Kerteminde Kommune

Informationssikkerhedspolitik

Indholdsfortegnelse

Versionshistorik

Udarbejdet/Revideret af - Dato:	Godkendt - Dato:
Mofa - 11/06/2019	Informationssikkerhedsudvalg - 04/06/2019

1 Indledning

Kerteminde Kommune arbejder aktivt med informationssikkerhed, cybersikkerhed, samt databeskyttelseslov. Denne politik skal udstikke retningen for dette arbejde.

Kerteminde Kommune behandler, i kraft af den myndighedsudøvelse kommunen er ansvarlig for, personoplysninger, heriblandt også følsomme personoplysninger. Der er tale om oplysninger om borgere, virksomheder og frivillige organisationer, men også om kommunes egne ansatte. Mængden af oplysninger, der behandles, vokser hele tiden i takt med digitaliseringen af opgaverne i dagligdagen.

Kerteminde Kommune skal naturligvis passe godt på de oplysninger, vi indsamler og modtager. Dette gøres ved at fokusere på både informationssikkerhed og cybersikkerhed ved hjælp af ISO 27001 standarden, som er internationalt anerkendt. Samt ved at sikre efterlevelse af Databeskyttelsesforordningen. Derved sikres de organisatoriske og teknologiske forudsætninger for, at persondata behandles forsvarligt og sikkert i kommunes varetægt.

Med afsæt i ovenstående skal indeværende dokument angive retningen for Kerteminde Kommunes arbejde med informationssikkerhed, der lægges endvidere vægt på compliance ift. Databeskyttelsesforordningen, samt Databeskyttelsesloven (Lov nr. 502 af 23/5/2018).

Denne Informationssikkerhedspolitik vil blive suppleret af en informationssikkerhedshåndbog. Håndbogen følger den internationale standard ISO 27001. Denne standard er udviklet med det formål at stille krav til implementering, vedligehold og løbende forbedring af ledelsessystem for informationssikkerhed. Informationssikkerhedshåndbogen findes separat og vil løbende blive opdateret i takt med tiltagende krav på området.

2 Formål

Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger er en grundlæggende rettighed. Herudover er der behov for i myndighedsudøvelsen at udveksle personoplysninger internt i kommunen for at leve op til vores myndighedsansvar. Nogle oplysninger behandles af kommunen med hjemmel i lovgivning, andre oplysninger kræver samtykke fra borgeren jf. databeskyttelsesforordningen.

Formålet med Informationssikkerhedspolitikken er at sætte de overordnede rammer for de initiativer, der skal beskytte personoplysninger, information og informationssystemer, som anvendes i Kerteminde Kommune.

Desuden er der fokus på, at gældende lovgivning og myndighedskrav overholdes. Dette indebærer iagttagelse af Databeskyttelsesloven, Databeskyttelsesforordningen samt ISO 27001.

Indeværende politik skal ligeledes understøtte Kerteminde Kommunes arbejde med at sikre stabil drift af organisationen, herunder minimering af risikoen for tab af, eller misbrug af Kerteminde Kommunes data, med evt. økonomiske og omdømmemæssige konsekvenser til følge.

3 Omfang

Politikken omfatter:

- **Alle IT-løsninger, der anvendes af Kerteminde Kommunes medarbejdere, ligeledes alle oplysninger, der behandles heri f.eks. personoplysninger af både almindelig og følsom karakter.**

- **Alt fysisk materiale og udstyr, der anvendes til at behandle oplysninger**
- **Alle lokationer hvor der behandles og opbevares data, herunder persondata**

Informationssikkerhedspolitikken gælder også for eventuel udliciteret drift, samt services indkøbt ved eksterne leverandører. I tilfælde hvor Kerteminde Kommune indkøber leverandører til at udføre behandling af personoplysninger indgås en databehandleraftale jf. Databeskyttelsesforordningens krav hertil.

