IT sikkerhedspolitik

for

Fredericia Kommune

Versionsstyring

Versions-nummer	Dato for version	Ændring	Årsag	Ansvar
1.00	01.06.2013		Ny politik godkendt i byrådet	Per Toftdahl
2.00	13.01.2016	Opdatering	Der er sket organisati-onsændringer og der er kommet nye politikker	Per Toftdahl

Indledning

Overordnet gælder, at IT-anvendelsen i Fredericia Kommune skal understøtte de enkelte afdelinger i opnåelse af kommunens servicemål. På samme tid skal kommunens sikkerhedsniveau sikres og overholde de love og regler der er udstukket centralt. Endelig skal der sikres et tilfredsstillende sikkerhedsniveau i forhold til anbefalinger fra kommunens revision.

Det er også Fredericia Kommunes værdibaserede holdning, at medarbejdere har en bevidst holdning til begrebet IT-sikkerhed, med vægt på reel sikkerhed frem for formel sikkerhed.

Det er Fredericia Kommunes holdning at kun gennem bevidstgørelsen af sikkerhedspolitikken kan der opnås en reel sikkerhed.

Fredericia Kommunes sikkerhedspolitik:

- Respektere de krav, datalovgivningen til enhver til måtte stille
- Har udgangspunkt i kommunens Digitaliseringsstrategi
- Understøtter kommunens IT-strategi
- Fastsætter hovedprincipper for den overordnede IT-sikkerhed i kommunen og placere et entydigt ansvar for varetagelse af IT-sikkerheden.
- Sikre ønsket om en reel IT-sikkerhed ved implementering af et brugerunderstøttende værktøj

IT-sikkerhedspolitikken er opbygget i to niveauer. Kommunens overordnede IT-sikkerhedspolitik der beskriver principper og som godkendes af Byrådet.
Bilag der mere i dybden beskriver de enkelte sikkerhedsområder og som godkendes af Direktionen. Bilagene benævnes IT-sikkerhedshåndbogen.

IT-sikkerhedspolitikken udmøntning i IT-sikkerhedshåndbogen er opbygget af en række bilag der hver beskriver et specifikt område indenfor sikkerhedsområdet:

Bilag 1. IT-sikkerhedsorganisationen
Bilag 2. Roller og ansvar
Bilag 3. Autorisationer og brugerstyring
Bilag 4. Systemer med IT-kontrol
Bilag 5. IT-brugerne
Bilag 6. Administrator og IT-medarbejdere
Bilag 7. Fysisk sikkerhed
Bilag 8. Hjemmearbejdspladser
Bilag 9. Bærbare arbejdspladser
Bilag 10. Mobilenheder
Bilag 11. E-post

Bilag 12. Internetsøgninger
Bilag 13. Overdragelse og bortskaffelse af udfaset udstyr
Bilag 14. Firewall administration
Bilag 15. Logning og anvendelsen af logning
Bilag 16. Lov om beskyttelse af persondata
Bilag 17. Konsekvenser ved sikkerhedsbrud
Bilag 18. Anvendelse af WI-FI
Bilag 19. Opkobling af tredje personer
Bilag 20. Undtagelseshåndtering
Bilag 21. Hændelseshåndtering
Bilag 22. Revision
Bilag 23. Anvendelse af privat udstyr, samt kommunalt udstyr til private formål

Rækkefølgen af bilagene er ikke et udtryk for betydning og kan ikke bruges til prioritering af sikkerhedsområderne.

Resten af dette dokument udgør Fredericia Kommunes IT-sikkerhedspolitik.

Hvem er omfattet af IT-sikkerhedspolitikken

IT-sikkerhedspolitikken gælder for alle personer der har adgang til kommunens interne netværkstjenester eller som har adgang til et system der anvendes i den daglige produktion på kommunen:

- Medarbejder i kommunen
- Politiker i kommunen
- Samarbejdspartner der har fået tildelt adgang

Disse grupper vil i den resterende IT-sikkerhedspolitik med tilhørende bilag blive beskrevet som "Medarbejdere".

Ajourføring af IT-sikkerhedspolitikken

Den øverste IT-sikkerhedspolitikansvarlige (se afsnittet om "ansvar og organisering") sikre vedligeholdelse og ajourføring af IT-sikkerhedspolitikken. Det er også den IT-sikkerhedspolitikansvarliges ansvar at sikre nødvendige ændringer, tilføjelser eller fjernelser i IT-sikkerhedspolitikken.

