Informationssikkerhedspolitik Næstved Kommune

27. februar 2020

Informationssikkerhedspolitik

Formål

Næstved Kommunes (herefter ”Kommunen") informationssikkerhedspolitik beskriver vigtigheden af arbejdet med informationssikkerhed i Kommunen og fastlægger vores ambitionsniveau herfor. Informationssikkerhedspolitikken indeholder derfor de overordnede sikkerhedsmålsætninger og danner grundlag for udformning af Kommunens informationssikkerhedshåndbog, der forstås som fællesbetegnelsen af informationssikkerhedspolitikken med de underliggende retningslinjer og forretningsgange.

Informationssikkerhedspolitikken er en vigtig del af Kommunens informationssikkerhedshåndbog og beskriver det ledelsesgodkendte niveau for informationssikkerhed og beskyttelse af persondata. Dermed skal politikken ligeledes understøtte bevidstheden om informationssikkerhed i Kommunens organisation og virke. De retningslinjer, der udformes for at understøtte informationssikkerhedspolitikkens hovedmålssætninger, skal sikre, at alle, der arbejder med Kommunens informationer, forholder sig til informationssikkerhed i det daglige arbejde.

Kommunen ser ikke kun et tilstrækkeligt sikkerhedsniveau som et krav for at kunne overholde lov- og myndighedskrav, men også som et kvalitetselement for at kunne tilbyde en sikker service for borgerne og virksomheder. Informationssikkerhed er derfor en nøgleværdi hos Kommunen, og den vil være en naturlig del af vores aktiviteter.

Informationssikkerhedshåndbogen følger principperne i den internationale standard for informationssikkerhed, ISO 27001:2013, og er udarbejdet i et samarbejde mellem kommunerne i Digitaliseringsforening Sjælland. Målet med samarbejdet er en udstrakt harmonisering af medlemskommunernes ledelse og styring af informationssikkerheden med henblik på et tæt samarbejde for at opnå effektiviseringer og øget kvalitet på informationssikkerhedsområdet.

Herudover skal Informationssikkerhedshåndbogen og kommunens Informationssikkerhedspolitik også udgøre de overordnede rammer for kommunens efterlevelse af databeskyttelsesreglerne. Det vil navnlig sige EU’s databeskyttelsesforordning (GDPR) og den supplerende danske databeskyttelseslov (lov nr. 502 af 23. maj 2018). Informationssikkerhedspolitikken er gældende for alle uden undtagelse med en fysisk eller logisk adgang til Kommunens systemer, data og informationer.

Informationssikkerhedspolitikken omfatter alle typer af informationer herunder lyd, billede og tekst og uanset, hvordan informationerne anvendes og opbevares.

Gennemgang af politikker for informationssikkerhed

De informationssikkerhedspolitikker og retningslinjer mv., der indgår i denne Informationssikkerhedshåndbog, revurderes og godkendes mindst én gang hvert år, eller i forbindelse med eventuelle situationer, der tilsiger det. Ændringer af Informationssikkerhedshåndbogen skal koordineres med Digitaliseringsforening Sjælland.
Gennemgangen bør omfatte en vurdering af mulighederne for at forbedre organisationens politikker og metode til styring af informationssikkerhed som følge af ændringer i organisationen, forretningsforhold, juridiske forhold eller det tekniske miljø.
Gennemgangen bør tage højde for resultaterne af udført revision, tilsyn eller gennemførte audit.

Hovedmålsætninger og sikkerhedsniveau

Sikkerhedsmålsætning:
"Vi vil have et tilstrækkeligt informationssikkerhedsniveau for alle med relation til Kommunen og for anvendelsen af informationsaktiver."

Et tilstrækkeligt informationssikkerhedsniveau opnås igennem sikringsforanstaltninger, der sikrer:

1. Fortrolighed, integritet- og tilgængelighed af Kommunens systemer og data i forhold til den risikovurdering, der er fastsat for det enkelte system/data.
2. Beskyttelse af Kommunens informationsaktiver, organisationens image og informationer/data i Kommunens varetægt.
3. Sikring af databeskyttelse for fysiske personer, herunder ved efterlevelse af databeskyttelseslovgivningen.

