FREDERICIA KOMMUNE

Opdateret juli 2021

Informationssikkerhedspolitik

Indholdsfortegnelse

1. Formål 1
2. Rammeområde for informationssikkerhedspolitikken 1
   2.1. Hvem er omfattet af informationssikkerhedspolitikken 1
   2.2. Hvad er omfattet af informationssikkerhedspolitikken 1
3. Målsætninger og strategi 2
   3.1. Risikobegrænsning 2
   3.2. Ansvar og organisering 2
   3.3. Tilsyn og beredskab 3
4. Udmøntning og drift 3
5. Udarbejdelse, ikrafttrædelse, ansvarsfordeling og ajourføring 3
6. Databeskyttelsesrådgiver 4
7. Bilag 5

1. Formål

Formålet med informationssikkerhedspolitikken i Fredericia Kommune er at sikre en vedvarende lovlig forvaltningsvirksomhed samt tryghed og integritet for borgere i mødet med Fredericia Kommune.

Informationssikkerhedspolitikken er et strategisk styringsredskab, hvor Fredericia Kommune fastsætter målsætninger, afgrænsninger, ansvarsplacering og rammerne for arbejdet med informationssikkerhed.

2. Rammeområde for informationssikkerhedspolitikken

Informationssikkerhedspolitikken, de tilhørende informationssikkerhedsprocedure og de underliggende vejledninger følger den til enhver tid gældende lovgivning og regulering, herunder Databeskyttelsesforordningen og –loven, de forvaltningsretlige krav af betydning for informationssikkerheden og sikring af borgernes rettigheder i bred forstand.

Fredericia Kommunes styring af informationssikkerhed bygger på principperne i den internationale standard for informationssikkerhed, ISO 27001.

2.1. Hvem er omfattet af informationssikkerhedspolitikken

Efterlevelse af Fredericia Kommunes informationssikkerhedspolitik, de tilhørende informationssikkerhedsprocedure og vejledninger gælder for alle juridiske enheder under Fredericia Kommune, hvor Fredericia Kommune enten er dataansvarlig eller databehandler.

Informationssikkerhedspolitikken, de tilhørende informationssikkerhedsprocedure og underliggende regelsæt gælder også for alle ansatte, eksternt tilknyttede personer, herunder konsulter og servicemedarbejdere, politikere og samarbejdspartnere med adgang til Fredericia Kommunes informationsaktiver.

2.2. Hvad er omfattet af informationssikkerhedspolitikken

Al data i kommunens besiddelse er omfattet af informationssikkerhedspolitikken, herunder værdioplysninger og personoplysninger fra alle borgere, medarbejdere og andre personer, hvis oplysninger registreres af kommunen.

3. Målsætninger og strategi

Fredericia Kommunes konkrete strategi baserer sig på en række styringsprincipper, som med udgangspunkt i en risikobegrænsende tilgang skal sikre et optimalt og ensartet datasikkerhedsniveau i alle kommunens afdelinger og stabe. Sikkerhedsniveauet skal være et udtryk for afvejningen af sikkerhedshensynet, brugervenlighed og økonomi. Strategien skal således løbende vurderes og tilpasses efter behov.

Strategien lægger kommunens overordnede ramme for at opfylde datasikkerhedspolitikkens formål:

- *Formålet med informationssikkerhedspolitikken i Fredericia Kommune er at sikre en vedvarende lovlig forvaltningsvirksomhed samt tryghed og integritet for borgere i mødet med Fredericia Kommune.*

Med lovlig forvaltningsvirksomhed menes: at love og regler for behandlingen af personoplysninger udmøntes og udføres korrekt i forvaltningens daglige arbejde.

Med tryghed menes: at de registreredes rettigheder beskyttes, samt at de person- og værdioplysninger kommunen er i besiddelse af kun er tilgængelige for de medarbejdere, systemer eller eksterne parter, der har et lovligt behov for at tilgå oplysningerne.

Med integritet menes: at person- og værdioplysninger i alle tilfælde er korrekte og der er garanti, for at data ikke kan manipuleres eller misbruges.

