Allerød Kommune

ISO: 27001:2022

Informationssikkerhedspolitik for Allerød Kommune

Sagsnr. 21/8356

Indledning

Direktionen i Allerød Kommune har besluttet, at denne informationssikkerhedspolitik (herefter benævnt sikkerhedspolitik) er den overordnede ramme for den generelle informationssikkerhed i hele organisationen.

Informationssikkerhed betyder både beskyttelse af informationer i it systemer og fysisk sikring af lokaler, arkiver og udstyr, samt brugernes anvendelse heraf.

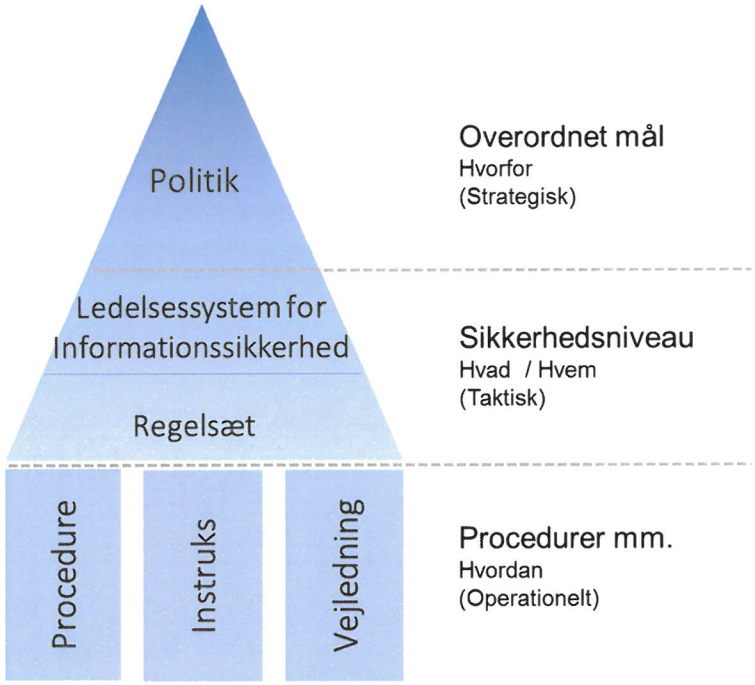
Målet med en sikkerhedspolitik er, at Allerød Kommune fremstår som en sikker, troværdig og pålidelig organisation over for kommunens borgere, samarbejdspartnere og den øvrige offentlighed.

Sikkerhedspolitikken og informationssikkerhedshåndbogen er tilgængelig på kommunens hjemmeside, Ak-tuelt.dk (intranet) og der henvises hertil for nye ansatte i forbindelse med deres ansættelseskontrakt.

Struktur for arbejdet

Allerød Kommune benytter den struktur, der er defineret i ISO 27001 standarden.
Strukturen (også kaldet ISMS) er udtryk for ledelsesstyringen af informationssikkerheden.

ISO 27001 standarden udstikker rammerne for arbejdet med Informationssikkerhed. Det indebærer bl.a. udarbejdelse af en sikkerhedspolitik samt underliggende regelsæt og procedurer.



Formål og omfang

Formålet med denne sikkerhedspolitik er at opnå en optimal beskyttelse af informationer og en stabil drift af kommunens informationsleverance internt, til byrådet og organisationens ansatte samt eksternt til borgere, virksomheder og samarbejdspartnere.

Kommunen skal samtidig overholde lovgivningsmæssige krav samt implementere sikkerhedsforanstaltninger, der beskytter organisationen, herunder Forvaltningen, decentrale enheder og virksomheder. Derudover gælder sikkerhedspolitikken også for it-aktiviteter under kommunens ansvar, der udføres af eksterne leverandører, samarbejdspartnere, borgere og andre.

