IT-Sikkerhedspolitik

Oktober 2011

Svendborg Kommune

1 Indledning

Svendborg Kommune tilstræber at optimere IT-anvendelsen. Samtidig ønsker Svendborg Kommune, at medarbejderne har en åben og positiv holdning til begrebet IT-sikkerhed, hvor der lægges vægt på reel sikkerhed.

IT-sikkerhedspolitikken for Svendborg Kommune har udgangspunkt i kommunens IT-baserede forretningsprocesser, som omfatter alle anvendte IT-systemer.

IT-sikkerhedspolitikken respekterer de krav, som datalovgivningen til enhver tid måtte stille til registre med personhenførbare oplysninger.

IT-sikkerhedspolitikken fastsætter hovedprincipperne for den overordnede IT-sikkerhed i Svendborg Kommune, herunder placerer ansvaret for varetagelse af IT-sikkerheden.

I nødvendigt omfang uddybes de overordnede regler dels i en række bilag til politikken og dels i en folder til brugerne. Ydermere skal selve jobudførslen af væsentlige sikkerhedstiltag beskrives og vedligeholdes i operationelle instrukser.

Som følge heraf vil miljøet bevæge sig fra det mere statiske mod det mere dynamiske, jo længere man går ned i detaljen.

2 Formål

IT-sikkerhedspolitikken har til formål at sikre,

- at IT-sikkerheden er naturligt afbalanceret i forhold til de værdier og informationer, som skal beskyttes
- at ansvaret for de enkelte elementer i IT-sikkerheden er entydigt placeret
- at IT-sikkerheden skal i videst muligt omfang integreres i forretningsprocesserne i Svendborg Kommunes forvaltninger / enheder
- at sikkerheden etableres på et effektivt og ensartet niveau, så risikoen for alvorlige fejl begrænses

Svendborg Kommunes IT-sikkerhedspolitik skal afspejle såvel myndighedskrav som kommunens eget behov.

IT-sikkerhedspolitikken skal i overensstemmelse med Svendborg Kommunes vitale forretningsprocesser være en afvejning af væsentlighed og risiko. Sikringen skal stå mål med risikoen.

Det vil sige, at man ikke vil sikre sig for enhver pris, men være bevidst om enhver risiko.

For nogle af de efterfølgende områder er der opsat konkrete mål, som ønskes opfyldt med IT-sikkerhedspolitikken for Svendborg Kommune.

3.1 Ansvar i linien

Ansvaret for overholdelse af Svendborg Kommunes IT-sikkerhedspolitik ligger i linieorganisationen. Cheferne for Svendborg Kommunes forvaltninger / afdelinger er dermed ansvarlige for de respektive brugersystemer, som løser konkrete opgaver indenfor de pågældendes ansvarsområde.

Herudover har Svendborg Kommune en række medarbejdere, som er ansvarlige for delelementer i IT-anvendelsen eller konkrete anvendelsesspecifikke områder heraf.

3.2 Dataejer

Et gennemgående begreb i Svendborg Kommunes IT-sikkerhedspolitik er dataejer. For alle anvendte, definerbare datamængder identificeres en dataejer, som tildeles det grundliggende ansvar for, at der i forbindelse med anvendelsen af kommunens data varetages en hensigtsmæssig sikkerhed. Dataejerne kan outsource selve varetagelsen af IT-sikkerheden til interne eller eksterne samarbejdspartnere. Dataejer vil typisk være den fagansvarlige for et område.

For Svendborg Kommunes fælles, tværfaglige systemer vil der skulle udpeges én dataejer, som varetager den koordinerende rolle vedrørende dataanvendelsen.

3.3 IT-chefen

IT-chefen, eller eventuelt delegerede, er ansvarlig for det nødvendige overblik og skal påse, at der til stadighed er etableret forretningsgange og procedurer, som støtter overholdelsen af sikkerhedspolitikken.

IT-chefen har ansvaret for, at IT-sikkerhedspolitikken og tilhørende bilag løbende ajourføres i takt med udviklingen og eventuel ibrugtagning af nyt hardware eller software.

Ændringer i Svendborg Kommunes IT-sikkerhedspolitik skal samordnes i IT-udvalget.

3.4 Revision

Der skal årligt foretages en revision af, hvorvidt reglerne i Svendborg Kommunes IT-sikkerhedspolitik i praksis efterleves. Varetagelsen af sikkerheden kontrolleres / revideres ud fra en konkret vurdering af væsentlighed og risiko. IT-chefen er ansvarlig for, at denne revision foretages, eventuelt med ekstern bistand.

3.5 Opgaver og ansvar

Placering i organisationen	**Ansvar**
IT-chef	Koordinering, overblik, opfølgning, ajourføring.
IT-medarbejdere	Tekniske driftsopgaver, support, udvikling, beskrive.
Forvaltningschef	Ansvarlig for anvendelsen af brugersystemer - almindeligt ledelsesmæssigt ansvar for eget område.
Dataejere	Specifikt ansvar for data / system, datakvalitet - intern kontrol, stillingtagen til sikkerhed, beskrive. Dataejer vil typisk være den fagansvarlige.
Medarbejdere generelt	Varetagelse af IT-sikkerheden ved overholdelse af nærværende politik samt almindelig sund fornuft.

4 Regelsæt

Svendborg Kommunes IT-organisation er - og bør være - omgivet af en række retningslinier og regelsæt, som skal bidrage til, og være med til at sikre, en høj og ensartet kvalitet i forbindelse med IT-anvendelsen.

4.1 Udviklingsplan/-strategi

Det skal sikres, at der er overensstemmelse mellem kommunens overordnede mål og IT-kontorets mål, og at IT-kontoret er orienteret om de øvrige forvaltningers / afdelingers behov for IT-anvendelse.

IT-kontoret skal løbende arbejde for at implementere kommunens "Strategiplan for Informations-Teknologisk-udvikling i Svendborg Kommune", som forventes ajourført med to-tre års mellemrum.

4.2 Regler for IT-brugere

Den enkelte medarbejder, som i det daglige anvender en IT-arbejdsplads i Svendborg Kommune, skal modtage en sikkerhedsinstruks gældende for IT-brugere.
Udover en række praktiske oplysninger om anvendelse af programmel og hardware, beskriver retningslinierne ligeledes den enkelte medarbejders ansvar som IT-bruger.
Da IT-anvendelsen følger den generelle teknologiske udvikling, vil retningslinierne med jævne mellemrum blive ajourført af IT-kontoret.

5 Datalov

Dataloven har til formål at sikre følsomme data imod misbrug. Er der tale om en samling af oplysninger, eksempelvis en telefonbog, en adresseliste eller et personalekartotek, hvis indhold ligger på et edb-system, er Dataloven gældende.

Bilag 14 beskriver en række faktuelle forhold i forbindelse med Dataloven, herunder Svendborg Kommunes nødvendige tiltag på området.

5.1 Delegation

Dataloven er omfattet af den almindelige delegationsret.

5.2 Ansvar

Linieorganisationen har ansvaret for at overholde kravene i Dataloven samt for at udarbejde anmeldelser vedrørende behandling af personoplysninger. Dataejer har den udførende rolle.

IT-sikkerhedsfunktionen har ansvaret for at yde knowhow til linieorganisationen samt for at vedligeholde oversigter over Svendborg Kommunes anmeldelser.

IT-sikkerhedsfunktionen har desuden den koordinerende rolle i forbindelse med behandling af henvendelser fra borgere, brugere og myndigheder.

6 Fysisk sikkerhed

Mål:	**Den fysiske sikring af Svendborg Kommunes IT-installation skal være i overensstemmelse med afhængigheden af IT-driften og tillige afspejle den værdi IT-udstyr repræsenterer.**

Svendborg Kommune ønsker at sikre de fysiske installationer mod ulykker, hærværk og tyveri. Desuden skal der i fornødent omfang sikres mod forsyningssvigt. Sikringen skal dog stå i et naturligt forhold til de værdier, som skal beskyttes. Det vil sige, at der er strengere krav til sikringen af centralt udstyr end til sikringen af udstyr i eksempelvis kontormiljøer. Den fysiske sikring af de enkelte miljøer skal så vidt muligt ske i overensstemmelse med bilag 2 og nedenstående hovedpunkter.

6.1 Bygningsindretning

Opbevaringen af servere skal ske i specielt indrettede lokaler. Lokalerne skal indeholde de fornødne installationer og være sikret hensigtsmæssigt. Krydsfelter og netværksenheder skal behandles med tilsvarende omhu.

6.2 Adgangskontrol

Der skal være procedurer, som sikrer, at det kun er autoriserede medarbejdere, som har adgang til serverrum, krydsfelter og lignende.

6.3 Alarmsystemer

Svendborg Kommune skal etablere tilstrækkelige alarmforanstaltninger på relevante bygninger og lokaler, således at eventuelle uregelmæssigheder alarmeres til de ansvarlige.

6.4 Registrering af aktiver /forsikring

IT-kontoret har ansvaret for registrering af samtlige hardware- og softwareprodukter repræsenterende en væsentlig værdi, således at det via entydig identifikation er muligt at genfinde et produkt. Denne registrering, som foretages af de enkelte forvaltninger, har til hensigt at danne et overblik over kommunens IT-mæssige aktiver, herunder licensforhold

IT-kontoret skal løbende vedligeholde positivlister for hardware og software hvad angår den generelle edb-anvendelse i kommunen. Anvendelsen af eksempelvis fagspecifikke systemer har brugeren selv ansvaret for, og der kan ikke umiddelbart forventes support fra IT-funktionen på sådanne produkter. Nye produkter må ikke ibrugtages uden forudgående behørig aftestning og godkendelse.

Der skal føres overordnet kontrol med softwarelicenser, og der må ikke afvikles programmer, uden at der er behørig dokumentation for licensforhold.

Det er forbudt at afvikle software, som Svendborg Kommune ikke har licens til.

Den enkelte forvaltningschef træffer beslutning om, hvorvidt IT-udstyr skal forsikres i samarbejde med risiko-koordinatoren.

7 Datasikkerhed

Mål:	**Det skal sikres, at data, som anvendes i Svendborg Kommunes forretningsprocesser, til enhver tid har en tilstrækkelig høj kvalitet. Det er kun autoriserede brugere, der har adgang til Svendborg Kommunes data, blandt andet for at sikre mod misbrug af fortrolige oplysninger og manipulation af data. Der føres kontrol med anvendelsen af data for at forhindre fejl i løbet af databehandlingen. Der skal være stabilitet i driften.**

Datagrundlaget i Svendborg Kommunes IT-systemer repræsenterer en betydelig værdi, ligesom der kan være tale om fortrolige oplysninger. Disse værdier skal sikres mod uautoriseret adgang og imod tab og forvanskning.

Dataejer skal derfor i fællesskab med IT-funktionen fastsætte et sikkerhedsniveau, som modsvarer de værdier, der skal sikres, og samtidig gør det muligt for brugerne at opnå en fornuftig anvendelse af systemerne.

Fastsætte af sikkerhedsniveauet er beskrevet i følgende afsnit.

7.1 Adgang

Kun medarbejdere med et tjenstligt behov kan få adgang til kommunens IT-systemer herunder data.

Det er altid dataejer, som godkender autorisationer.

IT-chefen er ansvarlig for at udarbejde forretningsgange for tildeling, ændring og sletning af autorisationer, som sikrer ovenstående.

IT-chefen er ansvarlig for at definere, hvilke systemer eller informationer, kommunens medarbejdere skal have fri adgang til.

IT-udvalget er ansvarlig for at definere, hvilke systemer og informationer, kommunens borgere m.m. skal have fri adgang til.

7.2 Anvendelse

Der etableres et logningsniveau (registrering af system- og dataanvendelsen).

IT-chefen tager stilling til logningsniveauet for overordnede systemer. Dataejer tager stilling til logningsniveauet for den enkelte applikation.

Logningen skal som minimum være i overensstemmelse med Dataloven og erlægges ud fra en vurdering af væsentlighed og risiko.

For hvert enkelt system tages der stilling til omfanget af intern kontrol med medarbejdernes dataanvendelse, herunder udskrivning og behandling af statistikmateriale med videre.

7.3 Tab, herunder backup

For at sikre, at alle data bliver sikkerhedskopieret, skal alle edb-brugere placere arbejdsdokumenter, regneark og lignende på de centrale servere.

For hvert enkelt system skal der tages stilling til frekvensen i forbindelse med sikkerhedskopiering , og hvordan kopierne skal opbevares. Der skal for hvert system foretages en teknisk afprøvning af kopieringsrutinerne, herunder kontrol af genetableringsprocedurerne.

