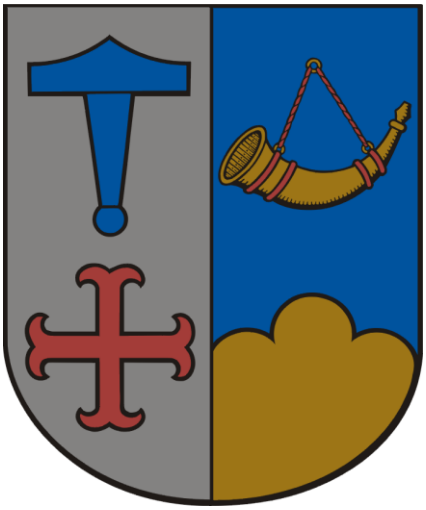
Politik for Informationssikkerhed



Ishøj Kommune

2007

Indholdsfortegnelse

Indledning

Denne politik for informationssikkerhed beskriver de vedtagne krav til beskyttelsen af kommunens informationer og definerer de overordnede principper for organisering af informations-sikkerhedsarbejdet. Dokumentet er opdelt i 2 hovedafsnit:

1. Overordnet politik for informationssikkerhed
2. Generelle sikkerhedsbestemmelser for informationsbehandling

Det første afsnit begrunder og forklarer kommunens behov for informationssikkerhed, og definerer hvor og hvornår politikken for informationssikkerhed gælder. Desuden beskriver den overordnede politik, hvorledes ansvar og opgaver omkring sikkerheden er placeret, og hvorledes sikkerhedsbrud skal håndteres. Den overordnede politik er opdelt i følgende afsnit:

- **Kommunens forretningsmæssige behov for informationssikkerhed**
- **Øvrige overordnede krav til informationssikkerheden, herunder love og aftaler**
- **Hvilke områder er dækket af informationssikkerhedspolitikken**
- **Informationssikkerhedens prioritering i forhold til andre forhold**
- **Informationssikkerhedsfunktionernes organisatoriske placering**

Det andet afsnit indeholder de generelle bestemmelser for informationssikkerheden, som gælder overalt i kommunen, uanset om man arbejder på rådhuset, på et af kommunens driftssteder, eller fra en politiker/hjemmearbejdsplads. De generelle sikkerhedsbestemmelser er opdelt i følgende afsnit:

- **Hvad er informationssikkerhed**
- **Klassifikation af kommunens informationer**
- **Definition af sikkerhedsområder**
- **Roller omkring informationssikkerheden**
- **Generelle regler for behandling af informationer**
- **Informationssikkerhedsorganisationen**

Som foreskrevet i Persondataloven, skal der ikke skelnes mellem informationer der er lagret på papir, og informationer der er lagret på elektroniske medier. Derfor er det vigtigt at pointere, at politikkens bestemmelser gælder al information – ikke kun den information der behandles eller lagres elektronisk.

Til politikken for informationssikkerhed hører følgende bilag:

- Bilag 1. Oversigt over fysiske- og elektroniske registre

- Bilag 2. Definition af informationssikkerhedsområder
- Bilag 3. Informationssikkerhedsorganisationen

Både politikken og dens bilag publiceres på kommunens Intranet, hvor bilagene løbende ajourføres af den særlige informationssikkerhedsmedarbejder.

Politikken for informationssikkerhed udmøntes i praktiske foranstaltninger, regler og procedurer, som tilrettelægges af den særlige informationssikkerhedsmedarbejder, og er dokumenteret i et separat dokument, *Specifikke IT-sikkerhedsbestemmelser*, som vedligeholdes af IT-center.

1. Overordnet politik for informationssikkerhed

1.1 Kommunens forretningsmæssige behov for informationssikkerhed

Borgerne har krav på, at persondata behandles forsvarligt, og at alle administrative informationsressourcer beskyttes mod tab, forvanskning og misbrug.

Kommunen har ansvaret for informationsbehandlingen på en række områder, med forskellige krav til sikkerheden. I visse tilfælde handler det om følsomme, personrelaterede informationer, mens det andre steder drejer sig om informationer, der i princippet er offentlige. Når informationerne behandles i centre og driftssteder, vil risikoen for misbrug være afhængig af de aktuelle sikkerhedstrusler i det pågældende arbejdsmiljø. Det betyder, at regler og sikkerhedsforanstaltninger både må tilpasses de informationer, der skal beskyttes og de anvendelsessituationer der forekommer.