Målsætninger

Målsætningerne for informationssikkerhed i kommunen er at:

- Beskytte informationer og informationssystemer uafhængigt af, hvor disse måtte findes
- Sikre, at alle med en relation til kommunen, kender og arbejder efter gældende regler og procedurer, der sikrer god skik ved anvendelsen af informationer og informationssystemer
- Sikre høj driftsstabilitet i forhold til tilgængelighed og brug af informationer i kommunens informationssystemer.

Sikkerhedsniveau

Allerød Kommunes informationssikkerhedsniveau bygger på:

- International Standard for Informationssikkerhed – ISO 27001 og ISO 27701
- EU's databeskyttelsesforordning, databeskyttelsesloven og anden gældende lovgivning
- NSIS og NIS2 stiller krav om, at sikkerhedsniveauet hænger sammen med risikostyring, informationssikkerhed og databeskyttelse (GDPR).
- Årlig risikovurdering

På baggrund af den årlige risikovurdering fastlægger kommunen et sikkerhedsniveau, der passer til de risici kommunen er udsat for. Informationssikkerhedsniveauet skal være stabilt og bestemt ud fra Allerød Kommunes aktuelle risikoniveau for henholdsvis databeskyttelse og informationssikkerhed.

Ansvar

Ansvars- og kompetencefordeling vedrørende Informationssikkerhed fastsættes i henhold til følgende:

- Direktionen har det overordnede ansvar for sikkerhedspolitikken.

- Kommunaldirektøren er den øverste sikkerhedsansvarlige og har ansvar for:
  - At udpege en ansvarlig for Informationssikkerhed i Allerød Kommune
  - At godkende den udarbejdede sikkerhedspolitik

- Den ansvarlige for Informationssikkerhed har ansvar for:
  - At etablere en informationssikkerhedsfunktion til varetagelse af den daglige administration og koordinering
  - At udpege en systemejer for hvert af kommunens IT-systemer
  - At sikre etablering af tilstrækkelig organisering (repræsentativ for alle forvaltningsområder), til varetagelse af opgaver inden for informationssikkerhed (herunder risikovurderinger, udvikling af procedurer og arbejdsgange, vedligehold og løbende kontrol med vedtagne regler og procedurer).

Denne overordnede sikkerhedspolitik og underliggende retningslinjer, procedurer og kontroller for it- og informationssikkerhed er bl.a. beskrevet i sikkerhedshåndbogen.

Styringen af informationssikkerhed i Allerød Kommune sker ud fra en risikobaseret tilgang bl.a. ved hjælp af risiko- og konsekvensvurderinger. I forlængelse af risikohåndteringen, er der beskrevet et SoA-dokument (Statement of Applicabillity) med sikkerhedstiltag fra NSIS.

Enhver, der kommer i berøring med kommunens informationer og informationssystemer, har et ansvar for at opretholde det til enhver tid gældende informationssikkerhedsniveau, baseret på sikkerhedspolitikken, informationsledelsessystemet, regler og procedurer.

Opfølgning

Allerød Kommune følger op på informationssikkerhed på følgende måde:

- Persondatasikkerhed i Allerød Kommune afholder statusmøder med kommunaldirektøren og den sikkerhedsansvarlige.
- Der gennemføres uafhængige tredjepartsrevisioner, herunder IT-revision og NSIS.
- I tilfælde af at den årlige revision fører til ændringer af denne informationssikkerhedspolitik, forelægges politikken kommunaldirektøren til underskrift.

Overtrædelser

Overtrædelser af sikkerhedspolitikken, herunder underliggende sikkerhedsregler og procedurer behandles i henhold til Allerød Kommunes personalepolitik, samt strafferetslige og aftalemæssige regler.

Revision

Sikkerhedspolitikken skal tages op til revision minimum én gang årligt. Den sikkerhedsansvarlige har ansvaret for at gennemføre denne revision. Såfremt revisionen resulterer i betydelige ændringer til politikken, skal den reviderede version forelægges og godkendes af byrådet.

13/3 -2024

Dato

Morten Knudsen, kommunaldirektør