Omsorgsforvaltningens net (KKnet).

IT-sikkerhedslederen skal godkende alle behandlinger af personoplysninger i Sundheds- og Omsorgsforvaltningen. Dette gælder også de situationer hvor behandlingerne kun omfatter almindelige identifikationsoplysninger uden fortrolige eller følsomme oplysninger.

For behandlinger af personoplysninger der skal godkendes af Sundheds- og Omsorgsudvalget samt anmeldes til Datatilsynet, udarbejdes indstillingen og anmeldelsen af den systemansvarlige sammen med IT-sikkerhedslederen.

Det er IT-sikkerhedslederen, der foretager selve anmeldelsen til Datatilsynet og koordinerer al korrespondancen med Datatilsynet.

Ændringer i anmeldelser behandles af IT-sikkerhedslederen, som vurderer hvorvidt ændringen skal godkendes i Sundheds- og Omsorgsudvalget og anmeldes til Datatilsynet og i givet fald står for at gennemføre denne procedure i samarbejde med den systemansvarlige.

IT-sikkerhedslederen udarbejder fortegnelser over Sundheds- og Omsorgsforvaltningens behandlinger af personoplysninger, både de anmeldte og de ikke-anmeldelsespligtige og sørger for opdatering af kommunens oversigter over disse.

Alle henvendelser fra Datatilsynet, herunder høringer i forbindelse med klager til Datatilsynet, skal behandles af IT-sikkerhedslederen, som sørger for indsamling af oplysninger og besvarelse af henvendelserne.

Borgeres anmodning om indsigt i behandlinger i Sundheds- og Omsorgsforvaltningen ekspederes af IT-sikkerhedslederen efter retningslinierne i bilag 6.

Det er IT-sikkerhedslederens opgave at vejlede og rådgive Sundheds- og Omsorgsforvaltningen i spørgsmål om behandling af personoplysninger og dermed også i nødvendigt omfang at deltage ved udvikling af nye projekter med behandling af personoplysninger.

Hvis det er nødvendigt at Sundheds- og Omsorgsforvaltningen afviger fra IT-sikkerhedsregulativet er det IT-sikkerhedslederens opgave at udarbejde en skriftlig begrundet anmodning herom. Anmodningen skal

godkendes af Borgmesteren for Sundhed- og Omsorg og rapporteres til Økonomiudvalget, samt medtages i den årlige beretning om IT-sikkerhedsarbejdets forløb.

De udpegede stedfortrædere for IT-sikkerhedslederen kan via delegation udføre alle IT-sikkerhedslederens opgaver.

I Sundheds- og Omsorgsforvaltningen er de stedfortrædende sikkerhedslederes opgaver delt i to områder, dels stedfortrædende sikkerhedsledere for drift der varetager brugeradministration og rettighedstildeling med de opgaver, der følger dette område, dels stedfortrædende sikkerhedsledere der varetager opgaver relateret til myndighedsopgaver.

IT-sikkerhedslederen kan delegere sine opgaver efter de almindelige regler. Delegationen skal være entydig og skriftlig, og opgaverne kan ikke delegeres yderligere.

Der kan kun delegeres opgaver til medarbejdere, som har de fornødne faglige kvalifikationer, og der skal føres kontrol og tilsyn med opgavernes udførelse. Selv om en opgave er delegeret til en anden medarbejder kan IT - sikkerhedslederen stadig selv træffe afgørelser inden for området, lige som delegationen altid kan tilbagekaldes.

Når en opgave delegeres skal der gives nærmere skriftlige forskrifter for udførelsen af opgaven.

En del opgaver er delegeret til de nærmeste leder, jf. bestemmelserne i denne sikkerhedsinstruks.

Stedfortrædende IT – sikkerhedsleder
Stedfortrædende IT – sikkerhedsledere er i Sundheds- og Omsorgsforvaltningen delt på 2 funktions områder på grund af BUM. Det er derfor de stedfortrædende IT – sikkerhedsledere for udfører områder, der varetager brugeradministration og rettighedstildeling. Stedfortrædende IT – sikkerhedsledere i bestiller funktionen varetager myndighedsopgaver. Der er fortsat en IT – sikkerhedsleder, der forestår hele IT – sikkerheds området.