Alle ændringer registreres i afsnittet Versionsstyring samt i en ændringslog der dækker den samlede IT-sikkerhedspolitik.

IT-sikkerhedspolitikken vil hvis der er ændringer blive forelagt direktionen, hvor de eventuelle ændringer gennemgås. Kun ændringer af væsentlig karakter for kommunens drift foreligges politiks beslutning.

IT-strategi, Digitaliseringsstrategi, Velfærdsteknologistrategi samt IT-arkitekturen skal alle være compliant med IT-sikkerhedspolitikken og skal være gennem en godkendelse for den øverste IT-sikkerhedspolitikansvarlige.

Formål med IT-sikkerhedspolitikken

IT-sikkerhedspolitikken beskriver håndtering af IT-sikkerhed i Fredericia Kommune og fastlægger krav og forventninger til kommunens sikkerhedsniveau.

> Fastlæggelsen af IT-sikkerhedsniveauet beskrevet i IT-sikkerhedspolitikken tager udgangspunkt i en overordnet risikoanalyse. Den overordnede risikoanalyse skal være godkendt af direktionen og skal revideres og godkendes mindst en gang om året.

IT sikkerhedspolitikkens formål er, at

- Afspejle kommunens behov
- Afspejle myndighedskrav samt lovgivning
- Sikre drift og tilgængelighed af systemer og til data
- Sikre organisationen mod tab af data
- Sikre en entydig ansvarsplacering for IT-sikkerhed
- Sikre compliance med gældende revisionspraksis
- Dokumentere det gældende IT-sikkerhedsniveau i kommunen

Ansvar og organisering

IT-sikkerhedsorganisationen følger linjeorganisationen således, at ansvar og kompetencer omkring IT-sikkerhed er forankret i afdelingerne og optræder som en integreret del af forretningsprocesserne og medarbejdernes hverdag.

Øverste IT-sikkerhedspolitikansvarlige

Økonomiudvalget har det overordnede ansvar for IT-sikkerheden, og skal godkende IT-sikkerhedspolitikken.

Kommunaldirektøren er af økonomiudvalget udpeget som øverste sikkerhedspolitikansvarlige og har det overordnede ansvar for, at IT-sikkerhedspolitikken til enhver tid er ajourført. Endvidere har kommunaldirektøren kompetence til at godkende ændringer i IT-sikkerhedspolitikken og relaterede bilag.

Det daglige IT-sikkerhedsarbejde varetages af IT-sikkerhedsansvarlig mens chefer for afdelingerne er ansvarlige for at IT-sikkerhedsregler overholdes og udmøntes i betryggende håndtering og forretningsgange.

Der er almindelig delegationsret i forbindelse med it-sikkerhedsspørgsmål.

IT-sikkerhedsansvarlig

Der er udnævnt en IT-sikkerhedsansvarlig, som fungerer som øverste sikkerhedspolitikansvarliges stedfortræder i forbindelse med tilrettelæggelse af kommunens it-sikkerhed.

I forbindelse med IT-sikkerhedsopgaver refererer it-sikkerhedsansvarlige direkte til kommunens direktion.

Det er den IT-sikkerhedsansvarliges opgave at påse, at der til stadighed er etableret forretningsgange og procedurer, som understøtter overholdelsen af IT-sikkerhedspolitikken samt bilagene.

Ansvar i organisationen

Ansvaret for overholdelse af IT-sikkerhedspolitikken følger kommunens organisatoriske opbygning.

Afdelingschefer og institutionsledere er dermed ansvarlige for it-sikkerheden indenfor deres ansvarsområde. Ansvar er beskrevet i bilag 2 "Roller og ansvar".

Biblioteket er ansvarlig for sikringen af egne systemer og virtuelle netværk i overensstemmelse med it-sikkerhedspolitikken og relaterede bilag. Biblioteket er systemejer og har en it-ansvarlig for eget område og er dermed ansvarlig for, at der til stadighed er etableret forretningsgange og procedurer, som støtter overholdelsen af it-sikkerhedspolitikken. Dette medfører blandt andet, at bibliotekets it-funktion skal videregive den nødvendige information til kommunens it-chef til støtte for det samlede overblik over kommunens it-anvendelse.