Valget af sikkerhedsniveau skal foretages på baggrund af en klassificering af informationerne og anvendelsessituationerne, som er udtrykt i Kapitel 2: Generelle sikkerhedsbestemmelser for informationsbehandling.

1.2 Øvrige overordnede krav til informationssikkerheden, herunder love og aftaler

Kommunen skal bl.a. opfylde de krav som stilles i persondatalovgivningen, forvaltningslovgivningen, regnskabslovgivningen, samt øvrige gældende love og interne/eksterne regler.

Endvidere skal informationsbehandlingen opfylde de specifikke aftaler, som regulerer kommunens samarbejde med leverandører af services, produkter og ophavsretligt beskyttede værker.

1.3 Hvilke områder er dækket af informationssikkerhedspolitikken

Den overordnede politik for informationssikkerhed gælder alle steder, hvor kommunens informationer opbevares, anvendes eller behandles.

Desuden gælder politikken hos samarbejdspartnere, der opbevarer, anvender eller behandler informationer efter aftale med kommunen.

Sikkerhedspolitikken gælder således også for service- og systemleverandører, rådhuset, driftssteder, politiker/hjemmearbejdspladser, mobile enheder m.m.

1.4 Informationssikkerhedens prioritering i forhold til andre forhold

De regler og foranstaltninger, som fastsættes i henhold til den overordnede politik for informationssikkerhed, kan kun fraviges, hvis den øverste IT-sikkerhedsansvarlige har tilladt eller beordret det.

Det betyder, at informationssikkerheden altid har første prioritet, med mindre specifikke situationer gør det nødvendigt at fravige regler i overensstemmelse med den øverste ledelses beslutning.

1.5 Informationssikkerhedsfunktionernes organisatoriske placering

Kommunaldirektøren har det overordnede ansvar for informationssikkerheden, og kan bemyndige chefer i organisationen til, at udarbejde sikkerhedsforskrifter for de enkelte områder, inden for de rammer, der er udtrykt i de generelle sikkerhedsbestemmelser for informationsbehandling, og til at træffe beslutninger omkring behandlingen af informationssikkerhedsbrud.

De anvendte IT-systemer skal være godkendt af den øverste sikkerhedsansvarlige til de opgaver, de anvendes til at støtte. Det betyder, at systemernes sikkerheds-mæssige funktioner skal opfylde kommunens og lovgivningens krav om adgangskontrol, logning mm.

Der skal defineres ejerskab for alle informationer, baseret på de primære processer, hvori de indgår. Det er informationsejerens ansvar, at klassificere informationerne efter deres følsomhed og værdi, samt at sikre, at det administrative ansvar for informationssikkerheden er klart defineret.

Chefen for et center kan udpege lokale informationssikkerhedsmedarbejdere i sin organisation, som bemyndiges til at administrere lokale sikkerhedsforanstaltninger og påse at regler og procedurer efterleves.

IT-center kan være udførende i administration af informationssikkerheden i henhold til interne aftaler, men det formelle ansvar for informationssikkerheden er altid placeret i linieorganisationen, og aftaler med IT-centeret skal være dokumenteret skriftligt.

1.6 De overordnede krav til håndtering af informationssikkerhedsbrud og uheld

Overholdelsen af regler og procedurer påhviler chefen for det pågældende center eller lederen af det pågældende driftssted. Chefen kan udpege én eller flere medarbejdere i sin organisation som lokale informationssikkerhedsmedarbejdere, der har til opgave at rapportere alle tegn på mulige sikkerhedsbrud til den øverste ansvarlige for informationssikkerheden, eller til den ledende medarbejder, som er bemyndiget til at træffe beslutninger vedrørende informationssikkerheden i det pågældende sikkerhedsområde (center, driftssted eller del heraf, ifølge afsnit 2.3 Definition af sikkerhedsområder).

Teknisk overvågning foretages af den lokale informationssikkerhedsmedarbejder, suppleret af IT-center, hvor der foreligger en aftale herom.