Procedurerne for sikkerhedskopiering og reetablering skal beskrives, således at procedurerne til enhver tid er kendt af relevante medarbejdere i IT-organisationen.

Sikkerhedskopierne skal opbevares på en forsvarlig måde, helst i et aflåst datasikkerhedsskab, som er beregnet til det pågældende datamedie. Brandskabet skal opbevares forsvarligt, det vil sige helst i aflåste - sikre - omgivelser. Indholdet af sikkerhedskopier i brandskabet skal være entydigt mærket og kunne genfindes.

Backup og genindlæsningsrutiner skal aftestes mindst én gang om året, eller i forbindelse med omlægning af rutinen.

De konkrete retningslinier for sikkerhedskopiering af centrale og decentrale servere og af pc´er , som ikke er forbundet til kommunens IT-netværk (LAN), fremgår af bilag 10.

7.4 Datakvalitet

Aftestning af systemer

Systemer må ikke ibrugtages, før der er foretaget en aftestning, hvis omfang afhænger af væsentlighed og risiko. Efterfølgende ændringer af systemet skal tillige aftestes.

Dokumentation

Der skal foreligge dokumentation for systemers konstruktion og virkemåde, dels af hensyn til brugernes anvendelse af systemet og dels af hensyn til mulighederne for at kunne videreudvikle systemet.

Dette gælder for såvel egenudviklede systemer som for systemer, kommunen har fået specialudviklet hos en leverandør.

Intern kontrol

For hvert system skal der tages stilling til, hvilke interne kontroller, der skal udføres i forbindelse med databehandlingen, og hvem der er ansvarlig herfor.

Dataejer er ansvarlig for, at procedurerne iværksættes.

Se i øvrigt kapitel 9.

7.5 Virus

Svendborg Kommune skal etablere sikkerhedsprocedurer, som beskytter edb-systemerne imod virusangreb. Dette skal finde sted, dels ved at have nogle fornuftige værktøjer til at imødegå aktuelle risici, dels ved at motivere de enkelte slutbrugere til varetagelse af en god edb-skik. Se i øvrigt bilag 1 afsnit 5.

Det påhviler IT-kontoret, at IT-anvendelsen i kommunen til enhver tid er opdateret med den nyeste version af det anvendte antivirusprogrammel.

8 Datakommunikation

Mål:	**Sikre, at uvedkommende ikke kan få adgang til Svendborg Kommunes IT-installation.**

Samtidig med at Svendborg Kommune skal anvende Internet og relaterede nettjenester, skal man råde over et sikkert lokalnet.

8.1 Fire-wall

"Indgangsdørene" til Svendborg Kommunes LAN skal være sikret således, at det kun er "inviterede edb-brugere" som kommer ind.

IT-chefen er ansvarlig for, at adgangen til netværket er beskyttet via en firewall, samt at opsætning og administration af denne håndteres sikkerhedsmæssigt forsvarligt. Firewall-softwaren skal undergå løbende vedligeholdelse i takt med fremkomsten af nye risici.

Desuden har IT-chefen ansvaret for at overvåge aktiviteten i firewall´en.

8.2 Netværk

IT-kontoret er ansvarlig for opbygning og vedligeholdelse af netværket. Der vedligeholdes i denne forbindelse en oversigt over kommunens LAN.

Alle eksterne kommunikationsforbindelser skal godkendes af IT-kontoret, som vedligeholder oversigter over kommunikationen.

I forbindelse med pc´er, som er tilkoblet Svendborg Kommunes LAN, må der ikke anvendes modem-forbindelser, med mindre der gives særskilt tilladelse fra IT-kontoret.

8.3 Hjemmearbejdspladsen

Der skal udarbejdes og vedligeholdes et sæt retningslinier for anvendelsen af hjemmearbejdspladser i relation til jobudførslen i Svendborg Kommune.

8.4 Mobile arbejdspladser

Teknologien medfører stadigt nye typer af databærende / databehandlende udstyr, eksempelvis digitale kalendere, stregkodescannere med mere.

IT-chefen er ansvarlig for, at der i relevant omfang udarbejdes og vedligeholdes særlige sikkerhedsregler for sådant udstyr, som måtte blive taget i anvendelse i kommunen.

8.5 Internet, herunder e-mail

Der skal udarbejdes og vedligeholdes et sæt retningslinier for anvendelse af Internet og e-mail på Svendborg Kommunes udstyr.

9 Udvikling og anskaffelse af edb -udstyr

Mål:	**Ved anvendelse af fast definerede forretningsgange og standarder skal det sikres, at de systemer, der udvikles og vedligeholdes, er pålidelige og effektive.**

Der foretages i nogen omfang egenudvikling af applikationer i Svendborg Kommune.

De enkelte udviklere eller ansvarlige skal sikre, at de udviklede applikationer sikres i et tilfredsstillende omfang, dels via centralt opdaterede sikkerhedskopier dels ved udarbejdelse af præcis dokumentation af programmeringsgrundlaget. Se bilag 4.

IT-funktionen (basis IT-organisationen) skal altid inddrages i processen forinden anskaffelse af nyt software blandt andet af hensyn til kontraktlige forhold, aftestning, drift med mere.

Se i øvrigt afsnit 7.4.

10 Nødberedskab

Mål:	**At væsentlige forretningsprocesser indenfor en given tidsperiode kan videreføres i prioriteret og kontrolleret rækkefølge.** **Der skal foretages en vurdering af de væsentlige forretningsprocessers afhængighed af IT-driften og herudfra opstilles et relevant nødberedskab.**

Svendborg Kommune skal have og vedligeholde et nødberedskab, således at forretningsprocesserne ikke vil blive unødigt hæmmet i forbindelse med eventuelle nødsituationer i IT-driften. Nødberedskabet skal stå i naturlig forhold til vigtigheden af det driftsmiljø, som skal beskyttes.

Dataejerne - som også typisk er de fagansvarlige - har ansvaret for at foretage en vurdering af forretningsprocesserne i forhold til afhængigheden af IT-systemerne, idet et eventuelt behov for et nødberedskab fastlægges i samarbejde med IT-kontoret.

Afhængigt af det konkrete behov skal der defineres en organisationsplan, som i tilfælde af en katastrofe sikrer klare kompetence- og ansvarsforhold.

IT-chefen har ansvaret for at udarbejde og vedligeholde organisationsplanen og for at sikre den nødvendige teknik og ressourcer i relation til nødberedskabet.

1.1 IT-sikkerhedsbestemmelser for IT -brugere i Svendborg Kommune

Bilag 1.

IT-sikkerhedsbestemmelser for IT -brugere i Svendborg Kommune

Samtlige medarbejdere, som anvender en IT-arbejdsplads i Svendborg Kommune, skal kende nærværende retningslinier for IT-brugere. Retningslinierne vil blive ajourført af IT-kontoret, som tillige er ansvarlig for distribution af retningslinierne.

Ved en IT-bruger forstås enhver person, som anvender IT-udstyr stillet til rådighed af Svendborg Kommune.

Det er den enkelte brugers ansvar, at retningslinierne følges, og at IT-anvendelsen generelt finder sted i overensstemmelse med almindelig sund fornuft / god IT-skik.

sikkerhedsfolder.pdf

1 Den enkeltes ansvar som pc -bruger

Som IT-bruger i Svendborg Kommunes er du ansvarlig for det, der foregår på din pc. Det gælder fra du logger dig på, til du logger dig af igen. Hvis din pc overlades til en kollega, skal du først logge dig af, hvorefter kollegaen kan logge sig på. Du må ikke overlade din pc til en person, som ikke er autoriseret til Svendborg Kommunes systemer.

Som IT-bruger skal du iagttage de samme forholdsregler og fornuftsmæssige overvejelser, som er gældende for de øvrige elementer i din arbejdsdag.

Du skal være opmærksom på at i mange edb-systemer bliver der gemt oplysninger om hvad du har gjort. Disse oplysninger kan bruges ved mistanke om misbrug af edb-systemerne, og ved kontrol af anvendelsen.

2 Passwordsikkerhed

Når du som medarbejder i Svendborg Kommune får adgang til de fælles IT-systemer, får du samtidig adgang til en række ressourcer og oplysninger, som er fortrolige og strengt personlige. Derfor bliver alle IT-brugere udstyret med et hemmeligt og personligt password, som ikke må videregives til andre, heller ikke dine

nærmeste kolleger.

Midlertidigt password kan gives til eksterne konsulenter/teknikere af Stadsdirektøren eller af ham bemyndigede personer. De nedlægges straks efter brug.

Ingen medarbejder må udlevere password til eksterne teknikere eller i forbindelse med henvendelser på telefon, e-mail eller lignende.

2.1 Anvendelse af password :

Når arbejdspladsen forlades, skal der enten logges ud af systemet eller anvendes en pauseskærm med password. Husk at pauseskærmen skal være aktiveret, når arbejdspladsen forlades.

For at passwords skal have den ønskede effekt, er det nødvendigt at stille visse minimumskrav til opbygning og længde samt ændringsinterval.

Et godt password er en bogstav- / talkombination, som er nem at huske, men til gengæld er svær at gætte for andre. Undgå specialtegn som #, ¤, /, @ og lignende, da det i nogle henseender kan give problemer. Undgå også Æ, æ, Ø, ø, Å, å**,** da det er specielle danske bogstaver, som kan give systemmæssige problemer.

Anvend derfor kun tal samt de 26 første bogstaver i alfabetet. Anvend aldrig eget navn, egne eller den nærmeste families initialer, ord som findes i ordbøger, fødselsdage, bilnummer, hundenavn eller lignende, da det er oplagt at prøve den slags kombinationer for uvedkommende.

I dagligdagen skal du undgå, at andre får kendskab til dit password, da det ved et eventuelt misbrug umiddelbart er dig (indehaveren), der bliver gjort ansvarlig. Det skal i den forbindelse bemærkes, at forsøg på uautoriseret adgang til systemer eller dele heraf bliver registreret automatisk.

Selvom du har et godt password, skal det med jævne mellemrum skiftes ud. Alle passwords skal skiftes ud hver 3. måned.

Hvis du skulle få kendskab til forsøg på uautoriseret adgang til Svendborg Kommunes IT-systemer har du pligt til at underrette hotline, den centrale IT-sikkerhedsfunktion eller edb-koordinatoren.

Der er følgende minimumskrav til anvendelse af password i systemerne:

- Minimum 6 karakterer med en blanding af bogstaver og tal
- Skift hver 90. dag - passwords må ikke på noget tidspunkt genbruges
- Password skal altid ændres første gang, der logges på et system.

3 Programanvendelse , herunder licenser

De programmer, som må anvendes på Svendborg Kommunes IT-udstyr, fremgår af positivlisten for software. Alle ændringer i konfigurationen skal foretages i samarbejde med den stedlige IT-koordinator.

Svendborg Kommune råder over en række licensaftaler, som enten gælder for alle pc-arbejdspladser, konkrete afdelinger eller enkelte brugere. Installationen og anvendelsen af disse eller andre programmer aftales med den stedlige IT-koordinator.

4 Internet

I Svendborg Kommune er der adgang til Internet og elektronisk post. Hvis du er bruger af Internet eller e-post skal du være opmærksom på de særlige retningslinier anført i

IT-sikkerhedspolitikkens bilag 8 og 9.

5 Sikkerhed imod virus

5.1 Hvad er en virus ?

Virus er programstumper, som tilføjer uønskede "funktioner" i de installerede programmer. Samtidig kan der være risiko for smitte af andre programmer både på pc'en og på Svendborg Kommunes netværk.

De alvorligste vira kan eksempelvis slette oplysninger på harddisken.

Virus kan overføres via alle datakilder, eksempelvis disketter, cd-rom, Internettet, e-mail med videre.

5.2 Hvordan undgås virus ?

For at undgå virus anvender Svendborg Kommune et program, som kan finde og fjerne vira på både netværk og pc´er. For at kunne følge med den konstante udvikling i vira, bliver antivirusprogrammellet løbende opdateret således, at man konstant kan finde og fjerne de nyeste vira.

Antivirusprogrammet ligger aktivt på den enkelte pc, og følger med i, hvad der sker på pc'en. Men det er desuden muligt at køre en manuel virusskanning, såfremt der er mistanke om, at pc'en er inficeret.

Det er *ikke* tilladt at ændre i de foruddefinerede instillinger i antivirusprogrammellet, herunder at deaktivere det.

Det er vigtigt, at den generelle anvendelse af datakilder foregår under hensyntagen til sund fornuft.

