FREDERIKSSUND KOMMUNE

IT-sikkerhedspolitik

INDHOLDSFORTEGNELSE:

1 Indledning
2 Formål
3 Ansvar og organisation
  3.1 Øverste sikkerhedsansvarlige
  3.2 Ansvar i organisation (systemejer)
  3.3 Systemejer
  3.4 IT-ledelse
  3.5 Opfølgning og kontrol
  3.6 Ansvar
4 Lovgivning og regelsæt
  4.1 IT-strategi
  4.2 Retningslinier for IT-brugere
  4.3 Lov om behandling af personoplysninger (Dataloven)
    4.3.1 Den registreredes indsigtsret
    4.3.2 Videregivelse
5 Dokumentation
6 Fysisk sikkerhed
  6.1 Bygningsindretning
  6.2 Adgangskontrol
  6.3 Alarmsystemer
  6.4 Registrering af aktiver / forsikring
7 Datasikkerhed
  7.1 Adgangskontrol og autorisation
  7.2 Databehandling hos servicebureauer (databehandler)
  7.3 Logning
  7.4 Sikkerhedskopiering (BackUp)
  7.5 Udskrivning
  7.6 Destruktion af data
  7.7 Datakvalitet
  7.8 Virus
8 Datakommunikation
  8.1 Netværk
  8.2 Firewall
  8.3 Hjemme- og bærbare PC
  8.4 Internet og E-mail
9 Udvikling og anskaffelse
10 Nødberedskab
11 Sanktioner
12 Udarbejdelse og ikrafttrædelse

1 Indledning

IT-anvendelsen i Frederikssund Kommune har til formål at understøtte kommunens servicemål. For at sikre IT-anvendelsen, ønsker Frederikssund Kommune, at alle medarbejdere har en sikkerhedsorienteret kultur og en bevidst holdning til begrebet IT-sikkerhed, hvor der lægges vægt på reel sikkerhed fremfor formel sikkerhed.

IT-sikkerhedspolitikken tilstræber at være:	w Realistisk w Operationel w Logisk w Acceptabel w Kontrollerbar

Frederikssund Kommunes IT-sikkerhedspolitik har udgangspunkt i kommunens IT-baserede forretningsgange, som både omfatter kontorprogrammer og fagsystemer og samtidig inkluderer netværk og IT-infrastruktur.