Den særlige informationssikkerhedsmedarbejder kan på tegn på mulige informationssikkerhedsbrud træffe foranstaltninger til begrænsning af sikkerhedsbruddet. Den særlige informationssikkerhedsmedarbejder rapporterer efterfølgende til den øverste sikkerhedsansvarlige samt den ledende medarbejder vedrørende informationssikkerheden i det pågældende sikkerhedsområde.

Den særlige informationssikkerhedsmedarbejder skal sørge for, at der til enhver tid foreligger detaljerede skriftlige planer for håndtering af informationssikkerhedsbrud og tekniske uheld, og alle involverede personer i informationssikkerhedsorganisationen og linieorganisationen skal være bekendt med deres pligter og opgaver i forbindelse med sådanne hændelser.

Revision af informationssikkerheden skal foretages af en uvildig part (f.eks. konsulent eller revisor). Denne vurdering skal gennemføres mindst én gang årligt og omfatter en gennemgang af de aktuelle IT-sikkerhedsforanstaltningers effektivitet, samt en vurdering af sikkerhedsforanstaltningernes tilstrækkelighed i forhold til det aktuelle trusselsbillede.

2. Generelle sikkerhedsbestemmelser for informationsbehandling

2.1 Hvad er informationssikkerhed

Formålet med at opretholde et veldefineret sikkerhedsniveau omkring kommunens informationer er, at imødegå de forudsebare trusler, med foranstaltninger som står i et rimeligt forhold til, værdien af de informationer der skal beskyttes og understøtter en smidig og effektiv anvendelse af informationerne i forbindelse med kommunens arbejdsgange.

Informationssikkerheden opdeles her i fem egenskaber, som forklares i de efterfølgende afsnit:

- **Fortrolighed**
- **Tilgængelighed**
- **Integritet**
- ***Ægthed***
- **Uafviselighed**

2.1.1 Fortrolighed

Når informationer sikres, så de ikke kan læses af uvedkommende, taler vi om fortrolighed. Når man sætter en lås på sin dagbog eller opbevarer firmaets interne informationer i pengeskabet, forventer man, at informationerne kun kan læses af en bestemt kreds af personer, nemlig dem, som har en nøgle til låsen.

Den samme forventning har man til et IT-system, der indeholder personlige eller andre følsomme informationer.

Et lokalt system kan sikres med logiske kontroller (fx koder og passwords) - eller ved at kontrollere den fysiske adgang til anlæg, skærme, kabler osv.

Men ingen af disse metoder kan bruges til at sikre åbne netforbindelser, der fungerer som en slags offentlige transportmidler, hvor alle skal kunne være. Hvis man vil sikre sig fortrolighed i et åbent net, må man beskytte sine meddelelser med kryptering af informationerne , før de sendes af sted.

2.1.2 Tilgængelighed

Når brugeren kan finde, læse og bruge de informationer som han eller hun har retmæssig adgang til, taler vi om tilgængelighed. Det stiller krav til alle dele af systemerne, fra strømforsyning og lagringsmedier, til kommunikationsforbindelser og programmer.

For at opnå en høj tilgængelighed kan man benytte komponenter af høj kvalitet, eller man kan installere ekstra komponenter, der overtager opgaverne, hvis uheldet sætter bestemte enheder ud af drift.

Men selv hvis alle komponenter er dubleret, må man også sikre en hurtig reparationstid, så en dobbeltfejl ikke bliver katastrofal. Dette stiller krav til både organisation og logistik.

2.1.3 Integritet

Når informationer beskyttes, så de ikke ødelægges eller ændres af uvedkommende, f.eks. i et forsøg på hærværk, bedrageri o. lign. taler vi om integritet.

Ved papirdokumenter vil man ofte kunne afsløre forsøg på uberettigede ændringer ved en nærmere undersøgelse af selve papiret. Men når informationerne er repræsenteret som digitale data, vil de ofte kunne ændres, uden at det kan konstateres ved granskning af dokumentet.

Vil man sikre sig mod at data ændres uberettiget, kan det ske ved brug af matematiske teknikker (algoritmer), der f.eks. uddrager og sammenligner visse "fingeraftryk" af informationsindholdet for dermed at konstatere, om der er sket utilsigtede ændringer.

