Staben
Middelfart Kommune
Nytorv 9
5500 Middelfart
www.middelfart.dk

Telefon +45 8888 5500
Direkte +45 8888 5011
Fax +45 8888 5501

hanne.thouber@middelfart.dk

Dato: 16. marts 2023
Sagsnr.: 2023-000980-2

Organisering og styring af informationssikkerhed

Middelfart Kommunes *overordnede informationssikkerhedspolitik* skaber rammer for organisering af ansvar og styring af informationssikkerheden. Den overordnede politik bliver udmøntet i regler og procedurer for hvordan vi håndterer informationssikkerhed. Det er grundlaget for vores daglige arbejde med informationssikkerhed i Middelfart Kommune.

Informationssikkerhedsbeskrivelsen består af tre dokumenter.

- ***Den overordnede informationssikkerhedspolitik***.
- ***Organisering og styring af informationssikkerhed***
- ***Informationssikkerhedsregler***.

Organisering og styring af informationssikkerheden bliver, ligesom den overordnede informationspolitik, godkendt af Byrådet. De skal revideres mindst én gang årligt. *Informationssikkerhedsreglerne* godkendes efter behov af den øverste sikkerhedsansvarlige. *Informationssikkerhedsreglerne* er de konkrete regler, som alle medarbejdere skal kende og overholde i forbindelse med deres daglige arbejde.

Dokumentet er lavet med udgangspunkt i ISO27001-standarden.
De tre dokumenter danner grundlaget for en sikker håndtering af informationer i Middelfart Kommune.

Organisationens sammenhæng

Middelfart Kommunes administrative organisation består af en Direktion bestående af en kommunaldirektør og tre forvaltningsdirektører med tilhørende forvaltninger og driftsafdelinger under sig. Kommunaldirektøren har Staben (inkl. IT-afdelingen), Løn og Økonomi samt Job- og Vækstcenter som stabe under sig.

Følgende parter er relevante for informationssikkerheden.

- Ansatte i kommunen
- Borgere og virksomheder
- Leverandører og eksterne samarbejdspartnere
- Datatilsynet

Følgende to målsætninger konkretiserer behov og forventninger fra interne og eksterne parter:

1. Fortrolighed i forvaltningen
   Vi vil sikre, at behandling af data og informationer sker fortroligt og i overensstemmelse med god forvaltnings- og databehandlingsskik. Vi vil sikre, at informationer om borgere og virksomheder ikke kommer til uvedkommendes kendskab.

2. Sikre at kommunens medarbejdere, borgere og virksomheder har adgang til en stabil og korrekt kommunal service
   Vi vil sikre borgere og virksomheder tilgængelighed og pålidelig og sikker adgang til de eksisterende systemer på www.middelfart.dk og selvbetjeningsløsninger.

For de interne systemer skal der sikres stabil drift. IT-anvendelsen skal bygge på korrekte data. Vi ønsker at sikre korrekt service til tiden.

Forebyggende sikkerhed
Vi indfører forebyggende tekniske tiltag og kampagner af informativ karakter. F.eks gennem udvikling af medarbejdernes kompetencer og viden om informationssikkerhed.

Tekniske kontroller er væsentlige og sikrer en del. Men brugeradfærd ses som den største risikofaktor. Vi er derfor afhængige af medarbejdernes kompetencer og forståelse af deres rolle i forbindelse med informationssikkerhed. Ved at højne medarbejdernes kompetencer, får vi et højere niveau af sikkerhed.

Vi definerer informationssikkerhed som kommunens samlede tiltag til at sikre fortrolighed, tilgængelighed og integritet. Tiltag der både inkluderer tekniske, proceduremæssige, regel- og lovmæssige kontroller.

Juridiske krav som Middelfart Kommune bestræber sig på at omsætte i forbindelse med informationssikkerhed:

- Databeskyttelsesforordningen
- Databeskyttelsesloven
- Sikkerhedsforanstaltninger som svarer til sikkerhedsbekendtgørelsen og sikkerhedsvejledningen
- Forvaltningsloven
- Offentlighedsloven
- Arkivloven

Kontraktlige forpligtelser, der påvirker informationssikkerheden:

- Kontrakter på it-løsninger og samarbejde med eksterne parter
- Databehandleraftaler
- Licensstyring
- Ansættelsesbreve, således at nyansatte medarbejdere allerede før ansættelsen er bekendte med, at de i deres arbejde skal overholde kommunes regler for informationssikkerhed.

