Politik for informationssikkerhed for Fanø Kommune

Kvalitet i livet – hele livet

Version 2016

Politik for informationssikkerhed for Fanø Kommune

Indholdsfortegnelse

1. Indledning 4
2. Formål 4
3. Omfang 4
4. Ansvar og roller 5
5. I-sikkerhedsniveau 5
6. Formidling og uddannelse 6
7. Brud på i-sikkerheden 6
8. Retningslinjer for ledere og medarbejdere 6
   8.1 Ledelsens ansvar og rolle 6
      8.1.1.Kommunaldirektøren 6
      8.1.2 Systemejer / Afdelingsleder 7
      8.1.3 Autorisationer 8
      8.1.4 Journalisering 8
      8.1.5 Elektronisk borgerbetjening 8
      8.1.6 Digital signatur 8
   8.2 IT-koordinatoren 8
      8.2.1 Driftsdokumentation 9
      8.2.2 Firewall 9
      8.2.3 Antivirus 9
      8.2.4 Logning 9
      8.2.5 Udvikling, ændringer og anskaffelser 9
      8.2.6 Serverrum og fysiske installationer 9
      8.2.7 Beredskab 9
   8.3 Medarbejdere og interne brugere 10
      8.3.1 Internet 10
      8.3.2 E-mail 10
      8.3.3 Arbejds-pc 10
      8.3.4 Bærbare og fjernopkoblinger 10

8.3.5 Trådløst netværk 10
8.4 Samarbejdspartnere og eksterne brugere 10
8.4.1 Samarbejdet med Esbjerg Kommune 11
8.4.2 Samarbejde med andre myndigheder 11
8.4.3 Samarbejde med KMD og andre leverandører 11
8.4.4 Kommunens hjemmeside 11
9. Opfølgning og evaluering 11
A. Implementering af politikken 12
B. Bilagsoversigt 13

1. Indledning

IT og internettet gør det muligt for Fanø Kommune at løse opgaver effektivt. I nogle tilfælde muliggør IT højere kvalitet og service for de samme penge. Endelig kommer kommunens investeringer i it og netværksinfrastruktur borgerne til gavn i andre sammenhænge og dét underbygger vores vision om et moderne ø-samfund.

It-anvendelsen gør os samtidig sårbare. Eksempelvis kan systemnedbrud betyde, at væsentlige eller kritiske opgaver ikke kan udføres og at vi mister data, som er meget dyre at genskabe. Eller en forkert anvendelse af et system kan resultere i at følsomme oplysninger lækkes til internettet og ikke længere kan beskyttes af kommunen.

Med almindelig sund fornuft undgås mange risici, men visse risici kræver større indsigt og overblik, samt en koordineret og systematisk indsats. Som vi er vant til fra eksempelvis økonomiområdet. Sikkerheden opnås ved en generel høj bevidsthed hos medarbejderne samt ved at chefgruppens medlemmer varetager ledelsesmæssige prioriteringer, koordinering og opfølgning, med udgangspunkt i Dansk Standard for Informationssikkerhed ISO27001.

Den praktiske anvendelse og udmøntning af i-sikkerhedspolitikken er kort beskrevet i afsnit 10.

I-sikkerhedspolitikken er udarbejdet i samarbejde med BDO Kommunernes Revision A/S.

2. Formål

Formålet med politikken er at fastlægge principper og rammer for, hvordan risikoen for skader på informationsaktiverne effektivt minimeres.

Målet er at sikre,

- at informationer og services er tilgængelige, når autoriserede personer har behov for det,
- at informationer er korrekte og fuldstændige, at services fungerer korrekt, og
- at følsomme informationer beskyttes, så de forbliver hemmelige for uvedkommende.

Med politikken fastlægges:

- Ansvaret for beskyttelse af informationer og systemer i kommunen.
- Kommunens i-sikkerhedsmålsætning og i-sikkerhedsniveau.
- Hvordan i-sikkerhedsbrud skal håndteres.
- Retningslinjer for informationssikkerheden efter værdien af informationsaktiverne.