En simpel måde at beskytte integriteten på, er at anvende en checksum som elektronisk ”fingeraftryk”. Denne metode giver imidlertid kun en begrænset sandsynlighed for, at dokumentet er intakt - der er stadig en meget reel risiko for, at dokumentet kan være ændret, uden at det kan konstateres. Hvis den anvendte algoritme f.eks. er kendt af en ondsindet tredjepart, er det en smal sag for ham at ændre dokumentet, uden at det kan ses.

En bedre løsning er at benytte en digital signatur, der i princippet virker som en checksum, men er baseret på en stærkere algoritme, der matematisk ”væver” ophavsmandens nøgle ind i dokumentet og gør det meget svært at forfalske dokumentet, selv ved anvendelse af en kraftig computer.

2.1.4 Ægthed

Sikkerheden for, at en bestemt person er ophavsmand til bestemte (elektroniske) informationer, beskrives som ægthed. Det er ofte den sværeste parameter at få helt styr på, når vi taler om informationssikkerhed:

I papirets verden opnås denne sikkerhed gennem forsegling og underskrift. For digitale meddelelser kan dette kun bruges, hvor datamediet (f.eks. en CD-ROM) kun kan ændres en gang. For datamedier, der genbruges (f. eks disketter eller harddiske), eller på netværk, må man bruge andre midler.

For at skabe sikkerhed for ægtheden af digitale dokumenter kan man f. eks bruge en digital signatur. Det betyder at dokumentet er kodet med en nøgle, som er udstedt af en troværdig tredjepart. Signaturen kan altså ikke blot garantere at dokumentet er uændret (som beskrevet ovenfor under Integritet), men kan også bruges som en sikker identifikation af afsenderen.

2.1.5 Uafviselighed

Uafviselighed handler om risikoen for, at afsenderen af en digital meddelelse senere påstår, at han ikke har noget med meddelelsen at gøre. Denne egenskab er

vigtig, når man handler eller indgår aftaler elektronisk.

Et papirdokument med en personlig underskrift har traditionelt været accepteret som sikkerhed for, at afsenderen var forpligtet af dokumentets indhold. Men netop fordi underskriften er bundet til mediet (her papiret), kan denne metode ikke bruges til genbrugelige databærere, som f. eks harddiske eller på åbne netværk.

Her må man skabe en logisk sammenbinding af dokumentets indhold med afsenderens identitet (ægthed) og knytte dette til den konkrete transaktion. Det kan fx opnås ved brug af en digital signatur, hvor afsenderen med sit certifikat og password har bekræftet dokumentets afsendelse eller levering til modtageren.

2.2 Klassifikation af Ishøj Kommunes informationer

Alle informationer, som behandles i kommunen, skal klassificeres i en af de nedenfor nævnte kategorier. I de fleste tilfælde kan informationerne klassificeres udfra de systemer, som bruges ved databehandlingen. Systemerne kan grupperes efter kommunens centre, således som det fremgår af den detaljerede liste over fysiske og elektroniske registre i "Bilag 1. Oversigt over fysiske- og elektroniske registre".

Det pointeres, at en given kategori ikke skal beskrive informationernes art, men udelukkende angive, hvilket sikkerhedsniveau der er behov for.

2.2.1 Offentlige informationer

Denne kategori er i Bilag 1 betegnet som "O", og omfatter alle informationer, som kommunen behandler, benytter eller publicerer i forbindelse med varetagelsen af sine opgaver. Informationer i denne kategori kan fx omfatte:

- **Referencemateriale, love og bestemmelser**
- **Trykte og elektroniske publikationer**
- **Offentliggjorte telefonnumre og e-mail adresser**

De vigtigste IT-sikkerhedsegenskaber for informationer, der klassificeres som offentlige, til typisk være Tilgængelighed og Integritet.

2.2.2 Interne informationer

Denne kategori er i Bilag 1 betegnet som "I". I denne kategori placeres informationer, som benyttes af kommunens medarbejdere i forbindelse med interne opgaver, men ikke er bestemt til offentliggørelse eller brug udenfor de afgrænsede arbejdsgange.

Kategorien kan også omfatte informationer, som udveksles med eksterne samarbejdspartnere.