Stedfortrædende IT - sikkerhedsleder(e) for drift
Stedfortrædende IT - sikkerhedsleder for området drift varetager opgave vedrørende brugeradministration herunder oprettelse og rettighedstildeling.

Stedfortrædende IT - sikkerhedsleder(e) for myndighedsopgaver
Stedfortrædende IT – Sikkerhedsledere for området myndighedsopgaver varetager blandt andet udkast til anmeldelser til Datatilsynet og besvarelse af anmodninger om registerindsigt.

Institutionsledere/nærmeste ledere.
Den enkelte leder skal sørge for, at sikkerhedsbestemmelserne overholdes inden for ansvarsområdet.

Lederens ansvar og pligter omfatter de behandlinger af personoplysninger, som finder sted inden for ansvarsområdet.

Lederen tilrettelægger principperne for IT-autorisationer af medarbejderne inden for området i henhold til denne instruks. IT-sikkerhedslederen kan til enhver tid indrages.

Lederen bestiller IT-autorisationer, ændring af IT-autorisationer samt nedlæggelse af IT-autorisationer i overensstemmelse med arbejdsopgavernes udvikling.

Lederen skal sørge for, at samtlige medarbejdere inden for området til enhver tid kender de relevante sikkerhedsmæssige regler.

Lederen skal løbende være opmærksom på, at medarbejderne ikke har flere end de nødvendige IT - autorisationer samt sørge for inddragelse af overflødige IT-autorisationer.

I de systemer, hvor det er teknisk muligt kan lederen få uddelegeret ret til at give medarbejderne engangskendeord.

Hvis der konstateres misbrug eller mistanke om misbrug af IT-autorisationer skal lederen straks rapportere dette til IT-sikkerhedslederen og deltage i de undersøgelser, der er nødvendige.

Lederen besvarer henvendelser fra IT-sikkerhedslederen i forbindelse med de løbende stikprøver af sikkerhedsloggen.

Lederen kan afkræve ethvert led i organisationen inden for ansvarsområdet enhver oplysning af betydning for tilsyn og kontrol med sikkerhedsreglernes overholdelse, og skal herunder have adgang til lokaler hvor teknisk udstyr befinder sig.

Lederen kan ikke delegere deres opgaver eller ansvar til f. eks. superbrugerne

Systemansvarlige
For hvert system hvor Sundheds- og Omsorgsforvaltningen har systemansvaret udpeger Sundheds- og Omsorgsforvaltningens Direktion en systemansvarlig samt mindst en stedfortræder for denne.

Ved udpegning af systemansvarlige og stedfortrædere skal det påses at der ikke sker sammenfald med IT-sikkerhedslederen og den IT-ansvarlige.

Den systemansvarlige har ansvaret for det pågældende IT-systems funktionalitet, opbygning, anvendelse og sikkerhedsløsning.

IT - Sikkerhedslederen underretter den sikkerhedsansvarlige hos den databehandler, hvor systemet køres, om hvem der er systemansvarlig og stedfortræder. Disse oplysninger fremgår også normalt af aftalen mellem Forvaltningen og databehandleren.

Den systemansvarlige

- Fastlægger regler for tildeling af autorisationer/transaktionskoder til IT-sikkerhedslederne
- Sørger for at de nødvendige autorisationskoder lægges ind i sikkerhedssystemet, samt at disse er korrekt opdaterede med hensyn til placering i sikkerhedsgrupper m.v.
- Tildeler disse koder til Sundheds- og Omsorgsforvaltningens IT-sikkerhedsleder og til andre forvaltningers IT-sikkerhedsledere efter behov
- Klassificerer data, jfr. Persondatalovens §§ 6-8, og bistår IT-sikkerhedslederen med beskrivelse af behandlingen i forbindelse med anmeldelse til Datatilsynet
- er sikkerhedslederens konsulent i systemtekniske spørgsmål og skal fremskaffe og koordinere de oplysninger, der er nødvendige i denne forbindelse
- sikrer tilstrækkelig dataafgrænsning, funktionsadskillelse og nødvendige kontrolniveauer i forbindelse med systemudvikling og systemvedligeholdelse
- sikrer, at der efter endt systemudvikling/køb af IT-system foreligger aftaler om systemvedligeholdelse, service og driftsafvikling
- sikrer udarbejdelse af skriftlige grænsesnitaftaler i forbindelse med fremsendelse af data til og fra det konkrete system