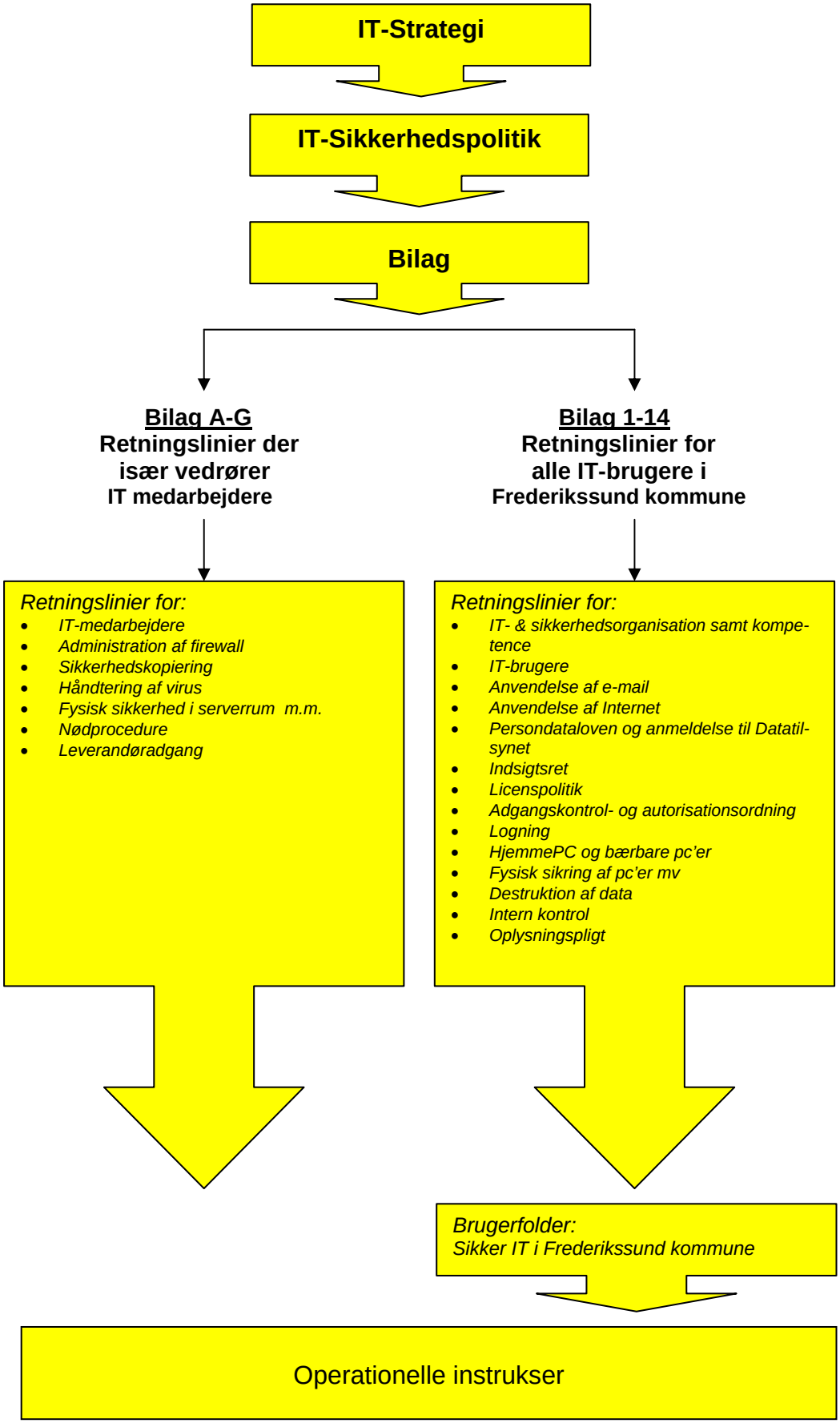
Samtidig respekterer IT-sikkerhedspolitikken de krav, som blandt andet datalovgivningen til enhver tid måtte stille til systemer og forretningsgange med personhenførbare oplysninger.

IT-sikkerhedspolitikken skaber grundlaget for, at Frederikssund Kommune også fremover kan have en visionær IT-anvendelse, der dels tilgodeser myndighedernes forventninger, dels at kommunens IT-sikkerhedsniveau muliggør en bredspektret IT-systemanvendelse. IT-sikkerhedspolitikken skal skabe rammerne for en sikker IT-anvendelse for borgere, politikere og medarbejdere i Frederikssund Kommune.

IT-sikkerhedspolitikken fastsætter hovedprincipperne for den administrative IT-sikkerhed i kommunen, herunder ansvaret for varetagelse af IT-sikkerheden. De overordnede regler uddybes i en række bilag til politikken, som det fremgår af figur på næste side.

Ændringer i IT-sikkerhedspolitikkens generelle niveau forudsætter Byrådetsgodkendelse, mens ændringer i bilagenes bestemmelser fastlægges af Chefgruppens IT-styregruppe.

IT sikkerhedspolitikken er offentlig tilgængelig. Af sikkerhedsmæssige årsager er de tilhørende bilag ikke almindeligt tilgængelige.


IT-Strategi
IT-Sikkerhedspolitik
Bilag
Bilag A-G
Retningslinier der
især vedrører
IT medarbejdere
Bilag 1-14
Retningslinier for
alle IT-brugere i
Frederikssund kommune
Retningslinier for:
IT-medarbejdere
Administration af firewall
Sikkerhedskopiering
Håndtering af virus
Fysisk sikkerhed i serverrum m.m.
Nødprocedure
Leverandøradgang
Retningslinier for:
IT- & sikkerhedsorganisation samt kompetence
IT-brugere
Anvendelse af e-mail
Anvendelse af Internet
Persondataloven og anmeldelse til Datatilsynet
Indsigtsret
Licenspolitik
Adgangskontrol- og autorisationsordning
Logning
HjemmePC og bærbare pc'er
Fysisk sikring af pc'er mv
Destruktion af data
Intern kontrol
Oplysningspligt
Brugerfolder:
Sikker IT i Frederikssund kommune
Operationelle instrukser

2 Formål

IT-sikkerhedspolitikken har til formål at sikre,

- at kommunen opfylder gældende lovgivning, herunder ar data ikke misbruges.
- at driftsikkerhed og tilgængelighed til systemer og data er til stede.
- 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 indarbejdes i daglige forretningsgange i Frederikssund Kommunes forvaltninger.
- at sikkerheden etableres på et effektivt og ensartet niveau, så risikoen for alvorlige fejl begrænses.
- at væsentlige værdier ikke går tabt.