For at minimere risikoen for, at din pc bliver inficeret med virus kan følgende huskeregler anvendes:

- Du må aldrig installere programmer uden at kontakte IT-koordinatoren.
- Der må aldrig være en diskette i pc´en, når den tændes.
- Du skal altid være ekstra opmærksom på anvendelsen af disketter, som har været i brug i udstyr, som ikke tilhører Svendborg Kommune.
- Afbryd aldrig virusprogrammet, når det kører.
- Afbryd aldrig pc'ens logon procedure, idet det er her virusprogrammet opdateres.

Hvis du mener, at din maskine har fået virus, skal du straks slukke den for at undgå, at virus spredes yderligere. Endvidere skal hotline kontaktes.

Herefter bør du overveje, hvordan virus er kommet ind i systemet, for på den måde at undgå fremtidige forekomster.

Det er *ikke* flovt at have fået virus på sin maskine, men det er flovt at prøve at skjule det. Du skal derfor *ikke* holde det hemmeligt!

6 Dokumentdeling og drev -anvendelse

I Svendborg Kommune råder vi over en række centrale servere. Serverne fungerer som centralt placerede pc´er, som flere brugere samtidig kan trække på og blandt andet dele data fra. Ud over at rumme alle de fælles programmer, indeholder serverne også en række fællesdrev, som er områder på serverens harddisk, hvor filer skal gemmes. Som IT-bruger har du adgang til en del af disse

drev.

Det er vigtigt, at du altid gemmer dine dokumenter og andre filer på serverne. Dermed får fremmede personer ikke kendskab til disse filer, ved eksempelvis tyveri af din pc. Samtidig skal du ikke tænke på backup, idet dette foretages centralt.

Den konkrete anvendelse af netværksdrev kan oplyses ved henvendelse til den stedlige IT-koordinator.

7 Sikkerhedskopiering

I den daglige anvendelse af din pc forventer du at have en mængde data til din rådighed. Det vil også være tilfældet i de fleste tilfælde, men det *kan* gå galt! Konsekvensen af ikke at have en sikkerhedskopi i den situation kan være, at det er umuligt at genetablere de tabte data. En mulig genetablering kan endvidere være forbundet med et uforholdsmæssigt stort tidsforbrug.

Når du gemmer dine data på de centrale servere, som nævnt under kapitel 6 ovenfor, vil der altid blive taget centrale sikkerhedskopier, og du behøver derfor ikke at være bekymret for dine data.

Husk derfor altid at gemme dine dokumenter, regneark og andre filer, på serverne, og *ikke* på din egen pc , da der ikke tages sikkerhedskopi af dette.

Såfremt du anvender en pc uden netværksadgang, skal du i samarbejde med den stedlige IT-medarbejder sikre dig backup på for eksempel disketter.

De specielle forhold, som er gældende for anvendelse af bærbare pc'er, fremgår af bilag 11.

8 Udskrivning

Som IT-bruger udskriver du ofte dokumenter, notater og lignende. Disse dokumenter kan være fortrolige, hvorfor de skal behandles med omhu. Du er ansvarlig for at behandle fortrolige udskrifter, så de ikke kommer i de forkerte hænder. Du skal derfor altid - straks efter udskrivning har fundet sted - hente dokumenter, som er udskrevet på centrale printere. Det bemærkes, at fortrolige dokumenter ikke nødvendigvis indeholder personfølsomme oplysninger, men disse skal naturligvis også sikres.

Procedurerne for makulering fremgår nedenfor.

9 Bortskaffelse af datamedier

Datamedier er alle former for medier hvorpå der kan forefindes data, eksempelvis disketter, cd-rom'er, harddiske og lignende.

Desuden omtales her procedurerne for destruktion af papir indeholdende fortrolige oplysninger.

Se evt. bilag 15.

9.1 Elektroniske datamedier

Hvis du i forbindelse med dit arbejde anvender datamedier, skal du være opmærksom på, at de data, som du anvender, kan være fortrolige.

Disketterne med fortrolige oplysninger og som ikke længere er i brug skal enten:

- formateres ved at anvende de faciliteter, som allerede findes i Windows (hvis du er i tvivl kan du kontakte hotline) eller
- kasseres. Du kan eventuelt vælge at formatere disketten først således, at alle data bliver slettet. Ellers kan kasserede disketter afleveres til IT-koordinatoren, som herefter giver disketten videre til IT-kontoret, som varetager destruktionen.

Destruktion af øvrige datamedier indeholdende forretningsdata skal ske ved aflevering til IT-koordinatoren.

9.2 Papir

Fortroligt papir til destruktion skal altid opsamles i særskilte beholdere, hvis indhold tømmes og opbevares i aflåste omgivelser indtil destruktion.

10 Distancearbejdspladser & bærbare pc´er

Ved anvendelse af bærbare pc´er og hjemme-pc´er gælder principielt de samme retningslinier, som for Svendborg Kommunes almindelige IT-arbejdspladser: Den enkelte bruger skal således sikre, at der så vidt muligt opretholdes en sikkerhed, som er på højde med den sikkerhed, som gælder stationære pc´er i kommunens vante rammer.

Derudover er der i IT-sikkerhedspolitikkens bilag 11 beskrevet en række forhold, som du som bruger skal være opmærksom på.

11 Udvikling , herunder regneark og databaser

Hvis du som bruger foretager systemudvikling i specielle værktøjer eller udarbejder regneark, databaser eller lignende er der en række forhold, som du forinden udarbejdelsen skal være specielt opmærksom på og diskutere med din chef.

De konkrete forhold fremgår af bilag 4, Retningslinier for egenudvikling samt tilhørende instruks. Forholdene angår blandt andet godkendelse, test og dokumentation.

12 Hold dig ajour om IT -sikkerhed

For at sikre, at Svendborg Kommunes IT-installation og anvendelse til stadighed er forbundet med optimal sikkerhed, er det vigtigt, at du som IT-bruger holder dig ajour om nye tiltag og forhold, der har betydning for IT-sikkerheden.

I den forbindelse vil det altid være muligt at få et overblik over gældende regler og ændringer ved opslag på "Svendborg Nyheder".

13 Support

Hvis du har spørgsmål i forbindelse med anvendelse af din IT-arbejdsplads eller specifikke programdele er der i Svendborg Kommune oprettet en hotline-funktion, som står til din rådighed.

Som IT-bruger kan du desuden kontakte IT-koordinatoren eller Hotline, hvis du har spørgsmål eller problemer.

14 Hvis du er i tvivl ...

- eller har spørgsmål om IT-sikkerhed, kan du kontakte hotline-funktionen eller din leder.

2.1 Fysisk Sikkerhed

BILAG 2

Fysisk sikkerhed

1 Hvorfor fysisk sikkerhed

Sikkerheden i et hvert edb-system er grundlæggende afhængigt af, at kravene til den fysiske sikkerhed er opfyldt. Disse krav til fysisk sikkerhed skal sikre at edb-udstyr i Svendborg Kommune er optimalt beskyttet mod følgende risici:

1.1 Hærværk

Edb-udstyret skal fysisk være beskyttet, så en aggressors ikke har uhindret adgang til edb-udstyret.

1.2 Tyveri

Tyveri af HW og SW.

1.3 Datatyveri

Den fysiske sikring skal besværliggøre adgangen for en aggressor til Svendborg Kommunes edb-udstyr.

Sikre edb-udstyr mod skader forårsaget af vand, brand samt overophedning og lynnedslag.

Lynnedslag kan forårsage tre former for skade:

- Brandskade som en direkte følge af lynnedslaget
- Elektrisk skade fordi lynet kan følge elektriske ledninger
- Elektromagnetisk impulser som kan ødelægge computerudstyr.

Den billigste og simpleste måde at beskytte sig mod lynnedslag er ved at installere transientbeskyttelse.

2 Forsikring

Svendborg Kommune er som hovedregel selvforsikret, men nogle institutioner har dog valgt at tegne forsikringer.

3 Registrering af aktiver

Der skal føres en registrering af, hvilke aktiver Svendborg Kommune råder over, samt hvor disse aktiver er placeret. Denne registrering af aktiver er vigtig overfor kontrol-instanser.

Registreringen kan så indgå som dokumentation overfor revisionsmyndighederne i forbindelse med en eventuel særlig

revision på edb-området.

Ved skrotning af pc'er skal følgende registreres: Dato for skrotningen, maskintype, model og serienummer.

4 Licenser

Se bilag 3.2 vedr. licensforhold

5 Svendborg Kommunes HW

Svendborg Kommunes Hardware-installation kan deles op i 3.

1. Det fælles net, der er rygraden i Svendborg Kommunes edb-installation, højeste fysiske sikkerhed.
2. Forvaltningsservere, næsthøjeste fysiske sikkerhed.
3. Den enkelte PC, laveste fysiske sikkerhed.

6 Krav til fysisk sikkerhed , niveau 1 servere, "Det fælles net"

"Det fælles net" er betegnelsen for det udstyr som "binder" Svendborg Kommune sammen, som eksempel kan nævnes: Routere, switche, kabling, krydsfelter, centrale servere og eksterne netværk.
IT-chefen har ansvaret for den fysiske sikkerhed, og kan dispenserer efter en konkret vurdering dispensere fra nedenstående regler.

6.1 Anskaffelse

IT-chefen har ansvaret herfor. Anskaffelse sker i henhold til kravspecifikation og positivlisten.

6.2 Driftsansvar

Overordnet har IT-chefen driftsansvaret. I tilfælde af serviceaftaler med eksterne samarbejdspartnere er IT-chefen ansvarlig for de enkelte aftaler.

6.3 Placering af servere

Alle fællesservere skal placeres i aflåste serverrum og serverne skal være mærket tydeligt med Net-ID.

6.4 Adgangsforhold til serverrum :

Man skal være "autoriseret" af IT-chefen for at få adgang til rummet. For at blive autoriseret, skal man have et gyldigt ærinde i serverrummet, der nødvendiggør adgang til serverrummet.

Rummet skal altid være aflåst, når det ikke er "bemandet".

I rummet skal der være en UPS (nødstrømsforsyning) med den nødvendige dimensionering, der sikrer at vigtigste udstyr kan forsætte driften eller i det mindste sikre, at udstyret bliver lukket ned på en forsvarlig måde.

Der skal være køleanlæg i rummet, således temperaturen aldrig overstiger 27 grader celsius. Kølesystemet skal være "et lukket kredsløb", således støv og snavs ikke bliver cirkuleret ind i rummet. Samtidig skal der være temperaturmåler i rummet med alarmering i tilfælde af, temperaturen overstiger de 27 grader celsius.

6.5 Yderligere krav til serverrummet :

- Ingen tæpper på gulvet
- Ingen vandgennemføring
- Ingen kloak
- Væggene skal være mindst "standsende" iflg. SKAFOR's klassificering.
- Kun en adgangsdør
- Ingen vinduer
- Udstyret skal være hævet fra gulvet
- Automatisk brandslukningsudstyr og brandalarm skal forefindes i rummet.

6.6 Ved alarm

Ved alarmering pga. overophedning går der automatisk besked til IT-kontoret

Ved brandalarm går der automatisk besked til brandvæsenet

Tyverialarm skal installeres i serverrum.

Ved Tyveri-alarm går der besked til IT-kontoret.

7 Krav til fysisk sikkerhed niveau 2, Forvaltningsservere

Forvaltningsservere bruges kun af en forvaltning.

7.1 Anskaffelse

Den enkelte forvaltning har ansvaret herfor. Anskaffelse sker i henhold til kravspecifikation samt Svendborg Kommunes HW-positivliste.

7.2 Driftsansvar.

IT-kontoret har driftsansvaret. I tilfælde af serviceaftaler med eksterne samarbejdspartnere er IT-kontoret ansvarlig for de enkelte aftaler.
IT-kontoret udarbejder servicedeklarationer på de enkelte servere. Disse deklarationer skal indeholde dokumentation for serverens opbygning, mål for oppetider, svartider, servicetilkaldstider mv.

7.3 Specifikt vedr. niveau 2 servere:

7.3.1 Placering af servere.

Alle servere skal placeres i aflåste serverrum.

Man skal være "autoriseret" af IT-chefen for at få adgang til rummet. For at blive autoriseret, skal man have et gyldigt ærinde i serverrummet.

Rummet skal altid være aflåst, når det ikke er "bemandet".

I rummet skal der være en UPS (nødstrømsforsyning) med den nødvendige dimensionering, der sikre at vigtigste udstyr kan forsætte driften eller i det mindste sikre, at udstyret bliver lukket ned på en forsvarlig måde.

Der skal være køleanlæg i rummet, således temperaturen aldrig overstiger 27 grader celsius. Kølesystemet skal være "et lukket kredsløb", således støv og snavs ikke bliver cirkuleret ind i rummet. Samtidig skal der være temperaturmåler i rummet med alarmering i tilfælde af, temperaturen overstiger de 27 grader celsius.

