Ringkøbing-Skjern Kommune

Ringkøbing-Skjern Kommune

Informationssikkerhedspolitik

Indholdsfortegnelse

1. Indledning

Denne sikkerhedspolitik udgør den overordnede ramme for informationssikkerheden i Ringkøbing-Skjern Kommune.

Fordi vi tager hånd om vores borgere og kolleger, sikrer vi at dette sker på betryggende vis. De data vi har ansvaret for:

- er *tilgængelige* – alle har adgang til relevante data.
- har den nødvendige *integritet* – indholdet af vores data er korrekte og fuldstændige.
- er *fortrolige* – når data er fortrolige behandles de sikkert og med omhu.

Ringkøbing-Skjern Kommune behandler informationer af stor betydning for borgere og virksomheder. Det er derfor af afgørende betydning, at vores borgere og virksomheder har tillid til, at den nødvendige sikkerhed opretholdes.

2. Formål

Formålet med Ringkøbing-Skjern Kommunes informationssikkerhed er, at sikre, at data er tilgængelige, korrekte og ikke kommer til uvedkommende personers kendskab.

Ringkøbing-Skjern Kommune skal sikre, at konsekvenserne af et sikkerhedsbrud reduceres til et for Ringkøbing-Skjern Kommune acceptabelt niveau:

- Ringkøbing-Skjern Kommune skal sikre, at borgerne til stadighed kan føle sig trygge ved at overlade deres data til kommunen.
- Ringkøbing-Skjern Kommune skal sikre medarbejdernes tryghed og arbejdsvilkår.

Informationssikkerheden skal altid leve op til følgende krav:

- Ringkøbing-Skjern Kommune skal leve op til de sikkerhedsmæssige krav, der udspringer af lovgivningen. Her har specielt Databeskyttelsesforordningen og persondataloven betydning som følge af Ringkøbing-Skjern Kommunes omfattende opgaver med behandling af personhenførbare/personrelaterede data.
- Ringkøbing-Skjern Kommune skal desuden leve op til de sikkerhedsmæssige krav, der er indgået aftale om med andre myndigheder.
- Beredskabsplaner for informationssikkerhed skal efter et nedbrud, der ikke kan håndteres inden for de normale rammer for daglig driftsafvikling, muliggøre genoptagelse af drift indenfor de aftalte tidsfrister.

3. Holdninger og principper

Informationssikkerhed i Ringkøbing-Skjern Kommune skal fastlægges som en afvejning af de ofte modstridende hensyn til på den ene side ønsket om høj sikkerhed, på den anden side hensynet til brugervenlig it-anvendelse og på den tredje side omkostninger ved investeringer i sikkerhed.

Det er ligeledes vigtigt at finde en god balance mellem hensynet til den helhedsorienterede sagsbehandling og afvejningen af informationssikkerheden.

4. Omfang

Politikken omfatter Ringkøbing-Skjern Kommunes informationer, som er:

- alle informationer, der tilhører kommunen, herudover også informationer, som ikke tilhører kommunen, men som kommunen kan gøres ansvarlig for. Dette inkluderer f.eks. alle informationer om borgere, personale, informationer om finansielle forhold, alle informationer, som bidrager til administration af kommunen samt informationer, som er overladt til kommunen af andre. Disse informationer kan være faktuelle oplysninger, optegnelser, registreringer, rapporter, forudsætninger for planlægning eller ethvert andet datagrundlag, som kun er til intern brug.
- alle informationer, ligegyldigt, hvilken form de opbevares og formidles på, herunder også informationer i papirform.

Politikken er gældende for:

- alle ansatte uden undtagelse - både fastansatte og midlertidigt ansatte.
- politikere.
- eksterne konsulenter, som arbejder i eller for kommunen.
- alle medarbejdere der er ansat under aftaleenheder, herunder selvejende institutioner.

Disse personer betegnes herefter som medarbejderen.

5. Sikkerhedsniveau

Kommunen fastlægger på baggrund af en risikovurdering et sikkerhedsniveau, som svarer til betydningen af de pågældende data. Kommunen vil gennemføre en risiko- og konsekvensvurdering under hensyntagen til sammenhæng mellem investering i tid til risikovurdering og sikkerhedsniveauet.

Der gennemføres mindst en gang årligt en risikovurdering, så ledelsen kan holde sig informeret om det aktuelle risikobillede. Der foretages ligeledes en risikovurdering ved større forandringer i organisationen eller systemerne.