IT-sikkerhedspolitikken skal således afspejle såvel myndighedskrav som Kommunens egne behov.

IT-sikkerhedspolitikken skal være en afvejning af væsentlighed og risiko. Sikringen skal stå mål med risikoen. Det vil sige, at Kommunen ikke vil sikre sig for enhver pris, men være bevidst om enhver risiko.

Endvidere har IT-sikkerhedspolitikken til formål, at skærpe de enkelte IT-brugeres opmærksomhed på sikkerhed i forbindelse med anvendelse af de forskellige systemer, samt sikre at alle IT-brugere er beskyttet af et entydigt regelsæt.

Frederikssund Kommunes IT-sikkerhedspolitik vedrører alle administrative brugere af kommunens IT-systemer og IT-baserede infrastruktur. Endvidere regulerer IT-sikkerhedspolitikken øvrige områder, hvor der sker systematisk databehandling, elektronisk eller manuelt.

3 Ansvar og organisation

Beskrivelse af den kommunale organisering på IT-området. Formålet er, at optimere overblik over ansvar og kompetence i forhold til IT-anvendelsen.

3.1 Øverste sikkerhedsansvarlige.

Det overordnede ansvar for Frederikssund kommunes IT-sikkerhed er placeret hos øverste sikkerhedsansvarlige, som er borgmesteren. Den administrative opgave er via Kommunaldirektøren delegeret til Social- og IT-direktøren.

Det daglige sikkerhedsarbejde varetages af IT-chefen og medarbejderne i IT-afdelingen. For en række specialsystemers vedkommende og forvaltningsområder varetages sikkerhedsarbejdet desuden af lokale "sikkerhedsansvarlige".

3.2 Ansvar i organisationen

Ansvaret for overholdelse af IT-sikkerhedspolitikken følger kommunens organisatoriske opbygning. Forvaltningscheferne er dermed ansvarlige for IT-sikkerheden i de respektive systemer, som løser konkrete opgaver indenfor de pågældendes ansvarsområder.

Herudover har Frederikssund kommune en række medarbejdere, som er ansvarlige for delelementer i IT-sikkerheden. Skemaet i afsnit 3.6 beskriver disse ansvarsforhold.

IT- og sikkerhedsorganisering samt kompetence, er mere detaljeret beskrevet i bilag 1

3.3 Systemejer

Et gennemgående begreb i Frederikssund kommunes IT-sikkerhedspolitik er systemejer. For alle væsentlige, definerbare systemer identificeres en systemejer, som den der har ansvaret for, at der i forbindelse med anvendelsen af kommunens ***systemer*** varetages en hensigtsmæssig sikkerhed, specielt i forhold til persondataloven. Systemejeren er normalt den forvaltningschef, der er den største bruger af det pågældende system. Systemejer kan delegere ansvaret – eksempelvis til afdelingslederen.

3.4 IT-ledelse

IT-chefen skal påse, at der til stadighed er etableret forretningsgange og procedurer, som støtter overholdelsen af IT-sikkerhedspolitikken.

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

3.5 Opfølgning og kontrol

Der skal foretages løbende opfølgning af, hvorvidt reglerne i Frederikssund Kommunes

IT-sikkerhedspolitik i praksis efterleves. Varetagelsen af sikkerheden kontrolleres og revideres ud fra en konkret vurdering af væsentlighed og risiko. *Retningslinier for den interne kontrol fastsættes i* bilag 11

IT-chefen er ansvarlig for at de interne sikkerhedsforanstaltninger gennemgås én gang om året, eventuelt med ekstern bistand, med henblik på at sikre at de til stadighed afspejler de faktiske forhold.