Informationssikkerhedspolitikken er gældende for Kerteminde Kommunes politiske og administrative organisation, samarbejdspartnere og øvrige brugere af kommunens udstyr, systemer og netværk.

4 Principper og retningslinjer

I Kerteminde Kommune anvendes en risikobaseret tilgang til informationssikkerhed. Herved forstået, at sikkerhedskravene ikke er statiske, men derimod tilpasses de enkelte løsninger og situationer. Således undgås at bruge ressourcer på tiltag, som enten er uden effekt, eller ude af proportioner i forhold til anvendelsen. Endvidere vil der løbende blive lavet justeringer, som følge af gentagne risikovurderinger.

Det er essentielt at informationssikkerhedspolitikken er kommunikeret ud til, og tilgængelig for kommunens medarbejdere, samt øvrige interessenter, hvor dette er relevant.

4.1 Principper fra ISO 27001

Den internationale standard ISO 27001 er bygget op omkring principperne: Fortrolighed, integritet og tilgængelighed. Herudover er en hjørnesten risikostyring, hvilket giver den fleksibilitet, at vi via risikovurderinger kan afgøre det relevante niveau af sikkerhed, en given proces eller en løsning pålægges.

Løbende forbedring af informationssikkerheden i Kerteminde Kommune, samt forankring i øverste ledelse er ligeledes hjørnesten i ISO 27001 standarden, som anvendes i Kerteminde Kommune. Det er derfor essentielt at både direktionen og den politiske ledelse er bekendt med denne politik.

4.2 Principper fra Databeskyttelsesforordningen

Databeskyttelsesforordningens grundprincipper for behandling af personoplysninger er:

- **Lovlighed, rimelighed og gennemsigtighed**
- **Formålsbegrænsning**
- **Dataminimering**
- **Rigtighed**
- **Opbevaringsbegrænsning**
- **Integritet og fortrolighed**
- **Ansvarlighed**

Principperne følger af Databeskyttelsesforordningens Artikel 5. og udgør ”grundstammen”, hvoraf den øvrige lovgivning er afledt.

5 Ansvar og roller

Kerteminde Kommunes Byråd har overordnet ansvar for informationssikkerheden i kommunen. I det daglige varetages implementering og drift i Informationssikkerhedsudvalget, som delegerer til Informationssikkerhedskoordinatoren. Rollerne er udtømmende beskrevet i Informationssikkerhedshåndbogen.

- **Byrådet**
  - Fastlægger og godkender Informationssikkerhedspolitikken.
- **Økonomi Udvalget**
  - ØU varetager den umiddelbare forvaltningen af Informationssikkerhedsområdet

- **Øverste sikkerhedsansvarlige**
  - Kommunaldirektøren er øverste ansvarlige for informationssikkerheden i Kerteminde Kommune, Informationssikkerhedsudvalget er udførende på opgaven.
  - Kommunaldirektøren har ligeledes ansvaret for at der udformes en Informationssikkerhedspolitik, samt håndbog.
- **Informationssikkerhedsudvalget**
  - Udpeges af kommunaldirektøren.
  - Bestående af relevante chefer og Databeskyttelsesrådgiver (DPO).
  - Udvalget lægger informationssikkerhedspolitikken op til direktionen, som indstiller til godkendelse i byrådet.
  - Informationssikkerhedskoordinatoren er sekretær for udvalget.
- **DPO - Databeskyttelsesrådgiver**
  - Databeskyttelsesrådgiveren udpeges af øverste sikkerhedsansvarlige jf. Databeskyttelsesforordningens Artikel 37, stk. 1 litra a.
  - Databeskyttelsesrådgiveren varetager funktioner angivet i Databeskyttelsesforordningens art. 39
    - Databeskyttelsesrådgiveren rådgiver og vejleder kommunens politikere og medarbejdere om regler og politikker ift. håndtering af personoplysninger.
- **Systemejer**
  - Systemejerrollen bestrides af afdelingscheferne. Den enkelte systemejer har det fulde ansvar for systemets anvendelse i kommunen, herunder tekniske og organisatoriske foranstaltninger der efterlever det ønskede niveau herfor.