7.3.2 Yderligere krav til serverrummet :

Ingen tæpper på gulvet
Ingen vandgennemføring
Kun en adgangsdør
Ingen vinduer
Udstyret skal være hævet fra gulvet

IT-chefen kan efter en konkret vurdering dispenserer fra kravene i forbindelse med niveau 2 severe.

8 Generelt vedr. administration af servere

9 PC'ere

9.1 Adgangsforhold :

Skal være placeret i et bemandet område, hvis der ikke er personale I området, skal området være aflåst.
Pc'ere i særligt udsatte områder, kan evt. fastgøres for at besværliggøre evt. tyveri.

Alle Pc’ere skal mærkes med godkendte tyverisikringsmærkater

9.2 Bærbart udstyr

9.2.1 Anskaffelse

Den enkelte forvaltning har ansvaret herfor. Anskaffelse sker i henhold til Svendborg Kommunes HW-positivliste.

9.2.2 Driftsansvar

IT-kontoret har driftsansvaret. I tilfælde af serviceaftaler med

eksterne samarbejdspartnere er IT-kontoret ansvarlig for de enkelte aftaler.

Se bilag 11 for yderligere retningslinier.

9.3 Hjemme PC'ere

9.3.1 Anskaffelse

Den enkelte forvaltning har ansvaret herfor. Anskaffelse sker i henhold til Svendborg Kommunes HW-positivliste.

9.3.2 Driftsansvar

IT-kontoret har driftsansvaret. I tilfælde af serviceaftaler med eksterne samarbejdspartnere er IT-kontoret ansvarlig for de enkelte aftaler.

Se bilag 11 for yderligere retningslinier.

10 Krav til Kvaliteten af døre og låse

Foreningen SKAFOR (Dansk Forening for skadesforsikring) har en klassificerings-skala for, hvor sikker en given fysisk sikkerhedsforanstaltning (døre, låse, gitre m.m.) er.

Alle døre og låse til serverrum skal som minimum opfylde kravene i Svendborg Kommunes sikringspolitik. Kontakt risiko-koordinatoren i tvivlstilfælde.

11 Bortskaffelse af datamedier

Papir med personoplysninger skal makuleres, så man ikke efterfølgende kan se indholdet.

Disketter, bånd og CD'ere med fortrolige oplysninger skal destrueres efter forskrifterne I bilag 15 Bortskaffelse af datamedier

- 1 -Krav til de enkelte fysiske installationer i skematisk form

Installations-type	Niveau	Låst til rum	Tyveri alarm	Brandalarm	Brandslukningsudstyr	Køleanlæg	UPS	Ansvar	Andet
Kablingkobber i jord	Ex	-	-	-	-	-	-	Edb-chefen	Overvågningsudstyr
Kablingfiber i	Ex	-	-	-	-	-	-	Edb-kont	Overvåg-

jord								oret	nings udstyr
Kabelskabe	Ex	***	*	*	*	*	*	Edb-kontoret	
Kabling	"In house"	-	-	-	-	-	-	Forvaltningen	
Kabelskabe	"In house"	***	*	*	*	-	-	Forvaltningen	
Servere	Ekstra aflåst rum	***	***	***	***	***	***	Edb-chefen	Det fælles net
Central t Back Up TSM	Sikret aflåst rum	***	***	***	***	***	***	Edb-chefen	Meget høj sikkerhed kræves
Forvaltningsservere	Aflåst rum	***	***	***	***	*	*	Forvaltningen	Forvalt-nings-servere
Firewall	Aflåst rum	***	***	***	***	***	***	Edb-chefen	
Andet udstyr		***	***	***	***	***	***	Edb-chefen	Routere, switches, m.m.

*** angiver et ufravigeligt krav
* intet krav, men anbefales

Installations-type	Niveau	Lås til rum	Tyverialarm	Brandalarm	Brandslukningsudstyr	Køleanlæg	UPS	Ansvar	Andet
Kabling/kobber i jord	Ex	-	-	-	-	-	-	Edb-chefer	Overvågnings udstyr
Kabling/fiber i jord	Ex	-	-	-	-	-	-	Edb-kontoret	Overvågnings udstyr
Kabelskabe	Ex	***	*	*	*	*	*	Edb-kontoret	
Kabling	In house	-	-	-	-	-	-	Forvaltningen	
Kabelskabe	In house	***	*	*	*	-	-	Forvaltningen	
Servere	Ekstra aflåst rum	***	***	***	***	***	***	Edb-chefer	Det fælles net
Centralt Back Up									
TSM	Sikret aflåst rum	***	***	***	***	***	***	Edb-chefer	Meget høj sikkerhed kræves
Forvaltnings									
servere	Aflåst rum	***	***	***	***	*	*	Forvaltningen	Forvalt ningsservere
Firewall	Aflåst rum	***	***	***	***	***	***	Edb-chefen	
Andet udstyr		***	***	***	***	***	***	Edb-chefen	Routere, switches, m.m.

Krav til de PC'er og PDA'er i skematisk form

Pc'er	Kontormiljø (0)	***	*	*	-	-	-	Forvaltning	
Pc'er	Pc'er med borgeradgang	***	*	*	-	-	-	Forvaltning	Fastgørelse
Bærbare Pc'er	Transportable	-	-	-	-	-	-	Forvaltning	Må kun anvendes i tjenstligøjemed
Hjemme Pc'er	Placeret hos den enkelte medarbejder	*	*	*	-	-	-	Forvaltning	Specificeres i separat afsnit
PDA'er (Håndholdte computer)	-	-	-	-	-	-	-	Forvaltning	Logisk sikkerhed

*** angiver et ufravigeligt krav
** kan evt. fraviges efter tilladelse fra den øverste sikkerhedsansvarlige
* intet krav, men anbefales

3.1 IT-sikkerhedsbestemmelser for IT -medarbejdere

Bilag 3

IT-sikkerhedsbestemmelser for IT -medarbejdere

Samtlige medarbejdere beskæftiget med driften af kommunens IT-installation samt medarbejdere fra eksterne leverandører, er underlagt nærværende retningslinier. Retningslinierne bliver ajourført af IT-chefen.

Det er den enkeltes ansvar at retningslinierne følges, og at administration, support og drift af IT-systemerne i Svendborg Kommune generelt finder sted i overensstemmelse med sund fornuft og god IT-skik. Herudover bør ovennævnte medarbejdere - når det gælder kommunens IT-anvendelse - fremstå som eksempler til efterfølgelse.

1 Fysisk sikkerhed

Samtlige centrale og decentrale medarbejdere med IT-driftsopgaver (herefter IT-medarbejdere) skal overholde og styrke den fysiske sikkerhed på IT-området, i overensstemmelse med retningslinierne i bilag 2, Retningslinier for fysisk sikkerhed. IT-medarbejderne skal således sikre, at alle tekniske installationer, som er relevante i forbindelse med IT-anvendelsen, overvåges på behørig vis således, at driftsforstyrrelser undgås.

IT-medarbejderne skal ligeledes sikre, at adgangen til IT- og serverrum overvåges således, at uvedkommende ikke opnår adgang. Dette skal blandt andet sikres ved, at dørene altid holdes lukket og låst. Adgangskontrol skal i øvrigt være i overensstemmelse med bilag 2.

2 Programanvendelse

For IT-medarbejderne gælder endvidere de samme retningslinier, som for Svendborg Kommunes øvrige medarbejdere.

Forvaltningerne skal råde over licenser til samtlige programmer, der anvendes, også programmer, som udelukkende anvendes på forsøgs- og testbasis.

IT-chefen skal råde over licenser til samtlige fælleskommunale programmer, og forvaltningerne skal ligeledes råde over alle de forvaltningsspecifikke.

3 Passwordsikkerhed

Der er krav til anvendelse af password i forbindelse med brug af Svendborg Kommunes IT-systemer.

Kravene er følgende:

1. Minimum 6 karakterer
2. Tvunget skift hver 90. dag
3. Der gemmes password 36 generationer tilbage
4. Der kan kun ændres password 1 gang om dagen

5. Der kan ske lockout ved 3 gentagne fejlagtige forsøg på logon. Tælleren nulstilles efter 30. minutter. Såfremt en bruger er blevet lockoutet etableres adgangen på ny af sikkerhedsmedarbejderen.

I nødvendigt omfang skal systemerne konfigureres til at understøtte ovenstående krav.

Der kan dog være systemer, som ikke understøtter alle krav. Punkt 1 og 2 skal dog altid opfyldes, og såfremt dette ikke muligt, skal der indhentes dispensation fra IT-chefen.

4 Virussikkerhed

IT-medarbejdere har traditionelt en stor IT-baseret kontaktflade til eksterne parter. Derfor skal man være ekstra agtpågivende ved anvendelse af filer og programmer, som er modtaget via Internet og andre elektroniske opkoblinger. IT-medarbejdere har en forpligtigelse til at være ekstra forsigtige ved altid at virusskanne indkomne filer - også selvom det umiddelbart ser risikofrit ud. Viruskontrol skal i øvrigt finde sted i overensstemmelse med bilag 1.5.

5 Udskrivning

Ved udskrivning af filer og kommandoer, som beskriver IT-sikkerhedsrelaterede aspekter, eksempel brugerdatabase, sikkerhedsmæssige opsætninger, firewall-konfiguration med videre, skal IT-medarbejdere sikre, at oplysningerne ikke bliver tilgængelige for uvedkommende.

Dette kan sikres ved, at der udelukkende anvendes printere, som er placeret i lokaler, hvor kun IT-medarbejdere har adgang. Såfremt der alligevel anvendes en almindeligt tilgængelig printer, skal printet straks fjernes således, at det ikke bliver tilgængeligt for uvedkommende.

Placering af printere i øvrige sikkerhedsklasser skal ske således, at uvedkommende ikke har adgang til uddata. Behandlingen af uddata er desuden beskrevet i bilag 1, Retningslinier for IT-brugere i Svendborg Kommune.

6 IT-drift

Medarbejdere, som er beskæftiget med at holde Svendborg Kommunes IT-systemer i drift, har ansvaret for, at systemer og relaterede data, altid er tilgængelige for kommunens medarbejdere. Samtidig skal medarbejderne sikre, at Svendborg Kommunes data er struktureret således, at der skabes mulighed for en opdeling, som er baseret på medarbejdernes afdelingstilknytning eller andre specifikke ansættelsesforhold.

IT-medarbejdere skal sikre, at data og systemer ikke er tilgængelige for uvedkommende. Dette skal iværksættes ved hjælp af en anerkendt filtrering, som udelukker ikke autoriserede IT-brugere.

Filtrering i forhold til Internet finder sted via en firewall, som administreres af IT-kontoret. Retningslinier for administration af firewall fremgår af bilag 7.

For at opnå stabil drift af systemerne og samtidig sikre uafhængighed af enkelte IT-medarbejdere, skal der udarbejdes:

- Driftsplaner for servere, herunder sikkerhedskopiering,

batchkørsler, almindelig administration og service af hardware og software
- Driftsplaner for netværk, herunder overvågning, performancetest, brugeradministration, generel administration og service af hardware og software
- Driftsplaner for øvrigt udstyr, herunder printere, pc´er og andet. Procedurerne skal blandt andet indeholde et generelt overblik over antal, placering, bruger og konfiguration
- Der skal føres logbog over uregelmæssigheder i IT-driften således, at historikken kan komme Svendborg Kommune til gavn ved gentagelse af eventuelle uhensigtsmæssigheder

Driftsplanerne skal med passende intervaller tilpasses de systemer, som Svendborg Kommune anvender. IT-chefen er ansvarlig for - og skal sikre - at der til enhver tid foreligger ajourførte driftsplaner for alle Svendborg Kommunes IT-driftsmiljøer.

Retningslinier for sikkerhedskopiering fremgår af bilag 10.

7 IT-support

For at afvikle en tilfredsstillende IT-support er der oprettet en central hotline-funktion, hvor det er muligt at træffe en IT-medarbejder på telefon indenfor Svendborg Kommunes normale kontortid.

Der ydes kun support til pc-arbejdspladser, som overholder Svendborg Kommunes standard, som er defineret i hardware- og softwarepositivlister. Ved anvendelse af alternative programmer og applikationer kan hotline samt IT-medarbejdere afstå fra at yde support, idet der kun ved godkendelse fra IT-chefen må ændres på standardkonfigurationen.

8 Systemudvikling

De IT-medarbejdere og øvrige medarbejdere, som er beskæftiget med simpel udvikling, skal overholde de retningslinier som er beskrevet i bilag 4 vedrørende systemudvikling i Svendborg Kommune.