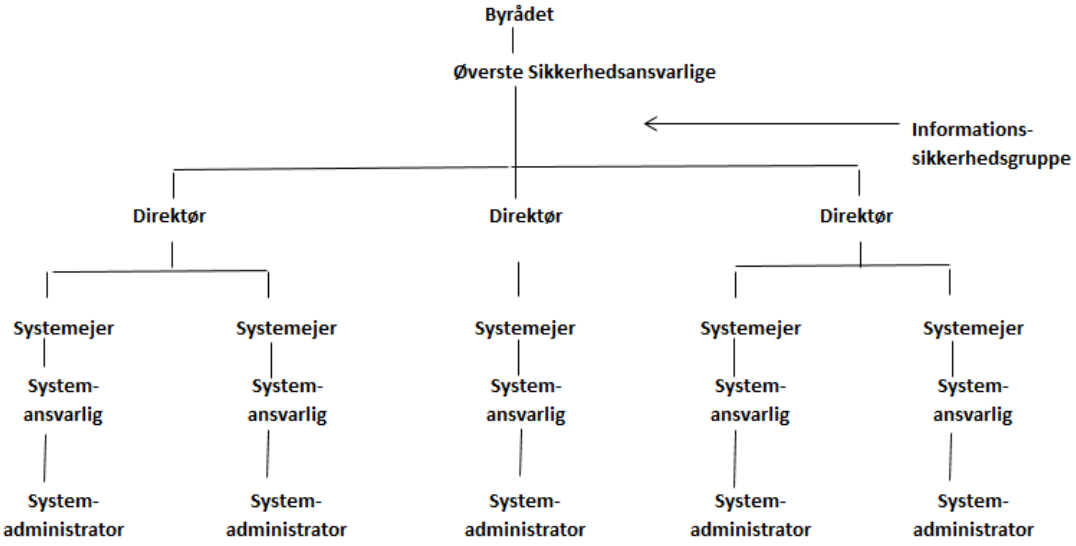
Anvendelsesområdet for informationssikkerhedsregler

Informationssikkerhedsreglerne gælder for alle organisatoriske enheder i Middelfart Kommune. Politikere og administration er underlagt reglerne. Det samme er eksterne parter, der har adgang til Middelfart Kommunes data.

Reglerne gælder for informationer både i digital form og fysisk.

Roller, ansvar og beføjelser i organisationen

Sikkerhedsorganisation



Byrådet er dataansvarlige.

Informationssikkerheden varetages af Løn- og Økonomichefen, der er øverste sikkerheds-ansvarlige.[1]

Det daglige arbejde udføres i samarbejde med Sikkerhedsorganisationen. Denne består af den øverste sikkerhedsansvarlige, direktører og systemansvarlige. Ofte med bistand fra Informationssikkerhedsgruppen.

Sikkerhedsorganisationen har ansvar for at sikre, at regler og politik for informationssikkerhed er synlig, koordineret og i overensstemmelse med kommunens overordnede principper og mål for informationssikkerhed.

Ansvar for tilsyn og koordinering af sikkerheden på tværs af organisationen påhviler den øverste sikkerhedsansvarlige.

Direktører skal sikre udbredelse af informationssikkerhedsbeskrivelsen til egne medarbejdere. Direktørerne skal endvidere sikre at informationssikkerheden overholdes, dels i de fagspecifikke områder og dels i fagsystemer inden for eget ansvarsområde.

Kompetence- og opgavefordeling i sikkerhedsorganisationen:

Øverste sikkerhedsansvarlige har følgende kompetencer, opgaver og er ansvarlig for

- Tilsyn og koordinering af sikkerhed på tværs i organisationen, herunder overholdelse af kommunens informationssikkerhedsbeskrivelse.
- Udarbejdelse af informationssikkerhedsregler, dvs. de konkrete regler for behandling af personoplysninger. Reglerne laves med udgangspunkt i ISO27001 standarden for informationssikkerhed.
- Årlig revision af den overordnede informationssikkerhedspolitik og organisering og styring af informationssikkerhed, samt at den forelægges Byrådet.
- Gennemgang af informationssikkerhedsregler efter behov. Det skal dog ske mindst én gang hvert år for at sikre, at de er fyldestgørende og afspejler de faktiske forhold i kommunen.

[1] Kommunaldirektøren er som udgangspunkt øverste sikkerhedsansvarlige, men kompetencen som øverste sikkerhedsansvarlige er pr. 16. marts 2023 delegeret til Løn- og Økonomichefen.