3. Omfang

I-sikkerhedspolitikken med bilag omfatter alle Fanø Kommunes virksomheder og alle informationsaktiver, der tilhører kommunen eller er i kommunens varetægt. Der er således ikke kun tale om personoplysninger, men om informationer generelt, som har betydning for kommunen og for Fanø.

I-sikkerhedspolitikken omfatter alle brugere af kommunens informationer, it-systemer og it-infrastruktur.

Fanø Kommunes samarbejde med eksterne leverandører og samarbejdspartnere må ikke forringe sikkerheden. Sikkerheden kan øges på fagområder, hvis lederen af området finder det nødvendigt. Eventuelle skærpelser skal koordineres med IT-koordinatoren.

Der er særlige regler for skolen og øvrige dele af kommunens it-installation, som borgere og virksomheder har direkte adgang til.

4. Ansvar og roller

Kommunaldirektøren har det overordnede ansvar for informationssikkerheden i Fanø Kommune. Kommunaldirektøren har ansvaret for, at værdien og risikoen ved alle digitaliseringsprojekterer beskrevet, inden de forelægges kommunalbestyrelsen, og at projekterne understøtter KL's og Digitaliseringens Styrelsen strategier. Outsourcing(udlicitering) kan have sikkerhedsmæssige og strategiske konsekvenser og skal derfor altid godkendes af kommunaldirektøren. Også på de områder, hvor Fanø har indgået samarbejder, skal det sikres, at samarbejdskommunen lever op til Fanø Kommunes i-sikkerhedsmålsætning.

IT-koordinatoren er kommunaldirektørens stedfortræder i spørgsmål om informationssikkerhed. IT-koordinatoren støtter chefgruppens koordinering af kommunens i-sikkerhed og yder støtte til hele organisationen.

Ændringer i i-sikkerhedspolitikken og retningslinjer besluttes af kommunaldirektøren i samråd med chefgruppen.

Forvaltningschefen på området har ansvaret for den fysiske sikkerhed, herunder indbrudssikring, brand, vandskader, ombygninger mm.

Derudover har alle medarbejdere ansvar for at holde sig orienteret om og efterleve reglerne for korrekt og accepteret brug af kommunens systemer og data.

5. I-sikkerhedsniveau

Stabil drift er afgørende for borgernes oplevelse af kvaliteten af kommunens services. Derudover skaber det generelt et bedre arbejdsmiljø, når værktøjer, der er nødvendige for at kunne løse opgaverne, fungerer. Kommunens drift har derfor højeste prioritet og skal sikres igennem klart definerede procedurer og aftaler med driftsleverandører.

Udvikling og anskaffelse af ny teknologi udgør generelt en øget risiko. Både med hensyn til ustabil drift og højt tidsforbrug. Fanø Kommune følger udviklingen tæt, men tager først nye løsninger i brug, når værdi og kvalitet dokumenteret modsvarer investeringen og når implementering kan ske uden nævneværdig risiko for driften.

Derudover skal i-sikkerhedsniveauet naturligvis tilgodese gældende lovgivning, myndighedskrav og samarbejdsaftaler med eksterne parter.

Teknisk anvendes et forsigtighedsprincip, hvor kun nødvendig funktionalitet er aktiveret, i de systemer og tjenester, som giver mulighed for begrænsning.

Indsatsen skal tilpasses de risici, der er følger af kommunens it- og informationsanvendelse. Sikkerhedsniveauet, herunder IT-beredskabet efterprøves løbende, med særlig fokus på højrisikoområder. Der gennemføres endvidere - ved større tekniske eller organisatoriske ændringer – og mindst en gang i en valgperiode en generel opfølgning og risikovurdering.