9 Administratoradgang

I forbindelse med administration og support af Svendborg Kommunes IT-systemer, tildeles IT-medarbejderne forskellige administratorrettigheder. Udover systemadministrator til operativsystemer, anvendes tillige administratorrettigheder til nogle af kommunens applikationer. For at undgå misbrug er der defineret en række konkrete regler i forbindelse med tildeling og anvendelse af administratorrettigheder.

9.1 Tildeling af administratoradgang

IT-medarbejdere tildeles administratoradgang i overensstemmelse med den enkeltes dokumenterede behov i relation til administrationen af de enkelte systemer.

Da administratoradgang giver den enkelte IT-medarbejder udvidede beføjelser i forhold til Svendborg Kommunes IT-anvendelse, er der en række forhold, som den enkelte skal være opmærksom på, jf. afsnit 9.2.

Normalt skal systempasswords skiftes med jævne mellemrum. Såfremt en medarbejder, som har haft administratoradgang fratræder sin stilling, skal alle systempasswords skiftes omgående.

9.2 Anvendelse af administratoradgang

IT-medarbejdere skal sikre, at uvedkommende ikke opnår administratoradgang.

Når administratoradgangen ikke anvendes, skal der altid være logget af systemet således, at risikoen for fejl og uhensigtsmæssigheder i systemerne minimeres.

Heller ikke IT-chefen, eller andre chefer, må kende administrator-passwords - med mindre der er tale om systemer, som vedkommende selv administrerer. I stedet skal alle systempasswords, opbevares i en forseglet kuvert i et datasikkerhedsskab eller bankboks. Dermed kan kommunens øvrige medarbejdere/eksterne konsulenter opnå administratoradgang til systemerne, hvis de(n) daglige administrator(er) er indisponible. IT-chefen skal med jævne mellemrum kontrollere, om seglet er brudt.

9.3 Eksterne administratorbrugere

Alle eksterne brugere som har adgang tilSvendborg Kommunes IT-systemer, skal underskrive samme brugerklæring som ansatte i Svendborg Kommune.

I forbindelse med support fra systemleverandører skal det tilstræbes, at de udelukkende tildeles administratoradgang til den relevante applikation.

Hvis det er netoperativsystemet, som skal serviceres, bør de anvendte passwords ændres i det pågældende tidsrum således, at udenforstående ikke opnår kendskab til Svendborg Kommunes generelle passwordstruktur.

I et vist omfang har Svendborg Kommune tegnet serviceaftaler med eksterne leverandører, som bevirker, at leverandørerne har permanent fjernadgang til Svendborg Kommunes driftsmiljø. I den forbindelse er det vigtigt, at der føres kontrol med adgangen, jf. bilag 6, afsnit 1.4.

9.4 Bærbare pc'er og hjemmearbejdspladser

Som det er beskrevet i bilag 13 og 11, gælder principielt de samme retningslinier som for Svendborg Kommunes almindelige pc-arbejdspladser.

Da IT-medarbejdere har administratorrettigheder i de forskellige systemer, skal der vises ekstra agtpågivenhed ved anvendelse af disse rettigheder fra bærbare pc'er og hjemmearbejdspladser.

4.1 IT-sikkerhedsbestemmelser i forbindelse med egenudvikling

bilag 4.

IT-sikkerhedsbestemmelser i forbindelse med egenudvikling

Svendborg Kommune anvender mange forskellige systemer, og foretager i den forbindelse egenudvikling på forskellige niveauer.

Hos Svendborg Kommune finder der nogen systemudvikling sted, når eksempelvis Notes eller fagspecifikke systemer skal tilrettes og udvikles.

Med etablering af pc-miljøer får flere slutbrugere værktøjer, som muliggør såkaldt "low-level" systemudvikling via regneark, pc-databaser og database-browsere.

Hvis det udviklede produkt leverer data eller beregninger, som anvendes i beslutningsprocessen eller i øvrigt af en væsentlig del af en forretningsgang, skal det overholde en række formelle procedurer. Dels skal opbygningen kunne dokumenteres, men det skal ligeledes kvalitetsikres, således at resultatet er i overenstemmelse med de opstillede rammer.

1 Krav til "moder-data"

Integritet i databasen vil sige at indholdet til enhver tid er fuldstændigt. En mangel på integritet kan være til stede, hvis der arbejdes på kopier af databasen, som ikke bliver opdateret før der arbejdes på en ny kopi et andet sted. Udgangspunktet skal altid være Svendborg Kommunes officielle "moderdatabase", som er placeret på de centrale servere.

De medarbejdere, som er impliceret i udviklingsarbejdet, skal også være opmærksomme på funktioner, som skaber samkøring af registre.

Endvidere afgør typen af de registrerede data, hvilke lovpligtige sikkerhedsforanstaltninger: Log, adgangsbegrænsning med videre, der skal være til stede.

2 Vurderinger

Der skal foretages en vurdering af væsentligheden i et slutbrugerværktøj, herunder systemets volumen og omfang.

De kvalitative udviklingsforanstaltninger er vigtige og derfor skal systemdokumentation såvel som brugerdokumentation være udarbejdet, hvis slutbrugerværktøjet vurderes som værende kritisk for selskabets drift.

Nøglepersoner bør undgås ved at sprede viden i arbejdsgrupper/afdelinger.

1 Kvalitetssikring

- Tilfredsstillende dokumentation
- Opretholdes et tilfredsstillende sikkerhedsniveau

- Udarbejde brugermanualer (hvor det skønnes nødvendigt)
- Varetage en overordnet kvalitetssikring.

Overholdelsen af disse kriterier skal blandt andet være til gavn i forbindelse med kontrol, vedligeholdelse eller videreudvikling.

1.1. Udvikling

Instrukser for udvikling er en kvalitetssikring, idet et struktureret udviklingsforløb altid vil være nemmere at styre.

1.2. Dokumentation

Dokumentationen skal medvirke til eliminering af nøglepersonproblematikken.

Dokumentationen skal så vidt muligt være opdelt i system- og brugerdokumentation.

1.3. Kontrol

Før systemet tages i brug, skal det sikres at de funktionelle, driftmæssige og sikkerhedsmæssige krav er overholdt.

Det bedste bevis for en sikker funktion fås ved at lave en systemmæssigt krævende aftestning.

1.4. Kvalitet

Kvaliteten i slutproduktet er meget vigtig. Ringe brugervenlighed, ventetid, uklarheder og andre irritationsmomenter er med til at øge risikoen for fejlbetjening.

1.5. Sikkerhed

Den ansvarlige bør ved sin kvalitetskontrol være opmærksom på, om der optræder registre med oplysninger af følsom karakter, eller om der er tale om samkøring. Hvis dette er tilfældet, skal der udarbejdes forskrifter i henhold til Dataloven.

Derudover skal det påses, at der i produktet er taget hensyn til de øvrige forhold omfattet af Svendborg Kommunes IT-sikkerhedspolitik.

4.0 Godkendelsesproces

For at sikre kvaliteten af den udviklede software, er det vigtigt at man har en formaliseret godkendelse procedure, så kvaliteten af den udviklede software opfylder den valgte standard.

5.1 IT-sikkerhedsbestemmelserslinier for brugerautorisation

Bilag 5

IT-sikkerhedsbestemmelser for brugerautorisation

Retningslinier for brugerautorisation har til formål at sikre, at alle brugere af Svendborg Kommunes IT-systemer og data har de nødvendige rettigheder, som kræves til løsning af opgaverne. Samtidig skal det sikres, at ingen brugere har rettigheder til systemerne, som ikke er arbejds- og opgavemæssigt begrundede.

Administrationen af administratorers rettigheder til IT-systemerne fremgår af bilag 3, Retningslinier for IT-driftsmedarbejdere.

Retningslinierne er opdelt i 6 kapitler, hvor de første fem beskriver forretningsgangene for brugerautorisationer. Kapitel seks beskriver opfølgningen på, om procedurerne administreres efter hensigten.

Nedenstående forretningsgange gælder samtlige systemer og data, som anvendes til opgaveløsningen i Svendborg Kommune.

1 Generelt

Alle autorisationer skal være dokumenteret.

Alle henvendelser vedrørende brugeres rettigheder til Svendborg Kommune systemer og data skal således ske via elektronisk autorisationsblanket.

Herpå angives, om der er tale om en oprettelse, ændring, sletning eller flytning. "Oprettelse" eller "Sletning" afkrydses, hvor der er tale om oprettelser eller sletninger *til* systemer, hvorimod ændringer af rettigheder *i* systemer angives via afkrydsning i "Ændring". Såfremt en medarbejder foretager intern rokering til en anden funktion i Svendborg Kommune afkrydses "Flytning".

Samtlige autorisationer skal dels godkendes af brugerens nærmeste overordnede og dels godkendes af dataejer. Godkendelsen skal være entydig og sporbar.

Der kan dog til generelle systemer være tale om engangsgodkendelser, hvor faste autorisationer tilknyttes faste arbejdsfunktioner. Her vil det ikke være nødvendigt med dataejers godkendelse i hvert enkelt tilfælde.

Dataejer skal i forbindelse med godkendelse af adgange forholde sig til, om adgangen er arbejdsmæssigt og legitimt begrundet. Der skal vurderes på relevansen af den ønskede adgang, herunder skelnes mellem rettigheder til at læse, rette, oprette og slette. Ydermere skal det vurderes, om tildelingen af adgang medfører, at der samtidig tildeles øvrig adgang, som ikke er hensigtsmæssig og som indebærer en yderligere risiko. Dette kan eksempelvis være tilfældet ved tildeling i form af systempuljer.

Den tekniske oprettelse foretages af systemernes administratorer, som kvitterer for oprettelsen på autorisationsblanketten.

Af hensyn til varetagelse af en hensigtsmæssig funktionsadskillelse skal minimum godkendelse og oprettelse være fordelt på forskellige personer. Den der godkender må ikke samtidig have mulighed for at foretage selve autorisationen i systemet.

Alle autorisationsblanketter skal af hensyn til senere opfølgning arkiveres så længe, brugeren er ansat i Svendborg Kommune, og tillige 1 år efter fratrædelsen. Arkivering sker i cpr-nummerorden. Ved intern rokering sendes autorisationsblanketter til brugerens nye ansættelsessted.

2 Oprettelse

Når en medarbejder første gang skal autoriseres til et eller flere systemer er der tale om en oprettelse.

På autorisationsblanketten angives, hvilket system eller systemer brugeren skal have adgang til. Tillige angives hvilke profiler eller rettigheder brugeren skal tildeles.

"Andet" angiver særlige systemer, som ikke anvendes generelt i Svendborg Kommune. For disse systemer skal systemnavnet anføres.

Brugeren tildeles ved oprettelsen et éngangspassword, som brugeren skal ændre straks efter ibrugtagelsen.

3 Ændring

Proceduren skal anvendes når en medarbejder skal have ændret eller ajourført rettighederne til et eller flere systemer, som medarbejderen allerede har rettigheder til.

Dette skal tillige ske ved anvendelse af autorisationsskemaet med angivelse af, at der er tale om en ændring.

Tillige afkrydses eller anføres det pågældende system, og der angives hvilke profiler eller adgange, der skal oprettes og / eller slettes.

Der kan være tale om en generel ændring i adgangen til et system, som berører flere brugere. I disse tilfælde godkender dataejer én gang for ændringerne, hvorefter de iværksættes på alle berørte brugere.

4 Intern rokering

Der kan være tale om, at en medarbejder skifter fra én funktion i Svendborg Kommune til en anden.

Efter sidste arbejdsdag i den tidligere funktion slettes alle rettigheder, som knytter sig til det hidtidige ansættelsesforhold. Procedurerne for sletning følges.

Derefter tildeles brugeren adgang til de systemer og data, som er påkrævet for løsning af de nye arbejdsopgaver. Procedurerne for oprettelse følges.

5 Sletning

Når en fratrædelse bliver kendt skal den fratrådte medarbejders adgang til systemer og netressourcer straks lukkes. Udfra en konkret vurdering i hvert enkelt tilfælde, kan adgangen genåbnes indtil endelig fratrædelse finder sted.

For at sikre gennemførelse af forretningsgangen, skal brugerens nærmeste overordnede altid orientere de stedlige IT-medarbejdere, når en opsigelse fra en IT-bruger er modtaget eller en afskedigelse effektueret.

6 Opfølgning på autorisationer

6.1 Generelt

Minimum 1 gang om året skal der ske en total gennemgang af autoriserede brugere i det pågældende system.

Formålet er, at registrere og derefter få slettet eventuelle brugere, som ikke længere er ansat i den pågældende funktion, men hvor brugeren endnu ikke er blevet slettet.