Informationerne kan fx omfatte:

- **Publikationer, der er under udarbejdelse**
- **Referater og regnskaber**
- **Interne notater og arbejdspapirer**
- **Intern og ekstern korrespondance, herunder e-mail**

Informationer, der klassificeres som interne, til typisk være sikret med henblik på Fortrolighed, Tilgængelighed og Integritet.

2.2.3 Følsomme informationer

Denne kategori er i Bilag 1 betegnet som ”F”. Behandlingen af informationer i denne kategori vil typisk være reguleret af eksterne bestemmelser, som f. eks persondataloven, eller interne regler omkring etablerede arbejdsgange.

Informationer, der kategoriseres som følsomme kan fx omfatte:

- **Politiske beslutningsoplæg**
- **Patientoplysninger i sundhedssektoren**
- **Klientoplysninger i socialsektoren**
- **Medarbejderoplysninger**

Informationerne i kategorien følsomme informationer, kræver som regel forholdsregler til sikring af egenskaberne: Fortrolighed, Tilgængelighed og Integritet.

Desuden kan informationer, som indgår i – eller er grundlag for – aftaler, kræve sikring af egenskaberne Ægthed og Uafviselighed.

2.3 Definition af informationssikkerhedsområder

Overalt, hvor kommunens informationer opbevares, anvendes eller behandles, skal der opretholdes et tilstrækkeligt informations-sikkerhedsniveau i forhold til de trusler som anvendelsessituationen medfører. Det betyder, at regler og foranstaltninger skal tilpasses de lokale forhold.

I praksis sikres dette ved at opdele kommunen i en række sikkerhedsområder, således at hvert område omfatter en eller flere lokationer, hvor anvendelsessituationerne er sammenlignelige.

Informationssikkerhedsområderne i Ishøj Kommune omfatter:

- **Det lukkede område**
- **Forvaltningsområdet**
- **Det offentlige område**

Ved opdelingen i områder er det taget i betragtning, hvorledes kommunens informationer opbevares og behandles i området, herunder

- Om der findes IT-arbejdspladser, forbundet til centrale systemer
- Om der findes netværkskomponenter, herunder adgang til stik
- Om der findes servere eller pc'er med eget datalager
- Om der opbevares datamedier (fx Cd-rom eller USB-lager)
- Om der opbevares fysiske informationer(fx arkivskabe)

Desuden er det ved opdelingen taget i betragtning, hvilken personkreds der har adgang til området, og hvilken type opgaver der udføres.

2.3.1 Det lukkede område

Dette område omfatter fysiske lokaler i centre og driftssteder, hvor publikum ikke har adgang, og kommunens medarbejdere følger særlige regler for adgang og anvendelse af informationerne.

F. eks er IT-center et lukket område, hvor kommunens medarbejdere kun har adgang ifølge aftale med øverste informationssikkerhedsansvarlige eller ansatte i IT-center. De adresser og lokaler, som tilhører det lukkede område, fremgår af Bilag 2.

2.3.2 Forvaltningsområdet

Forvaltningsområdet omfatter fysiske lokaler i centre og driftssteder, hvor borgere betjenes og kan få adgang til specifikke informationer, under kontrol af kommunens medarbejdere. De adresser og lokaler, som tilhører forvaltningsområdet, fremgår af Bilag 2.

2.3.4 Det offentlige område

Det offentlige område omfatter fysiske lokaler i centre og driftssteder, hvor den fysiske adgangssikring kan være svagere end for kommunens centrale afdelinger, og steder hvor der generelt er offentlig adgang til lokaler og udstyr.

Dette område inkluderer politikker/hjemmearbejdspladser og mobile enheder, hvor kommunens informationer opbevares eller behandles. Samarbejdspartnere, service- og systemleverandører, der behandler informationer for kommunen, eller har adgang til dette i forbindelse med tekniske ydelser, betragtes også som del af det offentlige område, med mindre der er oprettet en særlig aftale med samarbejdspartneren om beskyttelse af kommunens informationer.

2.3.5 Dokumentation af informationssikkerhedsområder

En komplet liste over fysiske adresser og lokaler i det lukkede område og forvaltningsområdet findes i ”Bilag 2. Definition af informationssikkerhedsområder”.