3.6 Ansvarsområder

Placering i organisationen	**Ansvar**
Borgmester	Øverste sikkerhedsansvarlige.
Social- og IT-direktør	*Delegeret øverste sikkerhedsansvar via kommunaldirektøren.*
Forvaltningschefer	Systemejere og ansvarlige for IT-sikkerheden via brugersystemer, herunder ansvar for intern kontrol.
Chefgruppens IT-styregruppe	Skal sikre, at der altid er en organisering der varetager de sikkerhedsmæssige aspekter.
IT-chef	*Varetager dagligt IT-sikkerhedsarbejde. Ansvarlig for opfølgning og kontrol.*
IT-medarbejdere	Varetager dagligt sikkerhedsarbejde i forbindelse med kommunens IT-anvendelse, herunder tekniske driftsopgaver og support. Stillingtagen til sikkerhed i fællesskab med systemejere. Varetager autorisation til netværk.
Systemejere	Systemejere er forvaltningscheferne. Systemejere har ansvaret for et specifikt programkompleks herunder anskaffelse, driftafvikling, vedligehold, udfasning, informationsindhold og kvalitet. Stillingtagen til interne kontroller i systemet samt sikkerhed.
Lokale sikkerhedsansvarlige	Administration af brugerrettigheder / autorisation m.m. i relation til Kommunedata m.f. systemer i egen forvaltning. Sikre, at kommunens sikkerhedsprocedurer, efterleves af egen forvaltning. Rådgive egen forvaltning i IT-sikkerhedsmæssige spørgsmål. Indgår i kommunens IT-sikkerhedsberedskab og er samtidig formidler af IT-sikkerhedspolitikken.
Medarbejdere generelt	Varetagelse af IT-sikkerheden ved overholdelse af Kommunens IT-sikkerhedspolitik samt almindelig sund fornuft

4 Lovgivning og regelsæt

Frederikssund Kommunes IT-anvendelse er reguleret af en række retningslinier og regelsæt, som er med til at sikre, en høj og ensartet kvalitet.

4.1 IT-strategi

IT-sikkerhedspolitiken skal løbende tilpasses de udmeldinger vedr. sikkerhed, som indgår i Kommunens overordnede IT-strategi.

4.2 Retningslinier for IT-brugere

Den enkelte medarbejder, som i det daglige anvender en pc-arbejdsplads i Frederikssund Kommune, skal introduceres til brugerrelaterede bilag 1-14 samt brugerfolderen "Sikker IT i Frederikssund Kommune" som har udgangspunkt i disse bilag.

Udover praktiske oplysninger om anvendelse af programmer, hardware, sikkerhedsprocedurer og lignende, beskriver retningslinierne ligeledes den enkelte medarbejders ansvar som IT-bruger.

Da IT-anvendelsen følger den generelle teknologiske udvikling, vil bilagene med jævne mellemrum blive ajourført.

4.3 Lov om behandling af personoplysninger (Dataloven)

Dataloven har til formål at sikre følsomme data imod misbrug.

Forvaltningscheferne ("systemejer" – se afsnit 3.3) har ansvaret for, at kravene i Dataloven overholdes. Endvidere har forvaltningscheferne ansvaret for, at IT-chefen er orienteret i forbindelse med oprettelse af nye lokale datasamlinger, der indeholder data af en karakter, hvor Dataloven er gældende jfr. Bilag 5.

IT-chefen har ansvaret for, at yde bistand til forvaltningerne samt for at vedligeholde oversigter over Frederikssund Kommunes anmeldelser.
Anmeldelse af behandlinger til Datatilsynet er forvaltningschefernes ansvar.

4.3.1 Den registreredes indsigtsret / oplysningspligt

For at opfylde Datalovens krav om registreredes indsigt, føres en central liste / oversigt over alle systematiserede personhenførbare informationer. Oversigten skal sikre, at det er muligt, at informere borgerne om, hvor registrering kan være foretaget.

Den centrale oversigt vedligeholdes af IT-chef. Borgmesterkontoret koordinerer behandling af henvendelser om indsigt.

”Retningslinier for håndtering af den registreredes indsigtsret samt oversigt over systemer der indeholder personoplysninger” er lagt ind på bilag 6. ”Retningslinier for håndtering af oplysningspligt samt samkøring i kontroløjemed” er lagt på bilag 14.

4.3.2 Videregivelse

Personhenførbare informationer må kun videregives i henhold til Dataloven. Såfremt der opstår tvivl om videregivelsens relevans, træffer forvaltningscheferne beslutning.