Kontrollen foretages af administratorerne af rettigheder i de enkelte systemer.

6.2 Administratorer af rettigheder

De medarbejdere, som foretager den tekniske autorisation til IT-systemerne har tillige adgang til at tildele sig selv adgang til systemerne.

Der skal således tages særlige forholdsregler for denne type medarbejdere således, at det sikres, at administratorer til stadighed udelukkende har adgange til systemer og data, som er arbejdsmæssigt begrundet.

Konkret skal der minimum 1 gang om året ske en kontrol af administratorers adgang til systemerne.

Kontrollen foretages af administratorens nærmeste overordnede i linieorganisationen.

6.1 IT-sikkerhedsbestemmelser for logning system - og dataanvendelsen

Bilag 6

IT-sikkerhedsbestemmelser for logning system - og dataanvendelsen

Retningslinier for logning af system- og dataanvendelsen har til formål at føre kontrol med, om det sikkerhedsniveau for logisk adgangskontrol Svendborg Kommune har valgt i IT-systemerne, eventuelt forsøges kompromitteret. Tillige føres kontrol med den systemmæssige drift af hensyn til driftsstabiliteten. Forretningsgangene for adgangskontrol er beskrevet i bilag **5**.

Logning skal medvirke til at sikre en hensigtsmæssig og betryggende anvendelse af IT-systemerne. Blandt andet opdages hændelige fejl, medarbejderne beskyttes mod uberettiget mistanke om svig, uregelmæssigheder i system- og dataanvendelsen registreres, der defineres en entydig ansvarsplacering etc.

Dette bilag indeholder retningslinier for interne kontroller i systemerne, hvorimod manuelle interne kontroller beskrives i instrukser eller forretningsgange for det enkelte system eller område.

Retningslinierne er opdelt i to dele. Første del fastsætter rammerne for definition af et konkret logningsniveau for de enkelte systemer. Anden del fastsætter rammerne for gennemgang af logningsmateriale samt afrapportering af resultatet.

De konkrete forretningsgange for kontrol i de enkelte systemer beskrives i uddybende instrukser for de enkelte systemer.

1 Logningsniveau

Niveauet for logning skal generelt defineres ud fra en vurdering af de enkelte data og systemers væsentlighed for opgaveløsningen. Desuden skal man ved vurderingen forholde sig til risikoen for uhensigtsmæssig anvendelse af systemer og data.

For systemer indeholdende et særskilt sikkerhedssystem skal alle tilgængelige faciliteter vurderes og som udgangspunkt implementeres. Der skal dog tages hensyn til omfanget af logningen samt systemernes hastighed.

Logningsmaterialet skal som minimum omfatte hvem (brugerens initialer), hvornår (tidspunkt) og hvad (biblioteksti og/eller fil og/eller kartotek).

1.1 Netværksoperativsystemer samt Notes

Der skal via systemernes indbyggede sikkerhedssystemer føres

kontrol med brugernes adgang eller forsøg på adgang til systemer og data. Fokus skal være på nægtet adgang, hvor brugeren har forsøgt adgang til systemer og data, som brugeren ikke er autoriseret til.

Logningen opdeles administrativt i to dele:

- Del 1 omfatter kontrol med IT-driften, hvor der fokuseres på den centrale sikkerhed og performance i systemet. Denne del defineres af IT-afdelingen.
- Del 2 omfatter kontrol med anvendelsen af system og data. Denne del varetages af dataejer.

1.2 Fælleskommunale systemer fra Kommunedata

Ansvaret for gennemgang af logningsmateriale er placeret hos dataejerne for de pågældende systemer.

Tilrettelæggelsen af kontrol med anvendelsen af Kommunedata's fælleskommunale systemer skal defineres i uddybende instrukser. Dataejer har den udførende rolle.

1.3 Brugersystemer

Logning af anvendelsen af Svendborg Kommunes data og systemer skal i det omfang det er muligt ske via applikationernes indbyggede sikkerhedssystemer.

I tilfælde, hvor der ikke er et særskilt sikkerhedssystem til rådighed, skal logningen ske via netværksoperativsystemet.

Afhængigt af den enkelte applikations væsentlighed kan der være behov for logning af hændelser direkte i databaserne. Ændringer i væsentlige kartoteker/felter skal være undergivet en konstant logning.

Desuden skal lovgivningens krav til logning af personfølsomme oplysninger overholdes. Logningen skal som minimum være i overensstemmelse med Dataloven.

Dataejer har ansvaret for definition af ovenstående, mens selve den tekniske opsætning og varetagelse foretages via de stedlige IT-medarbejdere.

1.4 Eksterne leverandører

Der kan være behov for, at eksterne leverandører eller andre samarbejdspartnere skal have mulighed for support af Svendborg Kommunes IT-systemer. Der kan blandt andet være tale om online-support fra en ekstern lokation.

I alle tilfælde skal der føres kontrol med leverandørers adgang til, samt handlinger i, de pågældende systemer. Ved anvendelse af online-support skal der tillige foretages logning via det anvendte kommunikationsudstyr.

I øvrigt henvises der til bilag **3**, Retningslinier for IT-driftsmedarbejdere, afsnit 8.3 vedrørende eksterne administratorbrugere.

Dataejer har ansvaret for definition af ovenstående, mens selve den tekniske opsætning og varetagelse foretages via de stedlige IT-medarbejdere.

2 Gennemgang af logs samt afrapportering

2.1 Gennemgang

2.1.1 Generelt

Ansvaret for gennemgang af logningsmateriale følger ansvaret for definition af logningsniveau, jævnfør ovenfor.

Undtaget er dog del 1 i afsnit 1.1, idet gennemgangen af dette er placeret hos de stedlige IT-medarbejdere, som håndterer driften af systemerne.

Der kan optræde poster i logningsmaterialet, som kræver nærmere undersøgelse. I nødvendigt omfang tages kontakt til brugeren eller andre relevante parter for afklaring.

2.1.1 Administratorer

Administratorer af de enkelte systemer kan have adgang til manipulation med logningsmateriale. Der skal således i nødvendigt omfang ske begrænsning i denne mulighed. Gennemgang af administratorens handlinger - både i egenskaben af administrator og som almindelig bruger - skal ske af administratorens nærmeste overordnede i linieorganisationen.

2.1 Afrapportering

Afrapportering af resultatet af gennemgangen af logningsmateriale skal ske til IT-sikkerhedsfunktionen og lederen, som skal vurdere eventuelle nødvendige tiltag.

2.2 Arkivering

Logningsmateriale samt dokumentation for gennemgang og afrapportering skal arkiveres i minimum 1 år således, at der blandt andet er mulighed for at følge tendenser og mønstre samt foretage opfølgning.

7.1 Administration af Svendborg Kommunes firewall

Bilag 7

Administration af Svendborg Kommunes firewall

For at sikre Svendborg Kommunes interne sikre netværk mod uautoriseret adgang fra eksterne netværk, herunder Internet, skal der være etableret en sikkerhedsløsning i form af en anerkendt firewall til filtrering af trafikken imellem Svendborg Kommunes netværk og omverdenen.

Det er vigtigt, at der er faste forretningsgange for administration af kommunens sikkerhedsløsning. Dette begrundes med, at der er tale om et meget dynamisk miljø, hvor der løbende opstår nye risici, som kræver konstant opmærksomhed. Samtidig optræder der et modsætningsforhold, idet man dels ønsker et sikkert internt netværk, men samtidig ønsker at have mulighed for ekstern kommunikation.

Svendborg Kommunes faktiske opfyldelse og tilrettelæggelse af nedenstående dokumenteres i instrukser, hvor eventuelle skriftlige aftaler med leverandører kan indgå.

IT-chefen har ansvaret for, at procedurerne bliver iværksat og følges.

1 Kontakt med leverandører

Ved kontakt mellem Svendborg Kommune og samarbejdspartnere angående sikkerhedsløsningen skal der skabes sikkerhed for, at de enkelte medarbejdere hos begge parter, er dem, de giver sig ud for at være. Dette kan eksempelvis ske ved forevisning af ID eller oplysning om kodeord.

Al e-mail kommunikation mellem Svendborg Kommune og leverandøren skal være krypteret og signeret.

Support fra leverandører kan enten ske via fremmøde i kommunen eller via fjernadgang og fjernstyring fra ekstern lokation. Leverandørens fjernadgang til sikkerhedsløsningen skal ske via en krypteret forbindelse.

Kravene anført i bilag 3, Retningslinier for IT-driftsmedarbejdere, afsnit 9.3 samt bilag 6, Retningslinier for af logning af system- og dataanvendelsen, afsnit 1.4, skal overholdes.

2 Konfiguration af sikkerhedsløsningen

Filtreringen i kommunens sikkerhedsløsning skal være en afvejning af sikkerhed og funktionalitet. Der skal således være adgang til det nødvendige, men omvendt være lukket for det sikkerhedsmæssigt uforsvarlige. Som udgangspunkt skal al trafik være lukket medmindre, det er eksplicit godkendt af IT-chefen.

Ændringer og justeringer i opsætningen foretages af administratorerne.

Det skal sikres, at ændringer kun finder sted i forbindelse med en

præcis kravspecifikation. Ved udformning af kravspecifikation kan leverandøren inddrages i en sikkerhedsmæssig vurdering.

Der skal opbevares dokumentation for opsætning samt dokumentation for alle ændringer i opsætningen, som er beskrevet i dette bilags kapitel 4.

2.1 Anvendelse

Svendborg Kommunes sikkerhedsløsning skal være dedikeret til formålet. Dette indebærer, at der ikke må afvikles services på udstyret, som er irrelevante for sikkerhedsløsningen.

Der må ikke være oprettet andre brugere end 2 administratorer - 1 primær og 1 sekundær. Kapitel 9 i bilag 3, Retningslinier for IT-medarbejdere skal i den forbindelse overholdes.

Der kan eventuelt træffes aftale med en ekstern leverandør i forbindelse med afprøvning af den faktiske funktionalitet i sikkerhedsløsningen.

2.2 Opfølgning på konfiguration

Det skal sikres, at Svendborg Kommune til stadighed anvender opdaterede versioner af det anvendte sikkerhedssoftware. Der skal i den forbindelse træffes aftale med en kompetent leverandør om, at der kommer meddelelse fra leverandøren ved påkrævede opgraderinger eller omkonfigureringer.

Dagligt skal der foretages kontrol af, om væsentlige filer i sikkerhedsløsningen er blevet ændret. Såfremt der er sket ændringer, skal de være dokumenteret i form af en kravspecifikation.

Minimum 1 gang om måneden foretager IT-chefen en vurdering og kontrol af, at sikkerhedsløsningen har den ønskede filtrering, og at filtreringen hverken er for åben eller for lukket.

3 Overvågning af sikkerhedsløsningen

Der skal i sikkerhedsløsningen være installeret konstant overvågning, som blandt andet giver mulighed for registrering og derefter nærmere undersøgelse af tvivlsom aktivitet.

Sikkerhedsløsningen skal overvåges med udgangspunkt i en fast plan. Uregelmæssigheder i driften skal fremgå af en driftshåndbog, som ikke må være tilgængelig for uvedkommende.

Den aktuelle aktivitet i sikkerhedsløsningen monitoreres.

Sikkerhedsløsningen skal endvidere have indbygget en alarmfunktionalitet, som sikrer, at administrator straks orienteres ved særligt kritiske aktiviteter. Alarmmeddelelser skal ske automatisk i form af e-mail, SMS eller lignende, som giver mulighed for øjeblikkelig reaktion. I nødvendigt omfang tager administrator kontakt til IT-chefen eller andre relevante parter. Kontaktprocedurerne fremgår af særskilt instruks.

Ved driftsstop skal sikkerhedsløsningen automatisk lukke for trafikken imellem Svendborg Kommune og omverdenen - såkaldt “closed on failure” funktionalitet.

3.1 Logning af anvendelsen

Sikkerhedsløsningen skal overvåges systematisk med regelmæssige mellemrum - mindst en gang om ugen. Ud over den aktuelle realtime overvågning, skal der systematisk indsamles og behandles logmateriale. Loggen skal sikre et overblik over de aktiviteter, der er sket i sikkerhedsløsningen den forgangne uge.

Det konkrete logningsniveau fastlægges i samarbejde med leverandøren af sikkerhedsløsningen.

For at sikre muligheden for indsamling af information om aktivitet i sikkerhedsløsningen, skal der allokeres tilstrækkelig diskplads til, at der bliver opbevaret logoplysninger i mindst 1 måned. Dermed har Svendborg Kommune mulighed for at lokalisere angrebsmønstre og andre tilbagevendende uregelmæssigheder i adgangen til Svendborg Kommunes netværk.