Informationssikkerhedspolitikken tager udgangspunkt i god it-skik, best praksis og standarder på området samt lovgivning indenfor it-sikkerhed.

Ringkøbing-Skjern Kommune vil leve op til ISO27001 i det omfang der er sammenhæng mellem sikkerhed, funktionalitet og økonomisk investering.

ISO27001 er en standard, som beskriver hvorledes it-sikkerhed implementeres og styres i en organisation.

6. Sikkerhedsbevidsthed, organisering og ansvar

Informationssikkerhed vedrører kommunens samlede data og gennemførelse af en informationssikkerhedspolitik kan ikke foretages af ledelsen alene. Alle medarbejdere har et ansvar for at bidrage til at beskytte kommunens data mod uautoriseret adgang, ændring og ødelæggelse samt tyveri. Alle medarbejdere skal derfor løbende uddannes i informationssikkerhed i relevant omfang.

Direktionen har det overordnede ansvar for, at styringen af informationssikkerheden er hensigtsmæssig og betryggende.

- Det overordnede ansvar for styring af informationssikkerhedsindsatsen og gennemførelse af den fornødne kontrol varetages af *direktionen*. Det er direktionen der godkender Informationssikkerhedspolitiken.
- *Direktionen* skal udpege den øverste it-sikkerhedsansvarlige med ansvar for den overordnede styring af informationssikkerhedsindsatsen, og sikre etablering af en organisatorisk it-sikkerhedsgruppe.
- *It-sikkerhedsgruppen* skal hjælpe den øverste it-sikkerhedsansvarlige med at vurdere, hvorvidt der er behov for ændringer i den gældende informationssikkerhedspolitik og dennes operative udmøntning. It-sikkerhedsgruppen godkender sikkerhedsreglerne.
- *Den øverste it-sikkerhedsansvarlige* har ansvar for den overordnede styring af informationssikkerheden. Den øverste it-sikkerhedsansvarlige sikrer udarbejdelse og vedligeholdelse af informationssikkerhedspolitikken, sikkerhedsregler, beredskabsplaner og risikovurderingen.
- *Databeskyttelsesrådgiveren er ansvarlig for at rådgive kommunen, i arbejdet med at overholde Databeskyttelsesforordningen og andre databeskyttelsesretslige regler. Databeskyttelsesrådgiveren er desuden kommunens kontaktled i samarbejdet med Datatilsynet.*
- *Koncern IT* har ansvar for at sikre implementering af informationssikkerhedspolitikken og sikkerhedsreglerne i den daglige drift. Ligeledes er Koncern IT en vigtig interessent i udarbejdelsen af disse dokumenter og krav.
- *Systemejere* har ansvar for at sikre deres egne systemer lever op til informationssikkerhedspolitikken, samt for at godkende ændringer og autorisationer på egne systemer.
- *Ledere* i Ringkøbing-Skjern Kommune har ansvar for at deres medarbejdere kender til informationssikkerhedspolitikken, og for at sikre at medarbejderne kan leve op til den.
- *Alle medarbejdere og politikere* i Ringkøbing-Skjern Kommune har et personligt ansvar for, at informationssikkerhedspolitik og -regler følges i forbindelse med vedkommendes aktuelle ansvarsområde, arbejdsopgaver og hverv.

7. Operationalisering

Politikken skal af it-sikkerhedsgruppen omsættes til operative sikkerhedsbestemmelser dvs. sikkerhedsregler for administrative, fysiske og tekniske sikringsforanstaltninger. Der skal udarbejdes procedurer, retningslinier, forretningsgange og dokumenteres opfyldelse af krav.

Fag- og stabschefer, systemejere, de enkelte medlemmer af it-sikkerhedsgruppen, herunder Databeskyttelsesrådgiveren, samt ekstern revision skal rapportere status på informationssikkerheden til den øverste it-sikkerhedsansvarlige, som rapporterer til it-sikkerhedsgruppen.

8. Opfølgning

Informationspolitikken revurderes hvert 3. år, som et led i den overordnede sikkerhedsstyring. I revurderingen tager den øverste it-sikkerhedsansvarlige og direktionen udgangspunkt i den løbende overvågning af, og rapportering om informationssikkerheden i kommunen.

9. Godkendelse

Denne informationssikkerhedspolitik er godkendt af,

It-sikkerhedsgruppen indstilling til Direktionen den 16.4.2018.

Direktionen, den 14.5.2018 beslutning med ikrafttræden den 25.5.2018.