IT-chefen

IT-driftsafviklingen varetages af IT-afdelingen enten gennem egen drift eller udlicitering.

IT-chefen er med mindre andet vedtaget IT-sikkerhedsansvarlig.

Ansvar hos samarbejdspartnere

Ansvaret for overholdelse af IT-sikkerhedspolitikken i forbindelse med arbejde udført af samarbejdspartnere påhviler de enkelte afdelingschefer i hvilket område samarbejdspartneren udfører arbejde.

Ansvarsområder

Placering i organisationen	Ansvar
Økonomiudvalget	Godkender it-sikkerhedspolitikken og udpeger øverste IT-sikkerhedspolitikansvarlige.
Kommunaldirektøren	Er øverste IT-sikkerhedspolitikansvarlige, som er ansvarlig for den overordnede tilrettelæggelse af IT-sikkerheden i kommunen, herunder ansvaret for opfølgning og kontrol. Det daglige IT-sikkerhedsarbejde er uddelegeret til it-sikkerhedsansvarlige.
It-sikkerhedsansvarlige	Delegeret it-sikkerhedsansvarlig. Foretager kontrol af IT-sikkerheden og varetager ajourføring af IT-sikkerhedspolitikken.
Byrådssekretariat	Koordinering og rådgivning i forhold til Persondataloven.
IT-chefen	Udpeget IT-sikkerhedsansvarlig. Er ansvarlig for udmøntning af kommunens IT-sikkerhedspolitik i forretningsgange og procedurer, som støtter overholdelsen af IT-sikkerhedspolitikken og bilagene.
It-afdelingen	Varetager dagligt IT-sikkerhedsarbejde i forbindelse med IT-anvendelsen. Har ansvaret for tekniske driftsopgaver og support. Stillingtagen til IT-sikkerhed i fællesskab med systemejere.
It-medarbejdere	Varetager udmøntningen af det daglige IT-sikkerhedsarbejde og skal i den forbindelse understøtte retningslinjerne i IT-sikkerhedspolitik og bilag.
Systemejere	Har ansvaret for et specifikt programkompleks, herunder anskaffelse, driftsafvikling, vedligeholdelse og udfasning. Stillingtagen til interne kontroller i systemet samt sikkerhed. Systemejere kan uddelegere ejerskabet til en stedfortræder, som varetager det daglige sikkerhedsarbejde i forbindelse med systemet.
Medarbejdere generelt	Varetagelse af IT-sikkerheden ved overholdelse af kommunens IT-sikkerhedspolitik og relaterede bilag.

Regler

Datalovgivningen har til formål at sikre følsomme data imod misbrug. Datalovgivningen omfatter såvel enkeltstående data som samling af data, eksempelvis en telefonbog, en adresseliste eller et personalekartotek.

Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger (Persondataloven) indeholder en række regler, som giver den registrerede forskellige rettigheder over for myndigheder og virksomheder (den dataansvarlige), som behandler oplysninger om den pågældende.

Loven gælder for behandling af personoplysninger, som helt eller delvist foretages ved hjælp af elektronisk databehandling, og for ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Den ny EU Persondataforordning indeholder en række stramninger og ændringer i forhold til persondataloven og kommunen skal inden 1. januar 2018 have implementeret stramningerne og ændringerne.

Systemejer har ansvaret for, at kravene i datalovgivningen overholdes, og skal forinden iværksættelse af en behandling af oplysninger omfattet af Persondataloven foretage anmeldelse til Datatilsynet.

Den enkelte medarbejder, som er autoriseret til at anvende en PC-arbejdsplads, skal gøres bekendt med retningslinjer for it-brugere.
Ud over en række praktiske oplysn
inger om anvendelse af programmer og hardware beskriver retningslinjerne ligeledes den enkelte medarbejders ansvar som it-bruger. Da it-anvendelsen følger den generelle teknologiske udvikling, vil retningslinjerne med jævne mellemrum blive revideret

Lovgivning for datasikkerhed er beskrevet i DS484/ISO27001. Denne lov er ikke obligatorisk for kommuner og følges i det omfang det virker understøttende for kommunens IT-sikkerhedspolitik.

Fysisk sikkerhed

Den fysiske sikkerhed 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.