Desuden kan der efter behov udtrækkes logoplysninger til særlige datamedier i form af tapes, optiske diske eller lignende.

4 Dokumentation

Det skal sikres, at al dokumentation vedrørende sikkerhedsløsningen udarbejdes og ajourføres samt opbevares på et sikkert sted. Dokumentationen skal have en fast defineret struktur og opbygning, som gør det muligt for personer med et basalt teknisk kendskab at tolke materialet.

Der skal opbevares dokumentation for følgende elementer:

- Dokumentation for udgangspunktet for opsætningen - kravspecifikation
- Dokumentation for den faktiske opsætning
- Dokumentation for ændringer i opsætningen
- Dokumentation for logning
- Driftshåndbog

8.1 IT-sikkerhedsbestemmelser for anvendelse af e -post

Bilag 8

IT-sikkerhedsbestemmelser for anvendelse e -post

Dette dokument har til formål at beskrive, hvordan medarbejdere i Svendborg Kommune, som anvender e-post via kommunens udstyr og e-postadresser, skal agere.

Retningslinierne er opdelt i 4 områder:

- Anvendelse af e-post
- Rettigheder til e-post
- Håndtering af e-post ved fratrædelse
- Anvendelse af e-post overfor eksterne parter

1 Anvendelse af e -post

Som medarbejder i Svendborg Kommune skal det tilstræbes, at man åbner og gennemgår sin e-post dagligt.

Officiel e-post vil normalt blive fremsendt til Svendborg Kommunes officielle e-post adresser. Alligevel bør der tages forholdsregler, som sikrer, at e-post behandles ved ansattes fravær:

- Det skal altid være muligt for minimum én kollega at åbne en anden kollegas e-post.
- Derudover kan du etablere automatisk svar funktion således, at afsender informeres om fraværet samt forventet svardato, eller man kan videresende al e-post til Svendborg Kommunes officielle e-postkasse.

Udveksling af personlige e-postadresser med samarbejdspartnere kan ske efter behov, hvor kommunikation via e-post er en naturlig kommunikationsform. Se dog afsnit 1.3 samt kapitel 4.

1.1 Officielle e-postadresser

Svendborg Kommune har en række fælles og personlige e-postadresser, som er offentliggjort. De pågældende e-postkasser administreres af de respektive enheder / personer.

1.2 Håndtering

Som det gælder med den øvrige korrespondance, herunder papirpost og telefonsamtaler, skal den enkelte medarbejdert vurdere den enkelte e-post og overveje håndteringen individuelt.

Såfremt der er tale om e-post, som er relateret til en konkret sag, skal denne gemmes, arkiveres og journaliseres sammen med de øvrige sagsakter. Dette giver mulighed for at genfinde de indlæg, som har indgået i sagsbehandlingen. Arkivering og journalisering skal finde sted i overenstemmelse med retningslinierne på området og være enten elektronisk eller i papirform. Det er sagsbehandlerens ansvar, at dette sker.

Ovenstående håndtering gælder både ind- og udgående e-post.

1.3 Hvad sendes via e-post

Hvilke dokumenter, der må sendes via e-post, skal aftales indenfor de enkelte fagområder. Det er forvaltningsdirektøren/afdelingslederen, der har ansvar for, at der træffes aftale med de enkelte samarbejdspartnere om, hvilke informationer, der kan udveksles via e-post. Det er vigtigt, at afdelingerne sammen med IT-kontoret sørger for at e-mail med fortrolige oplysninger bliver sendt krypteret.

1.3.1 Besvarelse af indgående post

E-post i sager, som kræver underskrift fra afsenderen, returneres med anmodning om fremsendelse i papirbaseret form.

Der skal altid snarest muligt ske besvarelse af modtaget e-post - og senest efter forvaltningslovens regler. E-post anses for modtaget, når den er modtaget på e-postserveren. Kan der ikke gives et konkret svar, sendes der til afsenderen en kvittering for modtagelsen, hvori der anføres den forventede videre sagsbehandling. Også her skal ovenstående arkivering og journalisering overholdes.

Hvis den enkelte medarbejder modtager e-post, som ikke er korrekt adresseret, skal den videresendes til rette modtager. Såfremt rette modtager ikke er kendt skal e-posten returneres til afsender med en bemærkning om forkert adressat.

1.3.2 Udgående post

Udgående post, herunder besvarelse af henvendelser, som modtages via e-post, må som udgangspunkt gerne ske via e-post, men du skal i hvert enkelt tilfælde vurdere og overveje håndteringen individuelt. Det kan være, at karakteren af e-posten gør, at et papirbaseret afsendelse er det rigtige. Dette gælder blandt andet hvor dokumentation for modtagelsen er relevant for den modtagende part eller hvor modtageren skal anvende

dokumentet i andre sammenhænge.

Korrespondance, som er fortrolig eller indeholder følsomme oplysninger må ikke ske via almindelig e-post, men skal finde sted via papirbaseret post eventuelt som krypteret elektronisk post.

1.4 Beskyttelse imod virus

Såfremt der er vedlagt filer på en e-post, skal filerne scannes for virus, inden de åbnes eller eksekveres, og inden de gemmes på egen harddisk eller på serveren. Retningslinier for håndtering i forbindelse med beskyttelse imod virus, fremgår af bilag 1.5.

1.5 Sletning af e-post

E-post bliver normalt ikke slettet fra systemet uden forudgående aftale.

Den enkelte kan slette e-post efter behov. Dog skal retninglinier i forbindelse med arkivering og journalisering, overholdes.

2 Rettigheder til e-post

2.1 Privat anvendelse

Medarbejdere i Svendborg Kommune må i begrænset omfang anvende e-post til privat korrespondance. Anvendelsen kan sidestilles med anvendelse af almindelig telefoni, som også i begrænset omfang, kan finde sted til private samtaler.

E-post og vedhæftede filer, som opbevares på Svendborg Kommunes post-server, tilhører i princippet Svendborg Kommune. Dette gælder også e-post mærket "fortroligt", "privat" og lignende. Såfremt du opretter en mappe med titlen "privat", vil e-post, der opbevares her, under normale omstændigheder ikke blive læst af andre. Det skal dog præciseres, at administrator til enhver tid har adgang til alle e-post, som opbevares på Svendborg Kommunes post-server, også selvom adgangen er beskyttet med et password. Dette kan være tilfældet af hensyn til systemets sikkerhed, sygefravær og lignende.

Medarbejderen vil dog blive orienteret, såfremt det har været nødvendigt at læse e-post i medarbejderens e-postkasse.

Du må ikke uden tilladelse gøre dig bekendt med indholdet af andre medarbejderes private e-post og vedhæftede filer.

2.2 Sikring af privat e-post

Der vil ikke blive etableret særlige sikkerhedsforanstaltninger i forbindelse med e-post i private mapper. Det skal derfor præciseres, at Svendborg Kommune ikke er erstatningspligtig overfor medarbejdere, hvis e-post i private mapper eller private e-post adresselister - ved et uheld - bortkommer. Det er den enkeltes eget ansvar at sikre privat e-post og private e-post adresselister.

3 Håndtering af e-post ved fratrædelse

3.1 Oprydning

Ved fratrædelse, skal medarbejderen selv indsamle de private e-post oplysninger, som vedkommende ønsker at beholde,

herunder arkiveret e-post fra privat-mappen og private e-post adresseoplysninger fra den private adresseliste.

Dagen efter den reelle sidste arbejdsdag i Svendborg Kommune vil e-post og adresseoplysninger ikke længere være tilgængelige. Dette gælder også selvom det ikke er sidste officelle ansættelsesdag.

E-post, som ikke er privat og som ikke er gemt i privat mappen, er Svendborg Kommunes ejendom og må ikke medbringes ved fratrædelse.

E-post stilles herefter til rådighed for forvaltningsledelsen.

3.2 Nedlæggelse af brugeren

Når en bruger er fratrådt og har haft sin sidste arbejdsdag vil adgang, til Svendborg Kommunes IT-systemer og teknologiske infrastruktur, blive lukket via sletning af brugeren.

3.3 Efterfølgende e-post

E-post til en fratrådt medarbejder, som modtages af Svendborg Kommunes post-server efter sidste arbejdsdag, vil blive returneret til afsender med bemærkning om, at brugeren ikke længere optræder i systemet.

4 Anvendelse af e-post overfor eksterne parter

4.1 Aftaleforhold

Såfremt korrespondance imellem Svendborg Kommune og en ekstern samarbejdspartner primært baseres på e-post, skal der indgås aftale om hvilke informationer, som er omfattet og hvilke informationer, som ikke kan formidles via e-post.

Endvidere skal sådanne samarbejdspartnere være orienteret om Svendborg Kommunes retningslinier for anvendelse af e-post således, at samarbejdspartneren kan forholde sig til Svendborg Kommunes håndtering af e-post.

Som nævnt i afsnit 1.3 skal der træffes aftale imellem den pågældende samarbejdspartner og det enkelte fagområde om hvilke dokumenter, der må sendes via e-post.

9.1 IT-sikkerhedsbestemmelser for anvendelse af Internet

Bilag 9

IT-sikkerhedsbestemmelser for anvendelse af Internet

Dette dokument har til formål at beskrive, hvordan medarbejdere i Svendborg Kommune, som anvender Internet via kommunens udstyr, skal agere.

1 Anvendelse

Som medarbejder i Svendborg Kommune skal du anvende internettet til arbejdsmæssige formål i den udstrækning, det er hensigtsmæssigt i forhold til de opgaver du skal løse.

Du må anvende internettet i begrænset omfang til private formål i arbejdstiden. Anvendelsen kan sidestilles
med muligheden for at telefonere og benytte e-post til private formål i arbejdstiden, jfr. bilag 8.

Udenfor arbejdstiden må du anvende internettet i ubegrænset omfang.

Generelt skal du altid agere efter almindelig god IT-skik.

Dette bevirker, at du blandt andet under ingen omstændigheder må foretage ændringer i det anvendte programmel, som kan medføre en forringelse af sikkerheden.

Når du bevæger dig rundt på Internet skal du være opmærksom på opretholdelsen af en net-etikette, idet du repræsenterer Svendborg Kommune. Dette gælder dog kun din anvendelse i arbejdstiden.

Internettet må kun anvendes til lovlig formål, der ikke krænker dansk lovgivning. Dette inkluderer bl. a. brugen af materiale, der er copyright på.

2 Registrering af anvendelsen

Generelt foretages der ikke kontrol af Svendborg Kommunes medarbejderes anvendelse af Internet.

Af sikkerhedsmæssige årsager, for eksempel virus, kan anvendelsen dog blive registreret. Endvidere vil det ske ved mistanke om en kriminel handling samt i tilfælde, hvor det kan konstateres, at der er sket brud på sikkerhedsbestemmelserne.

3 Download af filer

Ved besøg på hjemmesider kan der være mulighed for at downloade diverse nyttige filer og småprogrammer.

Der må kun downloades filer til arbejdsmæssigt brug - også selvom du er flexet ud. Begrundelsen herfor er, at der blandt andet

kan være risiko for virus og andre sikkerhedsmæssige brister. I den forbindelse henvises til Retningslinier for IT-brugere i Svendborg Kommune, bilag 1 afsnit 5.

Du må således kun downloade filer fra virksomheder, organisationer og lignende, som du stoler på.

Det bemærkes, at der kun må installeres programmer efter aftale med IT-kontoret.

10.1 Sikkerhedskopiering af data

Bilag 10

Sikkerhedskopiering af data

1 Hvilke data der skal sikkerhedskopieres

Det er dataejernes ansvar at specificere, hvilke data der skal tages back up af, samt angive hvor hyppigt dataene skal sikkerhedskopieres.

2 TSM

Sikkerhedskopierede data kan som standard genskabes 5 generationer tilbage, ved sletning gemmes 2 seneste versioner i 60 dage. Efter 60 dage gemmes 1 version i 365 dage.
Alle kommunes Lotus Notes postkasser gemmes i fulde versioner i 14 dage.

Dog skal lovens krav til opbevaring af logfiler og lign. altid overholdes.

Svendborg Kommune anvender et centralt Backup program (TSM) der via netværket henter data ind fra Svendborg Kommunes servere hver nat. De sikkerhedskopierede data gemmes på bånd, både i Svendborg kommune båndrobot i kælderen, Ramsherred 5 og på en OFF-site kopi (Yderligere en båndrobot) som står hos PPR, Ramsherred 12.

TSM tager backup af Svendborg Kommune's Servere, en aktuel liste over hvilke Servere der tages Backup af via TSM kan ses på serveren.

TSM tager Backup af ændrede og nye data hver nat.