6. Formidling og uddannelse

Informationssikkerheden vedrører alle medarbejdere og brugere. Beskyttelsen af kommunens data og systemer skal tilrettelægges på en måde, som kræver mindst mulig af den enkelte medarbejder og som påvirker effektiviteten og brugervenligheden mindst muligt. Ansatte i kommunen skal vide hvor og hvornår man skal passe særligt på.

Medarbejdere og andre brugere har selv et ansvar for at holde sig orienteret og for at henvende sig til IT-koordinatoren eller dennes afløser i tvivlsspørgsmål.

Medarbejdere, som har et særligt ansvar for kommunens aktiver, herunder ledere, og projektledere vil være i løbende dialog med IT-koordinatoren.

Medarbejderens leder er ansvarlig for at vurdere, om den pågældende medarbejder har tilstrækkelig viden og kompetencer til at varetage eventuelle i-sikkerhedsopgaver.

7. Brud på i-sikkerheden

Brud på informationssikkerheden er:

- Hændelser, der reducerer sikkerhedsniveauet, dvs. overtrædelser af i-sikkerhedspolitikken.
- Hændelser, der fører til skade på informationsaktiverne.

Hvis en medarbejder konstaterer et sikkerhedsbrud skal dette omgående meddeles IT-koordinatoren og nærmeste leder.

Overfor medarbejdere, som med forsæt bryder sikkerheden, vil disciplinære forholdsregler i overensstemmelse med kommunens gældende regler og personalepolitik bringes i anvendelse. Særligt grove overtrædelser kan medføre bortvisning og politianmeldelse.

Medarbejdere med ledelsesansvar har et aktivt ansvar for at forebygge brud på informationssikkerheden.

8. Retningslinjer for ledere og medarbejdere

Kommunaldirektøren har ansvaret for vedligeholdelsen af politikken og retningslinjerne.

8.1 Ledelsens ansvar og rolle

8.1.1 Kommunaldirektøren

Kommunaldirektørens rolle er at:

- Yde aktiv støtte til gennemførelse af de besluttede initiativer og sikre, at der er forståelse og accept i chefgruppen.
- Behandle spørgsmål af principiel karakter og fastlægge principperne for opfyldelse af politikkens målsætning.
- Sikre, at det besluttede sikkerhedsniveau udmøntes i budgetter og indgår i relevante handlingsplaner.
- Formulere de forretningsmæssige krav til sikkerheden i og omkring systemerne i samarbejde med IT-koordinatoren.
- Foretage en årlig vurdering af, om politik og retningslinjer efterleves i hele kommunen.

Opfølgning over for medarbejdere, som har et ansvar i relation til informationssikkerheden kan eksempelvis ske i forbindelse med medarbejdersamtaler og statusmøder, med udgangspunkt i afsnit 6.

Kommunaldirektøren har endvidere ansvaret for centrale fællessystemer.
Alle væsentlige ændringer og nyudvikling skal risikovurderes og godkendes af kommunaldirektøren inden ændringen gennemføres.

8.1.2 Systemejer / Afdelingsleder

Systemejeren er lederen af den afdeling, der primært anvender systemet. Hvis der er flere brugere, udpeger chefgruppen en systemejer.

Systemejere skal sikre, at retningslinjerne overholdes i alle forretningsgange, hvor systemet anvendes. Det indebærer:

- At sikre etablering af fornuftig databeskyttelse og dataanvendelse i henhold til retningslinjerne.
- Årlig risikovurdering og status på eget område.

Endvidere skal der risikovurderes i følgende situationer:

- Nye systemer
- Nye samarbejder
- Ændrede forhold i omgivelserne
- Nye eksterne krav
- Væsentlige hændelser, som har afdækket utilstrækkelige sikringsforanstaltninger.