Den fysiske sikkerhed er tilrettelagt ud fra en konkret risikovurdering. Den fysiske sikkerhed skal i relevant omfang være dokumenteret således, at kommu-

nens ledelse - som en del af den generelle IT-risikostyring, kan planlægge sikkerhedsprocedurer i forhold til den fysiske sikkerhed.

Den fysiske sikkerhed skal afvejes i forhold til mulige driftsforstyrrelser og driftstab. I praksis betyder det, at kravene til den fysiske sikkerhed er opdelt i 3 sikkerhedsniveauer:

- Fysisk sikkerhedsniveau 1: Omfatter centralt udstyr, herunder udstyr i centrale serverrum.
- Fysisk sikkerhedsniveau 2: Omfatter decentralt kommunikations- og netværksudstyr, herunder decentrale krydsfelter.
- Fysisk sikkerhedsniveau 3: Omfatter almindeligt it-udstyr i kommunens lokaler, herunder primært pc'er, printere og tilsvarende periferiudstyr. Endvidere omfatter sikkerhedsniveau 3 decentrale arbejdspladser og bærbare pc'er udenfor kommunens lokaler, herunder bærbare enheder som USB-nøgler, PDA, smartphones, tablets og lignende.

Fastsættelse af det fysiske sikkerhedsniveau indebærer mindst retningslinjer for;

- Serverrum, herunder placering, adgangskontrol, alarmsystemer samt andre tekniske løsninger, som køleanlæg, nødstrømsanlæg og automatiske brandslukningssystemer.
- Kabling og krydsfelter, herunder placering og sikkerhed.
- Pc-udstyr i kommunens lokaler, herunder hensigtsmæssig placering i forhold til både arbejdsmiljø og IT-sikkerhed. Lokalerne skal være betryggende sikret - enten døgnbemandet eller aflåst udenfor normal arbejdstid.
- Pc-udstyr på andre lokationer end kommunens, herunder hensigtsmæssig placering i forhold til arbejdsmiljø og IT-sikkerhed.
- Kassation og destruktion af udstyr, skal foretages miljømæssigt forsvarligt og finde sted efter betryggende sletning af data.
- Registrering af aktiver og forsikringer. Registrering - af alle enheder der repræsenterer en væsentlig værdi. Registrering - af alle licensforhold. Forsikringer følger kommunens almindelige regler vedrørende forsikring af aktiver.

Datasikkerhed

Data i kommunens it-systemer repræsenterer en væsentlig værdi, ligesom der kan være tale om fortrolige og/eller personfølsomme oplysninger. Disse værdier skal sikres mod uautoriseret adgang og mod tab og forvanskning.

Systemejer skal derfor i fællesskab med IT afdelingen fastsætte et sikkerhedsniveau, ud fra en konkret risikovurdering og samtidig gøre det muligt for brugerne at opnå en fornuftig anvendelse af systemerne.

Data der er personhenførbare og som anvendes til sagsbehandling må ikke gemmes på medier, der kan fjernes fra kommunens lokationer eller på tjenester, hvor kommunen ikke har den fulde kontrol.

Følgende områder skal indeholdes i risikovurderingen

Tildeling og ændring af autorisation

Ud fra hvilke kriterier tildeles adgang til IT-systemet herunder data.

Udarbejdelse af forretningsgange for tildeling, ændring, nedlæggelse og kontrol af autorisationer, som sikrer ovenstående. *Se bilag 3.*

Systemejer eller delegeret er ansvarlig for at definere, hvilke systemer eller informationer, medarbejderne skal have adgang til.

Registrering af dataanvendelsen

Systemanvendelsen skal registreres (logges). Der skal i risikoanalysen tages stilling til logningsniveauet for både overordnede systemer og de enkelte afdelingsspecifikke systemer.

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

Udskrifter

Det påhviler afdelingschefen at sikre, at udskrifter kun bliver anvendt i overensstemmelse med den afgrænsning, der findes i anmeldelsen for det pågældende system.

Herudover skal afdelingschefen sikre, at udskrifter, der indeholder følsomme data, bliver opbevaret betryggende, således uvedkommende ikke kan få adgang til disse. Udskrifter der indeholder følsomme data må ikke fjernes fra kommunens lokation med mindre der opsøges tilladelse.