For at fastholde det tilstrækkelige sikkerhedsniveau i Kommunen skal følgende overholdes:

- Der skal være implementeret retningslinjer og forretningsgange, som sikrer, at informationssikkerhed er en integreret del af Kommunens drift og daglige arbejde.
- Kommunen skal gennem kontrakt- og leverandørstyring sikre, at brugen af eksterne konsulenter, samarbejdspartnere og leverandører ikke udhuler Kommunens informationssikkerhedsniveau.
- Kommunen skal sikre en struktureret og kontinuerlig forbedringsproces af arbejdet med informationssikkerhed.

Organisation og ansvar

Sikkerhedsmålsætning:
"Alle har ansvar for informationssikkerheden. De er bekendte med og efterlever vores informationssikkerhedspolitik, informationssikkerhedshåndbog, retningslinjer og forretningsgange i Kommunen."

Planlægning, implementering og kontrol af informationssikkerhed er defineret af Kommunens ledelse. Informationssikkerhedskoordinatoren er ansvarlig for implementering og vedligeholdelse af informationssikkerhedssystemet i Kommunen og er ansvarlig for opfølgning på sikkerhedshændelser.

Kommunaldirektøren er ansvarlig for at arbejde med informationssikkerhed på et strategisk niveau, således at informationssikkerhedsmæssige overvejelser inddrages i alle væsentlige beslutninger. Ledere og medarbejdere er ansvarlige for at efterleve retningslinjer og procedurer for sikkerhed i det daglige arbejde.

Den nødvendige viden og kompetence om informationssikkerhed kommunikeres til alle, der arbejder med Kommunens informationer, og der bliver løbende arbejdet med holdninger og viden om informationssikkerhed. Ledelsen på alle niveauer er ansvarlig for, at informationssikkerheden overholdes.

Informationssikkerhedshåndbogen

Informationssikkerhedspolitikken uddybes i retningslinjer og forretningsgange. Tilsammen udgør politikken, retningslinjer, beredskabsplanen og forretningsgange informationssikkerhedshåndbogen.

Risikovurdering og klassifikation

Risikovurdering

Informationssikkerheden i Kommunen er på et niveau, der tilgodeser lov- og myndighedskrav, kontraktlige forpligtelser samt forpligtelser overfor de aktører, der skal anvende Kommunens informationsaktiver. Kommunen ønsker ikke at sikre sig for enhver pris, men ønsker at være bevidst om enhver risiko, og forholde sig tilfredsstillende til disse, hvormed et tilstrækkeligt sikkerhedsniveau etableres.

Ledelsen deltager aktivt i risikovurderingen og er ansvarlige for at vurdere trusler, konsekvenser og risici af informationssystemer og andre relevante områder.

Risikovurderingen opdateres mindst én gang årligt, samt ved eventuelle større ændringer i opgaver, leverandører, informationssystemer eller anvendelsen deraf.

Risikovurderingen skal ikke kun have fokus på risici for organisationens aktiver/værdier. Der skal også udføres risikovurdering med fokus på risici for fysiske personers rettigheder og frihedsrettigheder.

Klassifikation

Kommunens informationer skal klassificeres efter lovmæssige krav, værdi og efter, hvor kritisk og følsom informationen er i forhold til uautoriseret offentliggørelse eller ændring.

Baseret på klassifikationen samt risikovurderingen etableres relevante sikkerhedsforanstaltninger.

Overtrædelse af informationssikkerhedspolitikken

Alle i Kommunen er forpligtet til at efterleve den til enhver tid gældende informationssikkerhedspolitik med tilhørende retningslinjer, forretningsgange og relaterede bilag. En overtrædelse kan, efter omstændighederne, medføre sanktioner.

Hvis en medarbejder er vidende om, at Kommunens informationssikkerhed overtrædes, skal det meddeles til ledelsen.

Afvigelser

Hvis der opstår situationer, hvor kravene i informationssikkerhedshåndbogen ikke kan efterleves, skal der skriftligt anmodes om dispensation hos Kommunens formand for informationssikkerhedsudvalget. Eventuelle afvigelser fra kravene skal dokumenteres, og der skal indføres alternative sikringsforanstaltninger og en udløbsdato.

Udarbejdelse og ikrafttrædelse

Håndtering af ændringer i sikkerhedsdokumentationen foretages på følgende måde:

- Informationssikkerhedspolitikken: Godkendes af byrådet/direktionen.
- Informationssikkerhedshåndbogen samt bilag og retningslinjer: Godkendes af Informationssikkerhedsudvalget.
- Operationelle procedurer: Kan foretages af den lokale ledelse.