TSM anvender to båndrobotter, hvor den står Ramsherred 5, mens den andet står i en helt anden bygning, Ramsherred 12.

Hjertet i TSM er TSM`s database. Den tages der backup af hver dag med en kopi på begge båndstationer.

Log filer gennemgåes hver dag.

2.1 Driftsansvar.

TSM's drift IT-chefens ansvar.

2.2 Adgangsforhold:

Kun autoriseret personale har adgang til TSM.

Adgangsdøre og låse til TSM-rummet skal opfylde SKAFOR's røde klasse

Der er installeret tyverialarm.

Ved alarm går der automatisk besked til IT-vagten samt til alarmcentralen.

Rummet skal indeholde UPS med den nødvendige dimensionering, der sikrer at TSM kan forsætte driften og sikre en sikker nedlukning af TSM.

Der skal være **køleanlæg** i rummet, således temperaturen aldrig overstiger 27 grader celcius. Kølesystemet skal være "et lukket kredsløb", således støv og snavs ikke bliver cirkuleret ind i rummet. Samtidig skal der være **temperaturmåler** i rummet med alarmering i tilfælde at temperaturen overstiger de 27 grader celcius.

TSM-rummet skal sikres mod indtrængen af vand. Udover den fysisk sikring af rummet mod indtrængende vand, skal TSM-rummet også udstyres med fugtfølsomme sensorer, der er tilkoblet alarmanlægget.

Automatisk Brandslukningsudstyr og brandalarm skal forefindes i rummet.

Ved alarmering går der automatisk besked til **Falck og IT-vagten.**

2.3 Hvor der ikke er adgang til TSM

Hvis der ikke er adgang til TSM, påhviler det Forvaltningskonsulenterne at finde en alternativ måde at lave en sikkerhedskopiering af de specificerede data.

2.4 Test af backup sæt

Det er vigtigt at teste validiteten af sikkerhedskopierne, derfor skal sikkerhedskopierne testes med jævne mellemrum. Dog skal validiteten af sikkerhedskopien testes mindst en gang hver måned.

Validitetstesten af sikkerhedskopien, gennemføres ved at restore testfiler, der er placeret på alle servere, der tages backup af. Der foretages dernæst en sammenligning mellem de restore testfiler og de oprindelige.

Hvis der er uoverensstemmelse mellem de restore filer og de oprindelige testfiler, skal der udfærdiges en rapport til IT-chefen, der redegør for, hvilke fejl der er fundet samt hvilke tiltag der er iværksat for at sikre validiteten fremover.

11.1 IT-sikkerhedsbestemmelser for anvendelse af distancearbejdspladser , herunder hjemmearbejdspladser og bærbare pc'er.

Bilag 11

IT-sikkerhedsbestemmelser for anvendelse af distancearbejdspladser , herunder hjemmearbejdspladser og bærbare pc'er .

1 Definition

En distancearbejdsplads i Svendborg Kommune består af enten

- en stationær arbejdsplads placeret uden for kommunens lokationer stillet til rådighed af kommunen med opkobling til kommunens netværk (eksempelvis en hjemmearbejdsplads) eller
- en mobil IT-arbejdsplads i form af eksempelvis en bærbar pc, en Palm Pilot og lignende håndholdt udstyr.

Som følge af, at distancearbejdspladser befinder sig uden for kommunens vante rammer, og således opbevares i et ureguleret område, stilles der udvidede / særlige krav til anvendelse og sikring heraf.

2 Sikkerhed , generelt

Ved anvendelse af distancearbejdspladser gælder principielt de samme retningslinier, som for Svendborg Kommunes øvrige IT-arbejdspladser. Du skal som bruger således sikre, at der så vidt muligt opretholdes en sikkerhed, som er på højde med den sikkerhed, som gælder stationære pc'er tilkoblet Svendborg Kommunes netværk.

Det skal dog understreges, at uhensigtsmæssig adfærd kan resultere i, at hele Svendborg Kommunes sikkerhed kan blive svækket.

Følgende forhold er således specielt vigtige ved anvendelse af en distancearbejdsplads:

- Generelt skal du altid agere efter almindelig sund fornuft.
- Du skal altid opbevare pc'en forsvarligt. Det vil blandt andet sige, at man ikke forlader sit hjem ulåst, og at bærbare pc'er ikke efterlades synligt i køretøjer eller uden opsyn.
- Du må ikke ændre på pc'ens sikkerhedsindstillinger.
- Pc'en må udelukkende anvendes af dig som medarbejder i Svendborg Kommune.
- Pc'en er forsynet med antivirussoftware, som opdateres løbende ved opkobling til Svendborg Kommunes netværk. Såfremt du anvender en pc uden netværksadgang modtager du jævnligt en opdatering fra din IT-koordinator, som skal lægges ind på pc'en.

- Kør en total virusskan på din pc med jævne mellemrum.
- Der skal altid anvendes et opstartspassword på pc'en. Bærbare pc'er, som indeholder fortrolige oplysninger, skal være forsynet med et særskilt program, som krypterer harddiskens indhold.
- Når pc'en forlades skal den sikres mod uautoriseret adgang. Dette indebærer, at hjemmearbejdspladser skal slukkes helt, og på bærbare pc'er indeholdende fortrolige oplysninger skal password til krypteringsprogram indtastes på ny.
- Du skal være opmærksom på hvilke data, du har liggende på pc'en. Opbevar kun data på pc'en, såfremt det er nødvendigt. Anvend i stedet netværket til opbevaring af data.
- Du skal overføre dokumenter, regneark og andre filer til servernes fællesdrev, så ofte det er muligt.
- Anvendelse af disketter følger retningslinierne beskrevet i kapitel 9 i Retningslinier for IT-brugere i Svendborg Kommune.

I øvrigt skal det understreges, at retningslinier for brug af Internet og e-post som beskrevet i bilag 8 og 9 også er gældende her.

3 Dataadgang

Som udgangspunkt tildeles brugere af distancearbejdspladser samme rettigheder til netværket, som de har på arbejdspladsen i kommunen.

4 Sikkerhedskopiering

Der tages dagligt sikkerhedskopi af alle data på Svendborg Kommunes centrale servere. Det er således vigtigt, at du, så ofte som muligt, lagrer arbejdsrelaterede data her.

Såfremt der anvendes en pc uden mulighed for netværksadgang skal du via disketter, så ofte som muligt, foretage en manuel kopiering af data til serverne.

5 Udskrivning

Som udgangspunkt skal alt print foretages på Svendborg Kommunes fysiske lokationer.

Såfremt det er nødvendigt kan der dog ske udprintning udenfor kommunens fysiske rammer. Her skal du dog være ekstra opmærksom på kapitel 8 og 9 i Retningslinier for IT-brugere i Svendborg Kommune.

Papir indeholdende fortrolige data må aldrig bortskaffes med det almindelige husholdningsaffald eller afleveres til genbrug, men skal makuleres.

12.1 Nødplan

Bilag 12

Nødplan

Dataejerne skal sikre, at der foreligger en vurdering af om, der skal være udarbejdet en nødplan for det pågældende system, herunder eventuelle manuale rutiner. Kravene til nødplan skal foreligge på anskaffelsestidspunktet, og dataejeren skal løbende sørge for, at nødplanen for det pågældende system stadig er aktuel.

Ved nedbrud af fællessystemer kontaktes IT-kontoret for reetablering af systemet. IT-kontoret foretager efter en vurdering af kritiske områder prioritering af reetableringen.

Ved nedbrud af forvaltningssystem kontaktes koordinatoren for den pågældende forvaltningen. Koordinatoren foretager derefter den nødvendige prioritering af reetableringen.

Der henvises i øvrigt til Svendborg Kommunes beredsskabsplan.

13 Persondataloven

1 Persondataloven

Persondataloven omhandler behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling, og for ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register. Begrebet behandling omfatter enhver form for måde at håndtere oplysninger om personer på. Som de vigtigste former for behandling kan nævnes: Indsamling, registrering, systematisering, opbevaring, brug, videregivelse, samkøring og sletning.

1.2 Oplysningstyper

Personoplysninger kan inddeles i 3 kategorier:

- Følsomme oplysninger om menneskers rent private forhold. Det drejer sig om oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold.
- Andre typer af oplysninger om rent private forhold anses også for at være følsomme. Det drejer sig om oplysninger om strafbare forhold, væsentlige sociale problemer og lignende følsomme privatlivsoplysninger, f.eks. om interne familieforhold.
- Almindelige personoplysninger kan f.eks. være identifikationsoplysninger, oplysninger om økonomiske forhold, kundeforhold eller andre lignende ikke følsomme oplysninger.

1.3 Anmeldelse af behandlinger

Anmeldelsen skal indeholde oplysninger om følgende:

- Navn og adresse på den dataansvarlige, dennes eventuelle repræsentant og på en eventuel databehandler.
- Behandlingens betegnelse og formål.
- En generel beskrivelse af behandlingen.
- En beskrivelse af kategorierne af registrerede og af de typer af oplysninger, der vedrører dem.
- Modtagere eller kategorier af modtagere, som oplysningerne kan overføres til.
- Påtænkte overførsler af oplysninger til tredjelande.
- En generel beskrivelse af de foranstaltninger, der iværksættes af hensyn til behandlingssikkerheden.
- Tidspunktet for påbegyndelsen af behandlingen.
- Tidspunktet for sletning af oplysningerne.

Anmeldelsen skal fremsendes til datatilsynet af IT-sikkerhedsfunktionen. Hvis det drejer sig om følsomme oplysninger skal datatilsynet spørges forinden anmeldelsen og efterfølgende ibrugtagning. Drejer det sig der imod om almindelige oplysninger skal der ske en anmeldelse samtidig med ibrugtagning af behandlingen. Disse anmeldelser skal i nogle tilfælde ikke sendes til registertilsynet, men indgå i en oversigt over behandlinger som anvendes i Svendborg Kommune.

Det skal sikres:

- at Svendborg Kommune orienterer den registerede om, at der indsamles oplysninger om personen,
- at den registrede kan få indsigt i oplysninger om personen,
- at den registrede har ret til at gøre indsigelser mod en behandling,
- at den registrede kan gøre indsigelse mod, at oplysninger om en selv kan videregives med henblik på markedsføring,
- at den registrede kan få oplysninger, der er urigtige eller vildledende, rettet, slettet eller blokeret,
- at den registrede har ret til at klage til datatilsynet over en behandling.

2 Oversigt over behandlinger

Forvaltningen skal forinden ibrugtagning af en ny behandling - uanset om den er elektronisk eller ikke-elektronisk - sørger for at der foreligger en anmeldelse. Det arbejde koordineres med IT-sikkerhedsfunktionen, som sikrer at der er en oversigt over alle behandlinger i Svendborg Kommune.

3 Overholdelse af reglerne

Det er dataejers ansvar, at der udarbejdes en anmeldelse for alle behandlinger. Dataejer skal udover

ovennævnte oplysninger til anmeldelsen også være med til at specificere sikkerhedsniveauet , herunder specificere hvem der må behandle personoplysninger.

Linieansvar skal sikre at de medarbejdere som behandler personoplysninger har fået den nødvendige oplæring til dette arbejde. Det kan f.eks. ske ved at anvendelse af personoplysninger foretages af en bestemt stillingskategori.

Endvidere skal det sikres at det behandlingen af personoplysningen sker i henhold til anmeldelsen .

4. Indsigt

Generel udlevering af information til og fra borgeren. På blanketter og ved anden indhentning af oplysninger skal borgeren orienteres om muligheden for at få indsigt i den konkrete behandling. Endvidere skal der - efter en konkret vurdering - gives borgeren indsigt i de oplysninger som anvendes i en behandling af en person.

5. Klageadgang

Borgeren skal orienteres om klagemuligheden over en behandling. Dette skal ske ved alle henvendelser til borgeren.

Borgeren skal orienteres om klagemuligheden til Datatilsynet over Svendborg Kommunes behandling af en indsigelse fra en borger.

14 Bortskaffelse af datamedier

Bilag 14

Bortskaffelse af datamedier

Når kommunes løsøre kasseres, vil det kunne gives til institutioner og foreninger m.v., som kommunen ifølge reglerne om kommunalfuldmagt lovligt vil kunne yde støtte.

Hvis IT-udstyr overdrages til andre institutioner indenfor Svendborg Kommune, skal det sikres, at alle data på IT-udstyret bliver slettet permanent.

IT-udstyr der ikke mere kan finde anvendelse indenfor Svendborg Kommune, skal skrottes på en miljømæssig forsvarlig måde. Endvidere skal det sikres, at alle data på det skrottet udstyr bliver slettet permanent.