- At der er lavet fortegnelser over de behandlinger, som bliver foretaget i kommunen, herunder at sikre en årlig opdatering af fortegnelserne.
- At lave en procedure til håndtering og dokumentation af brud på persondatasikkerheden.
- At fastsætte en instruks til systemejer/systemansvarlige om krav til systemmæssig sikkerhed.
- At der udføres en overordnet risikovurdering af kommunens systemportefølje. Den opdateres én gang årligt i forbindelse med revision af informationssikkerhedsbeskrivelsen.
- Skal aktivt lede og støtte de medarbejdere, hvis opgave er at vedligeholde informationssikkerheden.

Direktørerne er – indenfor eget område – ansvarlige over for øverste sikkerhedsansvarlige, kommunens informationssikkerhedsbeskrivelse bliver overholdt.

Direktørerne er ansvarlige for;
- At der udpeges systemejer som ansvarlig for det enkelte system.
- At der udpeges systemansvarlig for det enkelte system til bl.a. at varetage det daglige sikkerhedsansvar.
- At der fastlægges instrukser, der fastlægger ansvaret for anvendelsen af it-udstyr.

Systemejer er ansvarlig for et system. Vedkommende er chef/leder og udpeget af topledelsen.

Systemansvarlig har det daglige ansvar for, at systemet overholder de sikkerhedsmæssige krav beskrevet i informationssikkerhedsbeskrivelsen.

Den systemansvarlige er endvidere ansvarlige for;
- At varetage det daglige sikkerhedsansvar for databehandlingen i systemerne og påse, at informationssikkerhedsreglerne for databehandlingerne til enhver tid overholdes.
- At overholde instruks om krav til systemmæssig sikkerhed.
- At der indgås en skriftlig databehandleraftale med leverandør, og evt. underleverandør, når dette er påkrævet.
- At der foretages årlige risikovurdering af systemerne.

Systemadministrator er ansvarlig for at implementere, opsætte og vedligeholde parametre i systemet og for second-line-support, samt for at kommunikere fejl, planlagte og uplanlagte driftsnedbrud mv.

Direktionens rolle og engagement
Direktionen skal inddrages og sikre ledelsesmæssig forankring af kommunens informationssikkerhed. Det indebærer, at Direktionen skal sikre, at ledere på alle niveauer støtter kommunens informationssikkerhed ved at udlægge klare retningslinjer, udvise synligt engagement samt sikre præcis placering af ansvar.

Det er Direktionens ansvar at sikre, at kommunens informationssikkerhed prioriteres som en vigtig ledelsesmæssig opgave, således at alle ledere forpligtes til at sørge for at egne medarbejdere:
- Er tilstrækkeligt informeret om deres roller og ansvar i forbindelse med informationssikkerhed
- Tilegner sig kompetencer og et opmærksomhedsniveau i spørgsmål vedrørende informationssikkerhed, der er i overensstemmelse med deres roller og ansvar i kommunen.

Direktionen skal sikre, at alle ledere kommunikerer betydningen af overholdelse af kravene til informationssikkerhed.

Direktionen skal aktivt fremme og støtte løbende forbedringer af informationssikkerheden.

Informationssikkerhedsgruppen
Informationssikkerhedsgruppen består af følgende repræsentanter:
Øverste sikkerhedsansvarlige, it-cheferne, digitaliseringskonsulent, konsulent fra det administrative område, jurist og kommunens databeskyttelsesrådgiver.

Informationssikkerhedsgruppen er en rådgivende gruppe, der hjælper øverste sikkerhedsansvarlige med udførelse af sine opgaver.

Informationssikkerhedsgruppen sikrer den løbende risikovurdering. Samtidig skal gruppen sikre information, der støtter ledelsen i deres arbejde med informationssikkerhed.

Informationssikkerhedsgruppen mødes straks ved alvorlige informationssikkerhedshændelser.

IT afdelingens rolle
I tilfælde af informationssikkerhedshændelser skal der straks tages kontakt til IT-afdelingen. Håndtering af nedbrud på IT-systemer varetages ligeledes af IT-afdelingen.

Ved registrering af informationssikkerhedshændelse træffer øverste sikkerhedsansvarlige og IT-chefen beslutning om handling og om Informationssikkerhedsgruppen skal indkaldes.

Distribution af informationssikkerhed
Viden om informationssikkerhed skal bredes ud i hele kommunens organisation. Det kan f.eks. ske på afdelingsmøder, møder mellem systemansvarlige eller gennem kampagner der hæver vidensniveauet og lignende.

Informationssikkerhedsbeskrivelsen skal være tilgængelig for alle medarbejdere på kommunens Intranet.

Sikkerhedsbevidsthed

Uddannelse i informationssikkerhed
Nye medarbejdere skal ved introduktionen præsenteres for den overordnede informationssikkerhedspolitik. Her skal også indgå en kort gennemgang af informations-sikkerhedsreglerne.