Den systemansvarlige er på det IT-sikkerhedsmæssige område kontaktperson i forhold til leverandøren af det pågældende IT-system. Ligesom de overfor databehandleren skal sikre, at disse som minimum får udleveret IT - Sikkerhedsregulativet og de i medfør heraf fastsatte bestemmelser herunder sikkerhedsinstruks for Sundheds- og Omsorgsforvaltningen. Dette som grundlag for udvikling og vedligeholdelse af det pågældende IT-system og driftsafvikling af den pågældende databehandling.

Ingen medarbejdere i Sundheds- og Omsorgsforvaltningen kan anmode en leverandør om eller aftale ændringer i et systems funktionalitet, opbygning og anvendelse samt driftsafvikling, med mindre sådanne ændringer skriftligt er godkendt af den systemansvarlige.

Der skal sikres en procedure for godkendelse af et IT-systems funktionalitet og opbygning, herunder sikkerhedsløsningen. I forbindelse med udvikling, løbende vedligeholdelse og driftsafvikling, skal fastlægges

en skriftlig aftale mellem leverandøren af det pågældende system og Sundheds- og Omsorgsforvaltningen i relation til de systemer Sundheds- og Omsorgsforvaltningen har systemansvaret for.

Ved landsdækkende og fælleskommunale IT-systemer skal proceduren fastlægges i en skriftlig aftale mellem Økonomiforvaltningen og leverandøren af det pågældende system samt driftsafvikleren. Den systemansvarlige skal godkende disse procedurer, som også skal omfatte, at den systemansvarlige automatisk underrettes om ændringer og fejlretning i et system efter systemets anskaffelse.

Den systemansvarlige skal forlods skriftligt godkende udtræk, udlevering eller videregivelse af alle oplysninger/data, herunder videregivelse, såvel internt i kommunen som til modtagere uden for kommunen, herunder eksterne databehandleres udtræk af oplysninger fra IT-systemerne. Godkendelse skal indhentes uanset om udtrækket, udleveringen eller videregivelsen sker elektronisk eller manuelt, herunder i form af skærmbilleder, filoverførsler, disketter, CD-ROM, på papir eller på anden vis.

Den systemansvarlige skal sikre sig, at rekvirentens behandling og brug af oplysninger er anmeldt til Datatilsynet og godkendt i overensstemmelse med Sikkerhedsregulativets bestemmelser herom.

Den systemansvarlige udarbejder forretningsgangsbeskrivelser, der sikrer, at der ikke behandles urigtige eller vildledende data.

Forretningsgangsbeskrivelserne skal udarbejdes under hensyntagen til de principper, der er fastlagt i rammebilag til Københavns Kommunes Budget- og regnskabshåndbog: »Intern kontrol generelt« og »Kontrolforanstaltninger for brug af edb-regnskabssystemer« m.v. og de kompetenceregler, der er fastlagt i den enkelte forvaltning. Der henvises til bilag 4 til Sikkerhedsregulativet.

Den systemansvarlige godkender driftsplanen for det enkelte system i samråd med databehandleren.

Den udpegede stedfortræder for en systemansvarlig kan udføre alle den systemansvarliges opgaver.

Den systemansvarlige kan delegere sine opgaver efter de almindelige regler herom. Delegationen skal være entydig og skriftlig, og opgaverne kan ikke delegeres yderligere.

Der kan kun delegeres opgaver til medarbejdere, som har de fornødne faglige kvalifikationer, og der skal føres kontrol og tilsyn med opgavernes udførelse. Selv om en opgave er delegeret til en anden medarbejder kan den systemansvarlige stadig selv træffe afgørelser inden for området, lige som delegationen altid kan tilbagekaldes.

Når en opgave delegeres skal der gives nærmere skriftlige forskrifter for udførelsen af opgaven.