Systemejeren har ansvaret for, sammen med IT-koordinatoren, at foretage anmeldelser til Datatilsynet jf. persondataloven, samt:

- at medarbejdere, som behandler personoplysninger i henhold til persondataloven, er bekendt med reglerne og får den fornødne instruktion.
- At regler for ind- og uddata samt anvendelse af it-systemer er beskrevet og opfylder persondatalovens krav.

Sekretariatet og It-koordinatoren sørger for, at kommunens anmeldelser til datatilsynet gennemgås en gang årligt.

Systemejere varetager herudover kontakten til leverandører via IT-koordinatoren og undersøger løbende, om anvendelse, indhold og pris kan optimeres.

8.1.3 Autorisationer

Der skal eksistere en forretningsgang for autorisation og brugeroprettelse, som sikrer at kommunens medarbejdere kun har de rettigheder, de har brug for. Fanø Kommune er en lille kommune og medarbejderne arbejder på tværs af mange områder. Det nødvendiggør, at medarbejdere generelt har mange rettigheder. Derfor lægges der særlig vægt på et højt bevidsthedsniveau hos medarbejderne. Ved ansættelse skal verifikation af medarbejderes kvalifikationer og pålidelighed altid overvejes.

Når en medarbejder første gang skal autoriseres til netværk og et eller flere systemer oplyser den medarbejderansvarlige ledere hvilken funktion medarbejderen har. Tildeling af rettigheder sker på baggrund af et funktions/autorisationsskema, som skal være godkendt af chefgruppen. Autorisationen skal skriftligt godkendes af systemejeren eller nærmeste leder. Oprettelse af brugeren varetages af KSP/CICS administratorer og IT-koordinatoren. Samme procedure følges ved ændringer og intern rokering. Særligt skal det sikres, at fratrådte medarbejdere fratages rettigheder og adgang.

Information om autorisationen, brugernavn og password, returneres fortroligt til brugeren sammen med relevante retningslinjer. Brugeren skal herefter bekræfte accept af retningslinjer.

IT-koordinatoren har udvidede rettigheder til administration af de systemer, Fanø Kommune selv varetager driften af, for at kunne udføre de nødvendige drifts-, support- og vedligeholdelsesopgaver.

Udvidede rettigheder gennemgås en gang årligt af kommunaldirektøren.

8.1.4 Journalisering

Systemejeren har ansvaret for at der udarbejdes en journaliseringsinstruks og for sikkerheden omkring anvendelsen af ESDH systemet

8.1.5 Elektronisk borgerbetjening

Systemejeren har ansvaret for kommunens selvbetjeningsløsninger på systemejerens område.

8.1.6 Digital signatur

Fanø kommune bruger digital signatur til sikker e-mail kommunikation, til håndtering af e-formularer og til på logning på bestemte systemer, som anvendes i den offentlige sektor. Medarbejdere, som har fået en medarbejdersignatur, må kun benytte signaturen til det formål, medarbejderen er autoriseret til.

8.2 IT-koordinatoren

IT-koordinatorens rolle er at:

- Vedligeholde retningslinjerne, så de svarer til politikken.
- Vurderer behovet for risikovurdering ved væsentlige ændringer i og omkring kommunens driftsfaciliteter, større digitaliserings- eller anlægsprojekter mm.
- Udarbejde en årlig samlet status til kommunaldirektøren
- Holde sig ajour med den generelle udvikling på i-sikkerhedsområdet og mindst en gang årligt gennemgå it-installationen for kendte sårbarheder og fejl.

IT-koordinatoren har ansvaret for alt udstyr og for it-infrastrukturen, dvs. fysiske servere, netværk, tekniske sikringsforanstaltninger og rum med it-installationer.

8.2.1 Driftsdokumentation

Kendskabet til it-driftsmæssige og it-tekniske forhold i Fanø Kommune er begrænset til meget få personer. Der skal derfor fastholdes en streng disciplin for udarbejdelse og løbende opdatering af driftsdokumentation. Dokumentationen skal være af en kvalitet, så alle væsentlige driftsopgaver med en begrænset indsats og med kort frist kan overtages af en ekstern leverandør eller flyttes til en anden leverandør. Ved udliciteringer skal kommunen sikre sig ejerskabet af eller adgang til al driftsdokumentation, som er nødvendig for en eventuel flytning. Dokumentationen skal behandles som fortrolig information.