Sikkerhedskopiering

For at sikre, at alle relevante data bliver sikkerhedskopieret, skal alle medarbejdere placere arbejdsdokumenter, regneark og lignende der anvendes i sagsbehandlingen på centrale servere. *Se bilag 5*.

For hvert enkelt system skal systemejer tage stilling til frekvensen i forbindelse med sikkerhedskopiering.
Der skal for hvert system foretages en teknisk afprøvning af kopieringsrutinerne, herunder kontrol af genetableringsprocedurerne, mindst én gang om året eller i forbindelse med omlægning af rutinerne. Sikkerhedskopier skal opbevares betryggende iht. risikovurderingen.

Datakvalitet

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

For hvert system skal systemejer tage stilling til, hvilke interne kontroller, der skal udføres i forbindelse med databehandlingen, og hvem der er ansvarlig herfor. *(del af ledelsestilsynet beskrevet af Økonomi.)*

Virus

IT afdelingen tilstræber, at alle relevante enheder, servere og PC arbejdspladser i kommunen til enhver tid er opdateret med den nyeste version af det anvendte antivirusprogrammel.

Endvidere skal de enkelte medarbejdere efterleve de retningslinjer, der er beskrevet. *Se bilag 5.*

Datakommunikation

IT afdelingen er ansvarlig for opbygning og vedligeholdelse af netværk og kommunikationsforbindelser, som giver medarbejderne hurtig og sikker adgang til relevante systemer. IT afdelingen vedligeholder oversigter for kommunens netværk og kommunikationsforbindelser.

Adgang til Fredericia Kommunes netværk skal være sikret, så det kun er autoriserede medarbejdere, der kan få adgang.

Serviceadgang for eksterne teknikere i enkeltstående tilfælde bliver kun etableret efter forudgående aftale med IT afdelingen og pågældende tekniker.

Serviceadgang af mere permanent karakter bliver kun etableret efter forudgående skriftlig aftale med serviceleverandøren. I begge tilfælde er det IT afdelingens ansvar at begrænse teknikerens adgang til de elementer i kommunens IT infrastruktur, som er nødvendig for at kunne løse opgaven.

Det er alene Fredericia Kommunes eget udstyr, som må tilkobles kommunens netværk, hvis der ikke er indhentet forudgående tilladelse fra IT afdelingen (*se bilag 23 omhandlende BYO*).

Anvendelse af kommunalt udstyr til private formål sker på brugerens ansvar og det er den enkelte bruger der sikre den nødvendige sikkerhed (*se Bilag 23*)

IT afdelingen er ansvarlig for, at adgangen til netværket via Internettet er beskyttet med en Firewall. *Se bilag 14.*

Hjemmearbejdspladser

IT afdelingen er ansvarlig for at udarbejde og vedligeholde retningslinier for anvendelse af hjemmearbejdspladser i relation til jobbets udførelse. *Se bilag 8.*

Nyt it-udstyr

Teknologien medfører fortsat nye typer af databærende og databehandlende udstyr, eksempelvis smartphones og tablets. IT afdelingen er ansvarlig for, at der i relevant omfang udarbejdes og vedligeholdes særlige sikkerhedsregler for udstyr af denne type, som måtte blive taget i anvendelse. *Se bilag 9 og 10.*

Internet og e-post

Der er udarbejdet retningslinjer for anvendelse af Internet og e-post. *Se bilag 11 og 12.*

Digital signatur og kryptering

Anvendelse af digitale signaturer finder stadig større indpas i den offentlige forvaltning. Digitale signaturer anvendes i dag til både adgangskontrol - logon - til en række offentlige tjenester og i forbindelse med afsendelse og modtagelse af elektroniske meddelelser, hvor sikkerhed for identitet, sikkerhed for indholdets autenticitet (uændrethed) og fortrolighed (kryptering) kan være ønsket eller påkrævet.

Kommunen ønsker at anvende digitale signaturløsninger som en integreret del af kommunens værktøjer både til kommunikation og til identifikation. Kommunen ønsker at kunne håndtere digitale signaturer, herunder udveksle signerede/krypterede elektroniske meddelelser med virksomheder, borgere og andre offentlige myndigheder.