IT – Ansvarlig(e)

For Sundheds- og Omsorgsforvaltningens IT-installationer udpeger Sundheds- og Omsorgsforvaltningens direktion en eller flere IT-ansvarlig(e) og mindst en stedfortræder for denne (disse).

Ved udpegningen skal det påses, at der ikke sker sammenfald med IT-sikkerhedslederen og de systemansvarlige.

Den IT-ansvarlige har ansvaret for, at sikkerhedsreglerne, herunder IT - Sikkerhedsregulativet, efterleves i forbindelse med opbygning og anvendelse af Sundheds- og Omsorgsforvaltningens IT-driftsmiljø og kommunikations-forbindelser indenfor sit område.

Den IT-ansvarlige skal udarbejde Sikkerhedsforskrifter for Sundheds- og Omsorgsforvaltningens IT-installationer indenfor sit område.

Den udpegede stedfortræder for den IT-ansvarlige kan udføre alle den IT-ansvarliges opgaver.

Den IT-ansvarlige kan delegere sine opgaver efter de almindelige regler herom. Delegationen skal være entydig og skriftlig, og opgaverne kan ikke delegeres yderligere.

Der kan kun delegeres opgaver til medarbejdere, som har de fornødne faglige kvalifikationer, og der skal føres kontrol og tilsyn med opgavernes udførelse. Selv om en opgave er delegeret til en anden medarbejder, kan den IT-ansvarlige stadig selv træffe afgørelser inden for området, lige som delegationen altid kan tilbagekaldes.

Når en opgave delegeres skal der gives nærmere skriftlige forskrifter for udførelsen af opgaven.

Kapitel 3

Behandling af Personoplysninger

Enhver behandling af personoplysninger skal som udgangspunkt godkendes af Sundheds - og Omsorgsudvalget og til udtalelse i og anmeldes til Datatilsynet inden behandlingen iværksættes.

Behandling af almindelige personoplysninger, som ikke omfatter oplysninger af fortrolig eller følsom karakter, er dog undtaget fra kravet om udtalelse og anmeldelse.

Sundheds - og Omsorgsudvalget har bemyndiget Borgmesteren, som den øverste daglige ansvarlige leder af Forvaltningen, til at træffe beslutning om behandlinger, der er undtaget fra pligten til anmeldelse. IT-sikkerhedslederen træffer disse beslutninger på Borgmesterens vegne.

Enhver enhed inden for Forvaltningen som ønsker at starte en behandling af personoplysninger, skal derfor ansøge om tilladelse hertil hos sikkerhedslederen. IT - sikkerhedslederen vurderer om behandlingen er anmeldelsespligtig og derfor skal godkendes i Sundheds - og Omsorgsudvalget og anmeldes til Datatilsynet.

Ansøgningen skal indgives til IT-sikkerhedslederen på blanketten i bilag 7

Behandlingen må ikke iværksættes før godkendelsen foreligger.

Kun IT-sikkerhedslederen må foretage anmeldelse af en behandling til Datatilsynet.

Anmeldelsen udarbejdes i et samarbejde mellem den systemansvarlige enhed og IT-sikkerhedslederen, hvor den systemansvarlige er ansvarlig for indholdet i anmeldelse. Det er dog den IT – sikkerhedsansvarlige der fremsender anmeldelsen til Datatilsynet jævnfør ovenstående ligesom det er IT – sikkerhedslederen, der er ansvarlig for udvalgsbehandlingen, herunder udarbejdelse af indstillingen.

Ændringer i godkendte anmeldelser skal besluttes af Sundheds- og Omsorgsudvalget efter retningslinierne for nye anmeldelser.

Hvis en behandling af personoplysninger vedrører flere forvaltninger skal beslutningen om behandlingen træffes i Økonomiudvalget.

IT - sikkerhedslederen udarbejder og vedligeholder fortegnelsen over behandlinger godkendt i Sundheds- og Omsorgsforvaltningen, såvel de anmeldte som de ikke anmeldelsespligtige. Sikkerhedslederen indberetter denne fortegnelse til Overborgmesteren, Borgerrepræsentationens Sekretariat i forbindelse med IT - Årsrapporten.

For anmeldelsespligtige behandlinger gælder en række særlige sikkerhedskrav, som skal være opfyldt inden proceduren med godkendelse i Sundheds- og Omsorgsudvalget og anmeldelse til Datatilsynet startes.