8.2.2 Firewall

Håndteringen af firewall er restriktiv for så vidt angår indgående trafik. Der åbnes kun for et minimum af porte og services og først efter at der er foretaget en konkret risikovurdering. IT-koordinatoren har ansvar for den løbende overvågning af firewall'en og skal mindst årligt verificere afprøvning i forhold til sårbarheder og korrekt konfiguration.

8.2.3 Antivirus

Der skal være etableret aktiv, opdateret virusbeskyttelse på samtlige pc'er og servere på netværket, inden tilslutning.

Udover anvendelse af virusbeskyttelse på pc'er og servere, skal kommunens e-post skannes for spam og malware (vira, orme, trojanere, spyware, ransomware etc.).

8.2.4 Logning

Der anvendes ikke logning udover standard logning i de systemer kommunen anvender. Behov for yderligere logning skal vurderes årligt på baggrund af stikprøver og fejlstatistikker, samt af den enkelte systemejer.

8.2.5 Udvikling, ændringer og anskaffelser

Alle ændringer, udvikling og anskaffelser udføres efter principperne i ITEL8.2.6 Serverrum og fysiske installationer

Servere og kritisk netværksudstyr i administrationsbygningen skal være tilsluttet backupstrøm (UPS og generator) i tilfælde af strømsvigt. Der skal være en procedure, som sikrer at kommunikation er mulig, informationer er tilgængelige, registreres korrekt og beskyttes efter følsomhed, under et systemnedbrud.

Serverrum og krydsfelter skal være sikret mod indbrud, brand og vandskade og adgangen skal begrænses til de nødvendige medarbejdere. Eksterne leverandører, efter konkret vurdering af IT-koordinatoren. Adgangen logges via kommunens låsesystem.

8.2.7 IT-Beredskab

Det skal sikres, at it-understøttelsen af kritiske forretningsprocesser kan retableres efter behov på en alternativ adresse, hvis rådhuset udsættes for en ødelæggende hændelse. Chefgruppen har ansvaret for, at kritiske forretningsprocesser er identificeret og at it-beredskabsbehovet er afdækket. Det er IT-koordinatorens ansvar, at det nødvendige udstyr kan skaffes og at styre etablering af et midlertidigt miljø på den alternative adresse.

8.3 Medarbejdere og interne brugere

Inden der gives adgang til kommunens systemer og data skal medarbejderen gøres bekendt med kommunens i-sikkerhedspolitik.

8.3.1 Internet

Alle kommunens it-brugere har fri adgang til internettet. Følgende regler skal overholdes:

- Det er ikke tilladt at lægge kommunens data på internettet.
- Det er ikke tilladt at hente og installere programmer fra internettet uden IT-koordinatorens forudgående vurdering og godkendelse.
- Det er kun tilladt at besøge netsteder, som brugeren har god grund til at have tillid til.
- Det er naturligvis ikke tilladt at hente eller distribuere ulovligt og ophavsretligt beskyttet indhold.
- I tvivlsspørgsmål skal der rettes henvendelse til IT-koordinatoren.

8.3.2 E-mail

Alle medarbejdere i kommunen, som har en arbejds pc, og som også har en e-mail adresse, kan i begrænset omfang benytte denne til private, lovlige formål.

Fortrolige eller personfølsomme oplysninger skal altid sendes på en måde, så vi sikrer os, at uvedkommende ikke kan få adgang til indholdet. Også hvis der forventes et svar retur, som kan indeholde følsomme oplysninger. Da skal adressen sikkerpost@fanoe.dk benyttes. Post ud af kommunen skal sendes med sikker e-post/digital post. Fortrolige og personfølsomme oplysninger kan fx være henvendelser som indeholder cpr-nummer, helbredsoplysninger eller oplysninger om en persons økonomi.