5 Dokumentation

Mål:	Dokumentation af systemer og forretningsgange skal sikre, at en almindelige IT-kyndig kan skabe sig tilstrækkelig indsigt i konstruktioner og procedurer til at kunne videreføre systemerne *i henhold til IT-sikkerheden.*

For alle væsentlige systemer og IT-relaterede forretningsgange skal der foretages en vurdering af behovet for dokumentation af virkemåde, procedurer med videre.

Systemejer er ansvar for (i samarbejde med IT-chef), at denne vurdering foretages og at evt. dokumentation bliver udarbejdet.

Dette gælder såvel driftsopgaver som sikkerhedsadministration og teknisk opsætning. Dokumentationen har blandt andet til formål, at eliminere afhængighed af nøglepersoner. Dokumentationen skal mindst indeholde følgende emner:

- Beskrivelse af systemet eller forretningsgangens formål.
- Overordnet beskrivelse af den tekniske opsætning.
- Redegørelse for handlinger, der er nødvendige i forbindelse med systemets eller forretningsgangens drift.
- Skitsering af Frederikssund specifikke forhold i forbindelse med det pågældende system eller forretningsgang.
- Angivelse af kontaktpersoner og beskrivelse af supportaftaler.

Dokumentation skal opbevares betryggende.

6 Fysisk sikkerhed

Mål:	Den fysiske sikring af Frederikssund Kommunes IT-installation skal være i overensstemmelse med afhængigheden af IT-driften samt

	afspejle den værdi IT-udstyr og data repræsenterer.

Frederikssund Kommune ønsker at sikre de fysiske installationer mod ulykker, hærværk, tyveri og forsyningssvigt. Sikringen skal stå i et naturligt forhold til de værdier, som skal beskyttes. Kravene til sikring af centralt udstyr er således højere, end kravene til sikring af udstyr i kontormiljøerne. Derfor er centrale servere og krydsfelter omfattet af sikkerhedsklasse I, mens pc'ere, printere og øvrigt slutbrugerudstyr, som er placeret i administrationsbygningerne, er omfattet af sikkerhedsklasse II. Øvrige stationære og bærbare pc'er, herunder distancearbejdspladser og pc'er på institutioner tilhører sikkerhedsklasse III.

Sikkerhedsniveauet i sikkerhedsklasse I-III skal fastsættes i henhold til nedenstående. Detaljerede beskrivelser fremgår af bilag E, 10 og 13.

6.1 Bygningsindretning

Opbevaring af servere og andet centralt udstyr sker i særligt indrettede lokaler. Lokalerne skal indeholde de fornødne installationer og være sikret hensigtsmæssigt. Krydsfelter og netværksenheder skal behandles med tilsvarende omhu.

6.2 Adgangskontrol

Der findes procedurer som sikrer, at det kun er autoriserede medarbejdere, som har adgang til serverrum.

6.3 Alarmsystemer

Frederikssund Kommune har etableret tilstrækkelige alarmforanstaltninger på relevante bygninger og lokaler således, at eventuelle uregelmæssigheder alarmeres til døgnbemandet funktion.

6.4 Registrering af aktiver/forsikring

Der skal foretages en registrering af samtlige hardware- og softwareenheder, som repræsenterer en væsentlig værdi. Licensforhold med videre styres i IT-afdelingen Registreringen har til formål, at danne et overblik over Kommunens IT-mæssige aktiver, herunder licensforhold.

Der må ikke afvikles programmer, uden at der er behørig dokumentation for licensforhold, jfr. afsnit vedrørende licenser i bilag 7.

Forsikring af systemer og hardware til sikring af Kommunens IT-infrastruktur, følger Frederikssund Kommunes almindelige regler vedrørende forsikring af aktiver. Kommunens risikostyringskoordinator har ansvaret.

7 Datasikkerhed

Mål:	Det skal sikres, at data som anvendes i Frederikssund Kommunes forretningsgange, til enhver tid har en tilstrækkelig høj kvalitet. Det er kun autoriserede brugere, der har adgang til Frederikssund Kommunes interne 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 Frederikssund Kommunes IT-systemer repræsenterer en væsentlig værdi, ligesom der kan være tale om fortrolige oplysninger. Disse værdier skal sikres mod uautoriseret adgang og imod tab og forvanskning.

Forvaltningscheferne skal derfor i fællesskab med IT-chef fastsætte et sikkerhedsniveau, som er i overensstemmelse med de værdier der skal sikres, og samtidig gøre det muligt for brugerne, at opnå en fornuftig anvendelse af systemet.