I en række funktioner vil det endvidere være nødvendigt at kommunens ansatte får mulighed for at anvende digital signatur som adgangsnøgle til offentlige tjenester og internetportaler.
Den øverste sikkerhedspolitikansvarlige har ansvar for, at kommunen udarbejder detaljerede procedurer for anvendelse af digital signatur og kryptering (*se bilag 3*).

IT afdelingen sørger for de praktiske foranstaltninger i forbindelse med anskaffelse og drift af faciliteter til signaturhåndtering, herunder administration og vedligeholdelse af udstedte certifikater og integration til kommunens ESHD- og andre it-systemer.

Selvbetjeningsløsninger

I forbindelse med den voksende udbredelse af selvbetjeningsløsninger i kommunerne, er der behov for at have en ensartet strategi for implementering af disse.

Systemerne bliver typisk udviklet af forskellige udbydere, og systemerne er uensartede i forhold til teknik, platform o.s.v. For at tilgodese dette behov og sikre, at systemerne lever op til de krav, der stilles bl.a. i Persondataloven, er det nødvendigt at systemejer foretager en grundig risikovurdering.

Anskaffelse af systemer

Fredericia Kommune udvikler som udgangspunkt ikke selv systemer.

IT afdelingen skal i samarbejde med systemejer sikre, at anskaffede systemer og driftsmiljøer etableres på en sådan måde, at retningslinjerne i IT-sikkerhedspolitikken og bilagene kan tilgodeses.

Systemejer har ansvaret for, at udviklede applikationer sikres i et tilfredsstillende omfang, dels via centralt opdaterede sikkerhedskopier dels ved udarbejdelse af præcis dokumentation af programmeringsgrundlaget.

Af hensyn til kontraktlige forhold, test og drift med mere, skal IT afdelingen altid inddrages i processen, inden installation af nyt software på kommunens administrative netværk.

Alle anskaffelser skal foretages under lovmæssige korrekte forhold. Der skal her henledes på forhold omkring udbudsbestemmelser.

Risikoanalyse

Hele IT-sikkerhedshåndbogen er baseret på risikoanlyser der afdækker sikkerhedsmæssige forhold. Systemejer er derfor ansvarlig for udarbejdelse af risikoanalysen der er til grund for sikkerhedspolitikker.

På centrale systemer og elementer er IT afdelingen systemejer og ansvarlig.

Nødberedskab

Fredericia Kommune skal råde over et ajourført nødberedskab således, at kommunens forretningsgange ikke vil blive unødigt hæmmet i forbindelse med eventuelle nødsituationer i IT-driften.

Nødberedskabet skal stå i naturligt forhold til vigtigheden af det driftsmiljø, som skal beskyttes. Fastlæggelse af nødberedskabet knytter sig tæt til den udførte risikoanalyse.

Den IT-sikkerhedsansvarlige har ansvaret for fastsættelse og ajourføring af det overordnede nødberedskab for it-anvendelsen.

Systemejer har ansvaret for, at udarbejde og vedligeholde nødberedskab for de enkelte systemer. Hvis der er behov kan it-afdelingen yde bistand.

Styring af IT-aktiver

Alle væsentlige it-aktiver i kommunen skal indgå i en fælles fortegnelse, hvor alle relevante karakteristika er angivet. Registreringen skal sikre en entydig identificering af de enkelte it-aktiver og sikre et betryggende overblik samt styring af opgradering og moderniseringsprojekter.

Det er IT afdelingen der har ansvaret for registreringen, herunder løbende vedligeholdelse af positivlister for hardware og software vedrørende kommunens generelle IT-anvendelse. Ansvaret for registrering af fagspecifikke systemer er placeret hos systemejer.

IT afdelingen fører endvidere kontrol med softwarelicenser på baggrund af indberetning fra serviceområder og stabe.
Retningslinjer for fysisk sikkerhed er endvidere beskrevet. *Se bilag 7*.

Opfølgning og kontrol

For at sikre en levende og ajourført IT-sikkerhedspolitik skal følgende elementer underkasten en årlig gennemgang:

- IT-sikkerhedspolitikken
- Bilag
- Risikoanalyser
- Systemejer lister
- Brugeradministration

Skabelon for bilag

Alle bilag skal indeholde oplysninger om:

- Bilagsnummer
- Hvad bilaget drejer sig om
- Hvem er målgruppen for bilaget
- Versionsstyring

IT afdelingen udarbejder en skabelon der anvendes til alle bilag.