Alle medarbejdere, der har en e-postkasse, har mulighed for at sende sikker e-post. E-post journaliseres efter samme principper som øvrige dokumenter.

8.3.3 Arbejds-pc

Medarbejdere må ikke selv installere programmer, tilføjelser eller udvidelser på arbejdspc'en. Ved særlige behov rettes henvendelse til IT-koordinatoren. Det er ikke tilladt at gemme kommunens eller andres data på lokale harddiske, usb-nøgler eller andre medier. Kommunens ESDH system eller det relevante forretningssystem **skal altid** benyttes.

8.3.4 Bærbare og fjernopkoblinger

Der er mulighed for sikker fjernopkobling til kommunen via internettet. Alle Fjernopkoblinger skal foregå via Citrix løsningen, med undtagelse af mail og intranettet, der kan tilgås udefra ved brugerid og password. IT-koordinatoren administrerer fjernopkoblinger.

8.3.5 Trådløs netværk

IT koordinatoren har ansvaret for netværket, og skal derfor godkende de brugere, der har adgang til de trådløse net. Undtaget er det åbne gæste net. Al trådløs trafik skal være krypteret og logges.
IT koordinatoren skal godkende "Access punkter", dvs. udstyr der giver trådløs netadgang på kommunens netværk.

8.4 Samarbejdspartnere og eksterne brugere

Fanø Kommune anvender kun leverandører med et højt sikkerhedsniveau og sund økonomi.

8.4.1 Samarbejdet med Esbjerg Kommune

Medarbejdere i Esbjerg Kommune er underlagt samme regler som Fanø kommunes egne medarbejdere, beskrevet i afsnit 8.3. Kommunens almindelige autorisationsprocedurer skal følges.

8.4.2 Samarbejde med andre myndigheder

Ledere har ansvaret for, at medarbejdere er bekendt med og efterlever andre myndigheders sikkerhedsregler. Kommunaldirektøren og IT-koordinatoren skal konsulteres inden samarbejder iværksættes for at sikre, at kommunens egne sikkerhedsregler ikke er i strid med aftalen og at de aktuelle tekniske og fysiske forhold lever op til den eksterne myndigheds krav.

8.4.3 Samarbejde med KMD og andre leverandører

Drift, udvikling og support af it-løsninger kan efter behov varetages af eksterne leverandører. Fanø Kommune har dog stadig det forretningsmæssige ansvar. Kommunaldirektøren har ansvaret for at samarbejdsaftalen ikke er i strid med kommunens sikkerhedsregler. IT-koordinatoren har ansvar for at reglerne og den indgåede aftale overholdes. Se endvidere afsnit 4.

8.4.4 Kommunens hjemmeside

Fanø Kommunes hjemmeside indeholder informationer til borgere, foreninger, turister, besøgende og erhvervsliv. Borgerservice har ansvaret for vedligeholdelse og drift af hjemmesiden og for publicering af indhold. IT-koordinatoren har ansvaret for at den tekniske sikkerhed hos hosting leverandøren lever op til kommunens krav.

Der må ikke publiceres fortroligt indhold på hjemmesiden.

9. Opfølgning og evaluering

Udviklingen i digitaliseringen af den offentlige forvaltning går stærkt og forudsætningerne for den aktuelle politik kan derfor også ændre sig på kort tid. Det betyder, at politikken og sikkerhedsbehovet løbende må revurderes.

En gang årligt eller efter behov drøfter chefgruppen status, med udgangspunkt i følgende punkter:

- Orientering fra IT-koordinatoren om drifts- og kapacitetsmæssige forhold, samt eventuelle væsentlige sikkerhedshændelser siden sidst, ændringer af betydning for kommunen som følge af fællesoffentlige digitaliseringstiltag og andre samarbejder mv.
- Orientering fra afdelingsledere om status på egne sikkerhedsbehov og udfordringer.