6 Informationssikkerhedsniveau

Informationssikkerhedspolitikken er baseret på gældende lovgivning indenfor informationssikkerhed, god itskik og best-practice på området. Informationssikkerhedshåndbogen er udarbejdet med ISO 27001 som referenceramme. Informationssikkerhedsniveauet fastsættes på baggrund af risikovurderinger, således at informationssikkerheden er afstemt efter behovet i kommunens data og systemer. Hermed tilrettelægges de sikkerhedsforanstaltninger der iværksættes, således at de modsvarer de identificerede risici for det pågældende område.

Risikovurderinger gennemføres med passende interval for kritiske forretningsprocesser og dertilhørende digitale løsninger, ligeledes ved indkøb af løsninger og tjenester i bredere forstand. Ved ibrugtagning af løsninger vurderes endvidere behovet for risikovurderinger, samt kadencen for disse. Ligeledes fastlægges her niveauet af sikkerhedsforanstaltninger, der anses for relevant for det enkelte system.

7 Informationssikkerhedsbevidsthed

Kerteminde Kommunes Informationssikkerhedspolitik omfatter den samlede systemanvendelse i kommunen, men også det samlede flow af oplysninger i kommunen, både internt, men også kommunikation rettet mod borgere og samarbejdspartnere. Informationssikkerhedspolitikken gælder for både digitale og fysiske oplysninger, hvilket det også er relevant at skabe en bevidsthed om i hele Kerteminde Kommune. I forlængelse heraf skal informationssikkerhed også tænkes ind i den fysiske sikring af kommunens lokationer.

Udmøntning og kommunikation af Informationssikkerhedspolitikken og Informationssikkerhedshåndbogen målrettes alle ansatte i Kerteminde Kommune. Alle medarbejdere vil ved ansættelsen blive instrueret i gælden regler og praksis vedr. informationssikkerhed.

Der vil løbende pågå et arbejde med at kommunikere til samtlige medarbejdere om informationssikkerhed, blandt andet via målrettede og brede awareness-kampagner.

Det er den enkelte leders ansvar, at deres medarbejdere løbende holder sig orienteret ift. informationssikkerhed relevant for deres område.

8 Persondata

Kerteminde Kommune håndterer i sin forvaltning en bred vifte af persondata. Persondata kan have forskellige beskyttelsesbehov alt efter karakteren. Behandlingen af almene persondata, særligt personfølsomme data og data knyttet til lovovertrædelser, nyder alle beskyttelse efter reglerne i Databeskyttelsesforordningen og behandles i overensstemmelse med principperne i nærværende informationssikkerhedspolitik punkt 4.2.

9 Overtrædelse

Hver enkelt leder og medarbejder er ansvarlig for at efterleve reglerne for Informationssikkerhed i Kerteminde Kommune.

10 Godkendelse og opdatering

Informationssikkerhedspolitikken godkendes i byrådet.

Politikken opdateres minimum hvert fjerde år, eller i tilfælde af større organisatoriske ændringer, som kan have følger herfor. Efter opdatering godkendes politikken på ny af byrådet.

11 Ordforklaring

ISO 27001 – Internationalt anerkendt standard for informationssikkerhed. Databeskyttelsesforordningen tilsiger at der arbejdes risikobaseret og standardiseret, ISO 27001 er eneste anerkendte standard på informationssikkerhedsområdet.

Compliance – Dette betyder at vi lever op til lovens ord på det enkelte område.

Awarenes – Bevidsthedstiltag med små videoklip om Databeskyttelsesforordningen (GDPR).

EU-Forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger – Generel forordning om databeskyttelse.

Lov om supplerende bestemmelser til EU-forordningen (Databeskyttelsesforordningen).