Fastsættelse af sikkerhedsniveauet skal ske i henhold til nedenstående.

7.1 Adgang og autorisation

Kun personer med tjenestelig behov kan få adgang til Frederikssund Kommunens interne IT-systemer herunder data. De samme retningslinier er gældende i forhold til de fælleskommunale systemer på Kommunedata og CSC.

Forvaltningscheferne / IT-chef eller delegeret er ansvarlig for at definere, hvilke systemer eller informationer, Kommunens medarbejdere, borgere og andre skal have adgang til.

IT-chefen har ansvaret for, at vedligeholde retningslinier for tildeling, ændring og sletning af brugeradgang / autorisationer.

Retningslinier fremgår af bilag 8.

7.2 Databehandling hos servicebureauer (databehandler)

Inden igangsætning af behandling af personoplysninger af en databehandler (f.eks. Kommunedata og CSC) på Frederikssund Kommune / Det Fælles Skattesamarbejdes

vegne, skal der foreligge skriftlig aftale, om at behandlingen ved databehandleren sker efter reglerne i persondataloven og sikkerhedsbekendtgørelse.

7.3 Logning

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

Bestemmelserne er ligeledes gældende for databehandlere f.eks. Kommunedata og CSC.

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

Procedure omkring logning er beskrevet i bilag 9.

7.4 Sikkerhedskopiering

Der skal foretages sikkerhedskopiering (backup), som gemmes efter nærmere fastsatte regler og procedure – se bilag B.

For hvert enkelt system skal der tages stilling til frekvensen i forbindelse med sikkerhedskopiering, og hvordan sikkerhedskopierne skal opbevares. Der skal for hvert system foretages en teknisk afprøvning af kopieringsrutinerne, herunder kontrol af genetableringsprocedurerne på dataniveau, mindst en gang om året, eller i forbindelse med omlægning af rutinerne.

Procedurer for sikkerhedskopiering og reetablering skal beskrives således, at procedurerne til enhver kan udføres af relevante medarbejdere i IT-afdelingen.

IT-afdelingen har det overordnede ansvar for den daglige backup af alle Frederikssund Kommunens servere.

7.5 Udskrivning

Ved udskrivning fra kommunens systemer skal det sikres, at oplysningerne ikke bliver tilgængelige for uvedkommende.

Dette sikres ved, at der udelukkende anvendes printere, som er placeret i lokaler hvor kun autoriserede medarbejdere har adgang. Såfremt der alligevel anvendes en almindelig tilgængelig printer, skal printet straks fjernes således, at det ikke bliver tilgængeligt for uvedkommende. Se bilag E / 13.

7.6 Destruktion af data

Bortskaffelse af data skal finde sted under betryggende forhold. Hvis der er tale om personhenførbare data eller andre former for følsomme data, skal det sikres, at data ikke bliver tilgængelige for uvedkommende. Uanset om data gemmes på manuelle eller elektroniske medier, er retningslinierne gældende.

Til sikring af, at destruktion finder sted under betryggende forhold, skal elektroniske databærende medier overdrages til IT-afdelingen, der varetager den videre behandling.

Retninglinier for destruktion af databærende medier er uddybende beskrevet i bilag 12.

7.7 Datakvalitet

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

For hvert system skal der tages stilling til, hvilke interne kontroller, der skal udføres i forbindelse med databehandlingen, og hvem der er ansvarlig herfor. Forvaltningscheferne (systemejer) er ansvarlig for at procedurerne iværksættes.

For egenudviklede systemer skal der foreligge dokumentation for konstruktion og virkemåde, dels for at sikre brugernes anvendelse af systemet og dels af hensyn til mulighederne for at kunne videreudvikle systemet. Dette gælder også for systemer, som Kommunen har fået specialudviklet hos en leverandør.

7.8 Virus

Frederikssund Kommune har etableret sikkerhedsprocedurer, som beskytter IT-systemerne imod virusangreb. Dette finder sted, dels ved hjælp af fornuftige værktøjer til at imødegå aktuelle risici, dels ved at motivere de enkelte IT-brugere til varetagelse af god edb-skik. Se i øvrigt bilag 2 (IT-brugere) og bilag C (Virus).

IT-afdelingen sikrer, at alle relevante enheder, servere og pc arbejdspladser i kommunen til enhver tid, er opdateret med den nyeste version af det anvendte antivirusprogram.