2.4 Roller omkring informationssikkerheden

Ved etablering og opretholdelse af informationssikkerheden i Ishøj Kommune er det essentielt at definere følgende roller:

- Informationsejer
- Leverandør
- Driftsansvarlig

Hver af disse roller indeholder et ansvar for informationssikkerheden, og kan indebære en række konkrete opgaver. Det bemærkes i den forbindelse, at opgaverne omkring sikkerheden kan uddelegeres, men ansvaret flytter ikke dermed.

2.4.1 Informationsejer

Ejerskab af informationer skal baseres på processerne, hvor informationerne skabes, vedligeholdes eller bruges. Når der er tale om elektroniske informationer, vil informationsejerskabet ofte være sammenfaldende med ejerskabet for de IT systemer som benyttes til lagring og behandling af informationerne.

For informationer, der overføres mellem systemer, skal den primære version identificeres, således at ansvaret for integriteten kan placeres entydigt.

Informationsejerens opgaver omfatter bl.a.:

- **Risikovurdering og klassifikation af informationer**
- **Definition af brugernes adgangsrettigheder i henhold til den aftalte procedure herfor**
- **Fastlæggelse af arbejdsgange og procedurer for informationsudveksling**
- **Sikring af at informationsanvendelsen til stadighed opfylder sikkerhedskravene, herunder gældende lovgivning**

2.4.2 Leverandør

Leverandøransvaret for IT-systemer placeres hos den, som har specificeret IT-systemets funktion, og som løbende påser at det opfylder de stillede mål. Når det handler om fagsystemer, er det typisk den organisation som har udviklet og leveret systemet, eller stiller det til rådighed som en service.

For generelle værktøjer som fx e-mail og tekstbehandling ligger leverandøransvaret hos den organisation, som har konfigureret værktøjet til kommunens brug. Ofte er dette kommunens IT-center, men det kan også være specialister hos kommunen eller dens leverandører.

IT-infrastrukturen (netværk, servere, arbejdsstationer) betragtes som et særligt system, der leveres og konfigureres af kommunens IT-center, i overensstemmelse med kommunens IT-strategi. IT-infrastrukturen omfatter de data, som er nødvendige for den tekniske drift (fx konfiguration, overvågning og adgangskontrol). Af-

grænsede dele af IT-infrastrukturen kan lokalt administreres af det enkelte center, efter retningslinier aftalt med IT-center.

Leverandørens opgaver omfatter bl.a.:

- **Specifikation af IT-systemets funktion og konfiguration**
- **Opsætning og afprøvning af IT-systemets funktion før ibrugtagelse**
- **Udarbejdelse af instrukser og procedurer for driften**

2.4.3 Driftsansvarlig

Denne rolle varetages af en IT-organisation, som udfører veldefinerede opgaver for IT-brugerne og de informationsansvarlige, i overensstemmelse med den gældende service niveau aftale, også kaldet SLA-aftale.

SLA aftalen beskriver IT-centerets ydelser i forbindelse med support, drift og vedligeholdelse af administrative IT systemer i Ishøj Kommune. Aftalen beskriver tillige rolle- og opgavefordelingen mellem kommunens brugere og IT-center, og den rapportering, der er aftalt.

2.4.4 Dokumentation af roller

En komplet liste over informationsejer, leverandør og driftsansvarlig for alle kommunens elektroniske og fysiske registre findes i ”Bilag 1. Oversigt over fysiske- og elektroniske registre".

2.5 Generelle regler for informationsbehandling

For al informationsbehandling i kommunens regi gælder et regelsæt, som afspejler kravene i den overordnede politik for informationssikkerhed og refererer til den struktur, som er udtrykt i de generelle sikkerhedsbestemmelser for informationsbehandling.

Reglerne er opdelt i Adgangsregler og Håndteringsregler:

2.5.1 Adgangsregler

Disse regler beskriver principperne for:

- tildeling
- administration
- benyttelse

af adgang til kommunens informationer.