Disse sikkerhedskrav er

- Adgang til oplysningerne kræver at medarbejderen er tildelt en personlig og fortrolig adgangskode.
- Der skal foretages en registrering, logning, af alle anvendelser af personoplysningerne.
- Logningen skal indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium.
- Der skal dog ikke foretages logning ved personoplysninger, som indgår i tekstbehandlings-dokumenter og lignende, der ikke er i endelig form eller ved dokumenter, der er i endelig form, hvis dokumenterne slettes inden for 30 dage fra dokumentet er oprettet.
- Hvis en medarbejder afvises af systemet på grund af manglende autorisation eller forkert kendeord tre gange skal medarbejderens adgang til systemet spærres.

- Alle sikkerhedskravene kan ses i Bilag 2 til IT - Sikkerhedsregulativet.

Generelt skal alle personoplysninger opbevares på servere eller centrale anlæg, aldrig på den personlige PC.

Kapitel 4

Brugerautorisation

Al adgang til IT-systemer, som er anmeldt til Datatilsynet, skal være betinget af konkrete autorisationer fra IT - sikkerhedslederen.

IT - sikkerhedslederen må kun autorisere medarbejdere, der er beskæftiget med det sagsområde, hvortil oplysningerne behandles. Den enkelte medarbejder må ikke autoriseres til at kunne se eller opdatere oplysninger, den pågældende medarbejder ikke har tjenstligt behov for.

Medarbejderen får adgang gennem en personlig autorisation med brugerident. og kendeord(password). Autorisationen tildeles efter indstilling fra de(n) underskriftsberettigede i samarbejde med medarbejderens chef.

I forbindelse med anmodning om autorisation til medarbejderne, har den lokale leder udpeget 1 - 3(4) personer, der må anmode om medarbejderoprettelse samt tildeling af rettighed til relevante systemer. Desuden oplyses hvilke rettigheder, den enkelte medarbejder skal have i de pågældende systemer.
I den forbindelse anvendes en række forskellige autorisationsblanketter, der er tilgængelige på KKnet. Autorisationsblanketterne på KKnet skal anvendes.

Det skal fremgå af autorisationen om medarbejderen må foretage opdateringer eller kun forespørgsler.

Hvis medarbejdere hos databehandlere eller samarbejdspartnere i øvrigt har behov for adgang til Forvaltningens systemer, skal der udarbejdes en skriftlig aftale med den pågældende virksomhed og de pågældende medarbejdere skal underskrive en erklæring hvoraf det fremgår at de er bekendt med sikkerhedsbestemmelserne og deres tavshedspligt. Disse erklæringer er medtaget som bilag 8

IT-sikkerhedslederen autoriserer de enkelte medarbejdere hos databehandleren og samarbejdspartneren med brugerident. og personligt og fortroligt kendeord.

Kapitel 5

PC anvendelse

Når medarbejderen er logget på PC'en er der dermed adgang til de systemer medarbejderen er autoriseret til. Kun den pågældende medarbejder selv må benytte sin adgang til systemerne.

Derfor skal medarbejderen logge af, hvis PC'en forlades midlertidigt.

Pauseskærmsfunktionen skal være aktiveret, således at pauseskærmen automatisk starter hvis PC'en ikke har været benyttet i 5 minutter.

Pauseskærmen skal være beskyttet af et personligt og fortroligt kendeord.

For alle PC'er på Sundheds- og Omsorgsforvaltningens netværk er disse regler automatisk sat på.

På alle PC'er i Sundheds- og Omsorgsforvaltningen, der er koblet op i netværk (permanent og periodisk), skal der være installeret et antivirusprogram, som løbende opdateres, og overvåges af de centrale netværksadministratorer.

Forvaltningen har udgivet et sæt retningslinier for brug af e-mail, Internet og Hjemme pc'er. Disse retningslinier suppleres af bestemmelser i sikkerhedsforskrifterne. Alle medarbejdere skal kende disse regler. bilag 9 og bilag 10

Kapitel 6

Kontrol

Registreringen af opslag på personoplysninger, sikkerhedsloggen, gemmes i 6 måneder.