- Generelle ændringer i trusselsbilledet og sikkerhedsbehovet
- Beredskabsplanens aktualitet
- Efterleves politikken godt nok.
- Betydningen af it-understøttelsen for kommunen.

- Er politikken stadig aktuel?
- Har vi de rette leverandører?
- Er funktions/autorisationsskemaet retvisende?
- Evt.

IT-koordinatoren udfører efter aftale med kommunaldirektøren og chefgruppen en række kontroller af efterlevelsen. Eksempler herpå er:

-
- Rettighedsadministration
- Udstyr på netværket
- Opfølgning på leverandørers efterlevelse af aftaler
- Ad hoc undersøgelser på baggrund af konkrete hændelser, mistanker etc.

10. Implementering af politikken

Implementeringen omfatter følgende aktiviteter:

- Sikre, at i-sikkerhedspolitikken og afledte bilag implementeres.
- Sikre en bestemmelse af værdien af de informationer, som er nødvendige for kommunen, samt at træffe rimelige forholdsregler til beskyttelse af disse informationer, herunder at afse de nødvendige midler og ressourcer hertil.
- At ansvaret for alle væsentlige informationer og informationssystemer placeres entydigt
- At klassificere og beskytte de informationer, som kommunen har ansvaret for.
- At forebygge og begrænse risici til en for kommunen kendt og accepteret størrelse.
- At udarbejde regler for informationskontrol og beskyttelse, som skal følges af de medarbejdere, der behandler og anvender informationerne.
- At etablere regler for adgang og brug af informationer samt at sikre, at reglerne bliver revideret med jævne mellemrum.
- At definere reglerne for arkivering af informationer, således at disse altid kan genskabes senere inden for en kendt og accepteret tidshorisont.
- At udarbejde en brugbar plan til at retablere daglig drift, såfremt informationerne eller informationssystemerne ødelægges, uanset af hvilken grund, således:
    - At omfanget af og konsekvenserne ved nødsituationen kan minimeres.
    - At væsentligste dele af den daglige forretningsmæssige drift i kommunen kan gennemføres via alternative, midlertidige forretningsgange.
    - At alle relevante berørte parter kan holdes orienteret i fornødent omfang.
    - At den fulde drift af informationssystemerne kan genoptages inden for en kendt og accepteret tidshorisont.
- At sikre, at enhver sikkerhedsmæssig følsom informationsaktivitet kan henføres til den person, som har udført aktiviteten, samt at sikre gennemførelse af de fornødne kontroller til opdagelse af misbrug eller forsøg herpå.
- At etablere regler for rettighedstildeling og funktionsadskillelse, som skal forebygge og begrænse konsekvenser af fejl, uheld og negative handlinger, der bevidst er foretaget af enkeltpersoner.
- At sikre at kommunens udvikling og implementering af systemer og services udføres under iagttagelse af betryggende sikkerhedsforanstaltninger.
- At sikre, at kommunens leverandører overholder de sikkerhedsforskrifter, som er gældende for kommunens informationer, faciliteter og medarbejdere i samarbejdet med virksomheden.

- At træffe de nødvendige forholdsregler for at sikre, at i-sikkerhedspolitikken og afledte retningslinjer bliver overholdt.
- At udarbejde den fornødne ledelsesrapportering om status for informationssikkerheden, herunder aktiviteter og hændelser.

Bilagsoversigt

A: Oversigt over systemejere Dok.nr. 563-2015-6376

B: IT-Beredskabsplaner for særlige kritiske systemer f.eks. omsorgssystem

KMD Care Dok.nr.563-2016-5584
Kritisk infrastruktur

C: Funktions / autorisationsskema

Dok.nr. 563-2016-6305