8 Datakommunikation

Mål:	Der skal stilles et netværk til rådighed således, at alle Kommunens IT-brugere kan opnå hurtig og sikker adgang til netressourcer. Samtidig skal det sikres, at uvedkommende ikke kan opnå adgang til Frederikssund Kommunes IT-systemer.

Fastsættelse af sikkerhedsniveauet skal ske i henhold til nedenstående.

8.1 Netværk

IT-afdelingen er ansvarlig for opbygning og vedligeholdelse af Kommunens netværk.

Alle eksterne kommunikationsforbindelser skal godkendes af IT-afdelingen, som vedligeholder oversigter over netværk og datakommunikation.

I forbindelse med pc'er, som er tilkoblet Frederikssund Kommunes netværk, må der ikke anvendes modemforbindelser, med mindre der gives tilladelse af IT-afdelingen.

8.2 Firewall

"Indgangsdørene" til Frederikssund Kommunes netværk skal være sikret således, at det kun er autoriserede IT-brugere som kan opnå adgang.

IT-afdelingen er ansvarlig for administration og håndtering af firewall - se bilag A.

8.3 Hjemme- og bærbare PC'er.

Der må kun etableres eksterne kommunikationsforbindelser, når der er truffet særlige foranstaltninger for sikring af, at uvedkommende ikke kan få adgang til personoplysninger. Det er ikke tilladt at sende personfølsomme oplysninger eller fortrolige oplysninger via E-post uden for Frederikssund kommunens lukkede netværk.

Se eDag2: "Send sikkert til Frederikssund Kommune med digital signatur"

Der skal foreligge nærmere retningslinier for brugen af Hjemme- og bærbare PC – se bilag 10.

8.4. Internet og e-mail

Politikere og en række medarbejdere i Frederikssund kommune har adgang til anvendelse af Internet. Der er en række sikkerhedsrelaterede forhold, som IT-brugeren skal være opmærksom på i denne sammenhæng. Disse forhold er nærmere beskrevet i bilag 3 og bilag 4 "Retningslinier for anvendelse af Internet og e-mail" på Frederikssund Kommunes udstyr.

9 Udvikling og anskaffelse

Mål:	At sikre, at de systemer der udvikles / anskaffes og vedligeholdes, er pålidelige og effektive.

Ved indkøb af helt nye systemer skal IT-afdelingen altid involveres fra begyndelsen. IT-afdelingen vil i samarbejde med den indkøbende forvaltning vælge det bedst tænkelige system for at sikre, at systemet har de nødvendige snitflader til kommunens øvrige systemer.

Se Kommunens "Generelle principper for anskaffelse eller udskiftning af IT-udstyr og programmer".

10 Nødberedskab

Mål:	At sikre, at væsentlige forretningsgange og opgaver, indenfor en given tidsperiode, kan videreføres i prioriteret og kontrolleret rækkefølge.

Kommunen skal fortsat kunne betjene borgerne, selv om der skulle ske beskadigelse / ødelæggelse af oplysninger.

I medfør af kommunens nødprocedurer tages sikkerhedskopier af alle data jfr. afsnit 7.4. – bilag B.

Der skal foretages en vurdering af, hvorvidt anvendelsen af de enkelte IT-systemet er en så kritisk faktor for den kommunale administration, at der skal etableres et egentligt nødberedskab. Systemejer (se pkt. 3.3) har ansvaret for, at foretage en vurdering af forretningsgangene i forhold til afhængigheden af IT-systemerne, idet et eventuelt behov for nødberedskab fastlægges i samarbejde med IT-afdelingen.

Der er udarbejdet interne retningslinier vedrørende nødprocedurer jfr. bilag F
I øvrigt henvises til Kommunens beredskabsplan.

11 Sanktioner

Ansvaret for at efterleve sikkerheden omkring Frederikssund Kommunes IT-anvendelse, er placeret hos den enkelte medarbejder. Det skal derfor fremhæves, at overtrædelse af IT-sikkerhedspolitikken samt relaterede bilag, efter omstændighederne, kan medføre ansættelsesmæssige konsekvenser.

12 Udarbejdelse og ikrafttrædelse

IT-sikkerhedspolitikken er godkendt af byrådet den 24.6.2003 og træder i kraft samme dag.