Reglerne beskriver:

- Ansvar og opgaver omkring definition af brugerkategorier
- Brugernes ansvar for informationssikkerheden
- Regler for fysisk adgang til informationer
- Regler for logisk adgang til informationer

2.5.1.1 Ansvar og opgaver omkring definition af brugerkategorier

IT-infrastrukturen
Den særlige IT-sikkerhedsmedarbejder er ansvarlig for, at definere brugergrupper og adgangsrettigheder til IT-infrastrukturen for disse grupper, efter oplæg fra de lokale sikkerhedsmedarbejdere. Ved oprettelse eller ændring af en brugergruppes rettigheder, skal ændringen aftales med de lokale sikkerhedsmedarbejdere. Brugergruppernes definition af rettigheder skal dokumenteres i af den særlige IT-sikkerhedsmedarbejder i dokumentet *Specifikke IT-sikkerhedsbestemmelser*, som vedligeholdes i IT-center. Den særlige IT-sikkerhedsmedarbejder har ansvaret for løbende at dokumentere, hvilke medarbejdere der er indmeldt i de enkelte grupper.

IT-systemer
I de enkelte systemer defineres brugergrupper af den pågældende informationsejer (se Bilag 1), som del af deres ansvar for at dokumentere den IT-sikkerhedsmæssige konfiguration for det pågældende system. Brugergruppernes definition af adgangsrettigheder og hvilke medarbejdere der er indmeldt i de enkelte grupper, skal dokumenteres af informationsejeren.

Den særlige IT-sikkerhedsmedarbejder skal udarbejde en procedure som skal følges ved oprettelse ændring eller sletning af brugergrupper i de enkelte systemer, og ved administration af brugerne. Denne procedure skal indgå i dokumentet *Specifikke IT-sikkerhedsbestemmelser*, som vedligeholdes i IT-center.

2.5.1.2 Brugernes ansvar for informationssikkerheden

Enhver bruger skal oplyses om sit ansvar for informationssikkerheden, når brugeren tildeles sine adgangsrettigheder. Oplysningen sker ved fremsendelse af følgende fysiske dokumenter:

- Adgangskoder til IT-systemerne.
- Brugernes ansvar ved anvendelse af IT-systemer.

og ved fremsendelse af referencer (links) til følgende elektroniske dokumenter:

- Politik for Informationssikkerhed med Bilag 1, 2 og 3 (dette dokument).
- Retningslinier for anvendelse af elektronisk post.

Brugeren skal med sin underskrift kvittere for modtagelse og læsning af dokumenterne og acceptere sit ansvar i henhold hertil.

2.5.1.3 Regler for fysisk adgang til informationer

Alle medarbejdere der ansættes i kommunen får som hovedregel udleveret en nøgle, der giver adgang til arbejdspladsen indenfor normal åbningstid. Der er imidlertid enkelte områder der er fysisk spærret for adgang, blandt andet IT-afdelingen.

De fysiske sikkerhedsforanstaltningerne er gradueret efter de enkelte sikkerhedsområder
(som er defineret i afsnit 2.3):

	Det lukkede område	**Forvaltningsområdet**	**Det offentlige område**
Lokaler holdes altid aflåst.	X		
Der er kun adgang for en begrænset personkreds.	X		
Skabe med IT udstyr holdes altid aflåst		X	X
Lokalet skal være under konstant opsyn af kommunens medarbejdere.		X	
Der er i lokalet forbud mod foto-, lyd- og videooptagelse uden tilladelse.		X	
Lokalet skal være aflåst når det ikke er bemandet.		X	

Computere i lokalet skal være placeret, så informationer på skærmen ikke kan ses af uvedkommende.		X	
Print, kopier og fax skal beskyttes, så de ikke kan læses eller medtages af uvedkommende.		X	X
Alt IT udstyr skal beskyttes, så det ikke kan betjenes eller fjernes af uvedkommende.		X	X
Alle papirdokumenter skal beskyttes, så de ikke kan læses eller fjernes af uvedkommende .		X	X

2.5.1.4 Regler for logisk adgang til informationer

Uvedkommende har ikke adgang til kommunens informationer.

Medarbejdernes adgang skal autoriseres på grundlag af arbejdsbetinget behov. Autorisering gives alene til data og funktioner, som er nødvendige for medarbejderens varetagelse af sine arbejdsopgaver. Fælles brugeridentifikation for større eller mindre personalegrupper må ikke anvendes.

Overførsel af informationer mellem kommunens IT-systemer må kun udføres i det omfang, der er fastlagt af procedurerne i afsnit 2.4.1.