Alle medarbejdere skal læse og sætte sig ind i de tre dokumenter, der tilsammen udgør informationssikkerhedsbeskrivelsen.

- Den overordnede informationssikkerhedspolitik
- Organisering og styring af informationssikkerhed
- Informationssikkerhedsregler, dvs. de konkrete regler

Den løbende kompetenceudvikling af medarbejderne i informationssikkerhed varetages af ledelsen. Ledelsens arbejde støttes af jævnlige tiltag fra informationssikkerhedsgruppen. Gruppen kan formidle på følgende måder: e-mail, video til afspilning på afdelingsmøder, opslag på kommunens intranet, skabeloner og hjælpeværktøjer, workshops, møder mv.

Evaluering og tilsyn og opfølgning på informationssikkerhed

Én gang årligt skal der laves en systematisk opfølgning på overholdelse af informationssikkerhedsbeskrivelsen i organisationen. Resultatet skal rapporteres til Direktionen.

Den øverste sikkerhedsansvarlige skal analysere resultaterne af den overordnede risikovurdering og risikohåndtering af forretningskritiske systemer. Og ud fra dette skal der ses på muligheder for løbende forbedringer. Informationssikkerhedsgruppen hjælper til med dette.

Informationssikkerhedsgruppen foretager tilsyn og intern kontrol af afdelingernes arbejde med sikkerhed.

Den interne kontrol skal sikre, at informationssikkerhedsbeskrivelsen er velimplementeret i organisationen. Vi vil sikre, at ansvar og regler overholdes. Denne kontrol forventes at ske i forbindelse med ledelsestilsynet. I dette tilsyn bør beskrivelser af årsager til afvigelser fra ansvar og regler beskrives. Samtidig skal der laves en handlingsplan, der beskriver, hvordan afvigelserne håndteres.

Kontrollen af sikkerhed for fagsystemer bliver foretaget som stikprøve. Udvælgelse af fagsystemer foretages af Informationssikkerhedsgruppen.

Informationssikkerhedsgruppen gennemgår og vurderer behov for revision af informationssikkerhedsbeskrivelsen én gang om året. Informationssikkerhedsbeskrivelsen revideres endvidere, når de forretningsmæssige behov eller virksomhedens mål ændres.

Håndtering af informationssikkerhedshændelser

Sikkerhedshændelser hos outsourcing-leverandør
Leverandøren skal registrere alle sikkerhedshændelser, dvs. brud på fortrolighed, tilgængelighed eller integritet. Middelfart Kommune og leverandøren skal gennemgå eventuelle sikkerhedshændelser sammen. Der skal tages skridt til, at sådanne situationer ikke sker igen.

Tilgængelighedshændelser
Hændelser, der har indflydelse på tilgængelighed, skal afklares i henhold til driftsaftaler. Driftshændelser skal udløse procedurer for hændelseshåndtering. De ramte brugere og systemejere/systemansvarlige skal informeres.

I tilfælde af afvigelser fra sikringstiltagene, skal IT-chefen håndtere hændelsen og afbøde evt. negative konsekvenser.

Hændelser, korrigerende handlinger og effekten af korrigerende handlinger drøftes på møder i Informationssikkerhedsgruppen. Ovennævnte hændelser m.v. dokumenteres i mødereferater.

Information om sikkerhedshændelser
Kommunen skal informere interne og eksterne parter, der måtte være berørt af eventuelle sikkerhedshændelser.

Den øverste sikkerhedsansvarlige skal godkende meddelelser til de berørte parter og håndtere eventuel presseomtale.

Opfølgning på rapporterede sikkerhedshændelser
Databeskyttelsesrådgiver indsamler alle rapporterede sikkerhedshændelser og orienterer i fornødent omfang øverste sikkerhedsansvarlige.

Informationssikkerhedsgruppen skal behandle større sikkerhedshændelser.

Overtrædelse af informationssikkerhedsregler
Det er ledelsens ansvar, at sanktioner for brud på kommunens informationssikkerhed håndteres konsekvent og i overensstemmelse med gældende lovgivning.

Ved overtrædelse informeres øverste sikkerhedsansvarlige. I samarbejde med Informationssikkerhedsgruppen aftales det, hvilken sanktion overtrædelsen skal resultere i.

Rapportering af informationssikkerhedshændelser
Informationssikkerhedshændelser skal rapporteres til databeskyttelsesrådgiver på dpo@middelfart.dk

\- O –

Organisering og styring af informationssikkerhed er godkendt af Byrådet på møde den 11. april 2023.