3.1. Risikobegrænsning

Informationssikkerhedsniveauet skal være stabilt og bestemt ud fra Fredericia Kommunes aktuelle risikoniveau. Den konkrete risiko skal løbende vurderes og omfanget af den økonomiske indsats skal fastlægges ud fra det aktuelle risikoniveau. Dog træder hensynet til overholdelse af gældende lovgivning forud for hensynet til kommunens økonomiske interesser.

3.2. Ansvar og organisering

Informationssikkerheden skal udmøntes gennem informationssikkerhedsprocedurerne, som skal understøttes af styringsprincipperne samt dokumenterede processer og det rette kompetenceniveau hos kommunens medarbejdere.

3.3. Tilsyn og beredskab

Tilsyn foretages ud fra en risikobegrænsende tilgang og gennemføres af de relevante instanser i Fredericia Kommune:

- Lovpligtig tilsyn
- Kommunaldirektøren
- Informationssikkerhedsudvalget
- Forvaltningens øvrige ledelse

Der skal foreligge opdaterede beredskabsplaner for de relevante områder og systemer til brug i de situationer, hvor systemer eller områder rammes af forhold, som aktiverer informationssikkerhedsberedskabet

4. Udmøntning og drift

Udmøntningen af informationssikkerhedspolitikken sker gennem informationssikkerhedsprocedurerne og de underliggende vejledninger, som regulere følgende hovedområder:

- Informationssikkerhed
- Persondatabeskyttelse
- IT-livscyklus samt årshjulet

5. Udarbejdelse, ikrafttrædelse, ansvarsfordeling og ajourføring

Fredericia Kommunes øverste ledelse fastlægger informationssikkerhedspolitikken og målsætningerne for informationssikkerhed.

Informationssikkerhedsudvalget (ISU) har ansvaret for, at informationssikkerhedspolitikken udarbejdes og opdateres, samt dennes realiseringen og efterlevelsen.

Informationssikkerhedspolitikken træder i kraft, når den godkendes af byrådet og gælder indtil en ny version er godkendt af byrådet. Informationssikkerhedspolitikken godkendes på almindelige vilkår efter de regler, som er fastsat i Fredericia Kommunes styrelsesvedtægter.

Kommunaldirektøren er Fredericia Kommunes øverste sikkerhedsansvarlige.

Chefer og ledere er ansvarlige for at implementere de gældende regler i deres afdelingers og stabes arbejdsprocedurer.

Informationssikkerhedspolitikken skal revurderes årligt, eller hvis der sker væsentlige ændringer i den kommunale organisation, lovgivning eller trusselsniveau.

Informationssikkerhedspolitikken offentliggøres på www.fredericia.dk.

6. Databeskyttelsesrådgiver

Det er et grundlæggende krav, at databeskyttelsesrådgiveren udfører sine opgaver uafhængigt. Dette betyder at databeskyttelsesrådgiveren ikke må modtage instrukser i forbindelse med udførelsen af sine opgaver og refererer til byrådet.

Databeskyttelsesrådgiverens opgaver omfatter følgende:

- Orientering og rådgivning af kommunens ledelse og ansatte om deres forpligtelser
- Overvåge at kommunen overholder forordningen
- Rådgive kommunen i forbindelse med udarbejdelse af konsekvensanalyser
- Holde kontakt med relevante myndigheder og andre eksterne samarbejdspartnere i forhold til databeskyttelseslovgivningen
- Samarbejde med og fungere som kontaktperson til tilsynsmyndigheden for databeskyttelse
- Fungere som kontaktperson for registrerede (borgere) angående spørgsmål om behandling af deres oplysninger Rapportere én gang årligt eller efter behov til byrådet
- Databeskyttelsesrådgiveren skal støtte og rådgive alle niveauer i Fredericia Kommune
- Databeskyttelsesrådgiveren har ingen ledelsesmæssig beslutningskompetence

7. Bilag

Bilag 1. Model for udarbejdelse, ikrafttrædelse, ansvarsfordeling og ajourføring

Politik, roller og ansvar

Byrådet godkender informationssikkerhedspolitikken.

Kommunaldirektøren er Fredericia Kommunes øverste ansvarlige for informationssikkerhed.

Informationssikkerhedsudvalget er ansvarlig for realisering og efterlevelse af informationssikkerhedspolitikken.

Chefer og ledere er ansvarlige for at implementere gældende regler i procedurer og arbejdsgange.

Alle er ansvarlige for at efterleve gældende regler.