Der må kun etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til kommunens IT-informationer. I praksis betyder dette, at alle eksterne kommunikationsforbindelser skal godkendes af IT-center.

2.5.2 Håndteringsregler

Her beskrives reglerne for

- lagring
- behandling
- overgivelse

af kommunens IT-informationer.

Reglerne beskriver:

- Indtastning, oprettelse og import af IT-informationer
- Procedurer for kopiering, udtræk og udskrivning af IT-informationer
- Samkøring og overførelse af IT-informationer mellem systemer

2.5.2.1 Indtastning, oprettelse og import af IT-informationer

Både indsamling af data og dannelse af nye registre udfra eksisterende informationer skal følge Datatilsynets retningslinier, herunder regler for anmeldelse og godkendelse af midlertidige og permanente datasamlinger.

Ved oprettelse af et register/ datasamling, skal registeret anmeldes til den særlige IT-sikkerhedsmedarbejder, før det tages i brug. Den samme procedure skal følges, ved ibrugtagning af et nyt IT-system, og ved modtagelse (import) af IT-informationer fra eksterne samarbejdspartnere og borgere.

Enhver bruger skal orienteres om sit ansvar og skal kvittere herfor, se afsnit 2.5.1.2 før brugeren får adgang til at registrere (indtaste) eller anvende IT-informationer i kommunens regi. Denne orientering skal omfatte vejledning omkring oprettelse af nye datastrukturer, med definition af et register, klassifikation af de oplysninger der behandles, og regler for anmeldelse af registre.

2.5.2.2 Procedurer for kopiering, udtræk og udskrivning af IT-informationer

Det er ikke tilladt for kommunens brugere, at kopiere kommunens data til andre drev eller datastrukturer end der hvor de anvendes. En sådan kopiering må kun foretages af den ansvarlige informationsejer, og betragtes som oprettelse af et nyt register/datasamling.

Udtræk af kommunens IT-informationer på et elektronisk medie, som f. eks diskette, CD eller bånd betragtes ligeledes som oprettelse af et nyt register. Dette skyldes, at IT-informationernes sikkerhed er afhængig af det miljø, hvori de opbevares eller behandles.

Udskrivning af IT-informationer på papir skal følge de gældende regler for arbejdsgangen, herunder regler for opbevaring og tilintetgørelse af udskriften.

2.5.2.3 Samkøring og overførsel af informationer mellem systemer

En samkøring af kommunens registre, må kun foretages med tilladelse fra informationsejeren, og under overholdelse af de procedurer, som denne har fastlagt for IT-informationsudveksling i henhold til afsnit 2.4.1. Den samme procedure skal følges, ved samkøring af kommunens interne informationer med informationer fra eksterne samarbejdspartnere og IT-informationsleverandører.

Hvis samkøringen omfatter overførsel af IT-informationer mellem forskellige sikkerhedsområder, skal informationsejeren foretage en risikovurdering og klassificering af samkøringens resultater, som om der foreligger et nyt register.

Hvis samkøringen resulterer i oprettelse af et nyt register/datasamling, skal registeret anmeldes til den særlige IT-sikkerhedsmedarbejder, før samkøringen foretages.

2.6 Informationssikkerhedsorganisationen

Ved opbygningen af de organisatoriske rammer for informationssikkerheden skal ledelsen sikre, at enhver enhed besidder den nødvendige faglige, tekniske og organisatoriske kompetence til, at varetage sit ansvar, dvs. at tage de relevante beslutninger på et oplyst grundlag.

Viden om de IT-sikkerhedsmæssige aspekter spiller her en afgørende rolle: Både hos ledelsen og hos medarbejderne er der brug for, en klar forståelse af behovet for IT-informationssikkerhed, og af det ansvar, som den enkelte forventes at tage.

Informationssikkerhedsorganisationen er som udgangspunkt en serviceorganisation overfor resten af organisationen og bistår med råd og vejledning omkring de forskellige aspekter, der måtte være i forbindelse med informationssikkerhedsopgaverne i de enkelte områder.

Personer og roller i informationssikkerhedsorganisationen fremgår af ”Bilag 3. Informationssikkerhedsorganisationen”.