IT-sikkerhedslederen gennemgår som et minimum en 2-timers udskrift af sikkerhedsloggen en gang i kvartalet, som udtages stikprøvevis blandt de anvendte systemer, der er anmeldt til Datatilsynet.

IT-sikkerhedslederen kan til enhver tid gennemgå udskrift af sikkerhedsloggen.

Under gennemgangen undersøges et antal tilfældigt udvalgte opslag nærmere.

Stikprøverne kan sendes til institutionslederne/nærmeste leder, som undersøger om de udvalgte opslag er sket tjenstligt og i overensstemmelse med sikkerhedsreglerne.

Gennemgangen af sikkerhedsloggen sker med henblik på at afsløre misbrug.

Ved mistanke eller viden om misbrug kan sikkerhedsloggen gennemgås for en enkelt person enten for alle systemer eller for udvalgte systemer og transaktioner i op til 6 måneder.

Sikkerhedsloggen må kun benyttes til rent sikkerhedsmæssige formål.

IT-sikkerhedslederen sørger for at udskrifterne af sikkerhedsloggen destrueres på forsvarlig måde.

Såfremt det konstateres at en autorisation er misbrugt eller der er mistanke om det, skal sikkerhedslederen straks foretage en nærmere undersøgelse.

En misbrugt autorisation skal straks inddrages.

Hvis misbruget af autorisationen kan have medført et økonomisk tab orienteres Økonomistaben, som sørger for orientering af Sundheds- og Omsorgsforvaltningens ledelse og af Revisionsdirektoratet.

Ved ethvert misbrug orienteres den pågældende medarbejders Institutionsleder/nærmeste leder og normalt også Personaleenheden, eventuelt inddrages Direktionen i sagens vurdering. Det er disse instanser, der vurderer alvoren i misbruget og hvilke sanktioner, der skal iværksættes.

Misbrug af autorisationer medtages i den årlige beretning, hvorved det sikres at Sundheds- og Omsorgs-udvalget og Økonomiudvalget orienteres.

Misbrug eller forsøg på misbrug, der kan henføres til ansatte i en anden forvaltning indberettes af IT - sikkerhedslederen til den anden forvaltnings IT - sikkerhedsleder.

Kapitel 7

Indsigt i Personoplysninger m.m.

Når en borger anmoder om indsigt i de oplysninger, der behandles i Sundheds- og Omsorgsforvaltningen om vedkommende, skal IT-sikkerhedslederen snarest muligt, og inden for 4 uger give borgeren de ønskede oplysninger.

IT-sikkerhedslederen skal sikre sig at den pågældende borger ved sin henvendelse har legitimeret sig på den foreskrevne måde, eller i øvrigt er identisk med den borger oplysningerne vedrører.

Hvis en anden person end den pågældende selv henvender, sig skal det sikres, at denne er berettiget til at handle på den pågældende borgers vegne.

Kan anmodningen ikke besvares inden 4 uger efter modtagelsen, skal den pågældende have meddelelse om grunden hertil samt om, hvornår svar forventes at kunne foreligge.

Personen har også ret til at få meddelelse om, at der ikke behandles oplysninger om vedkommende.

Meddelelsen om behandling af oplysninger sker normalt skriftligt ved at besvarelsen sendes til den pågældendes folkeregisteradresse.

Meddelelsen kan dog også gives mundtligt.

En person har ikke krav på ny meddelelse før 6 måneder efter sidste meddelelse, medmindre der godtgøres en særlig interesse heri

Proceduren for behandling af anmodninger om indsigt i personoplysninger er nærmere beskrevet i bilag 7.

Bestemmelserne om kommunens oplysningspligt, den registreredes rettigheder i øvrigt og om videregivelse af oplysninger behandles i overensstemmelse med reglerne i persondataloven og IT-sikkerhedsregulativet.

Kapitel 8

Ikrafttræden

Denne sikkerhedsinstruks træder i kraft den 7. december 2006 og erstatter den tidligere sikkerhedsinstruks fra 10. juni 2005.

Københavns Kommune
Sundheds- og Omsorgsforvaltningen

Den: 7. december 2006

Mogens Lønborg Jesper Fisker