



Politik for informationssikkerhed

Godkendt af Byrådet den 29.04.2021



Mariagerfjord
Kommune



Politik for informationssikkerhed

Formålet med politikken for informationssikkerhed er at sikre, at anvendelsen af informationer sker efter gældende lovgivning, anerkendte standarder og fastlagte regler.

Informationssikkerhed er en bred betegnelse for de samlede foranstaltninger, som skal sikre informationer i forhold til fortrolighed, integritet og tilgængelighed.

Informationer i såvel digital som fysisk format er omfattet af politikken.

Mariagerfjord Kommunes politik for informationssikkerhed bygger på principperne i den internationale standard for informationssikkerhed, ISO27001, i henhold til aftale mellem kommunerne og regeringen.

Politikken understøttes af en håndbog for informationssikkerhed, der fastlægger niveauet for informationssikkerheden og sætter retningen for de underliggende procedurer. Disse skal indgå som en integreret del af driften under hensyntagen til medarbejdernes sikkerhed og rettigheder.

Niveauet for informationssikkerheden fastlægges ud fra en risikobaseret afvejning mellem hensynet til lovmedholdelighed, sikkerhed, brugervenlighed og omkostninger.

Målsætning

Mariagerfjord Kommune vil opretholde et effektivt værn mod informationssikkerhedsmæssige trusler, således at borgernes retssikkerhed, de ansattes trygheds- og arbejdsvilkår og Mariagerfjord Kommunes omdømme sikres bedst muligt.

Beskyttelsen skal omfatte såvel naturgivne som tekniske og menneskeskabte trusler af bevidst eller tilfældig art.

De sikkerhedsmæssige tiltag skal beskytte kommunens informationer og understøtte at følgende opretholdes:

Fortrolighed

Kvalificeret behandling, transmission og opbevaring af informationer, og minimering af risikoen for at informationer kommer uvedkommende i hænde

Integritet

Korrekt funktion og brug af informationsaktiver med minimeret risiko for manipulation af og fejl i såvel informationer som systemer

Tilgængelighed

Driftssikkerhed med høj opetid og minimeret risiko for større nedbrud og tab af informationer der påvirker serviceniveauet i kommunen



Organisering og ansvar

Det overordnede ansvar for informationssikkerheden er placeret hos Direktionen.

Direktion og Chefgruppe (DC) fungerer som informationssikkerhedsudvalg, der arbejder med organisationens risikobillede og niveau for informationssikkerhed. Økonomidirektøren er formand for udvalget.

De daglige opgaver varetages af en informationssikkerhedskoordinator.

Politikken for informationssikkerhed udmøntes i Håndbog for Informationssikkerhed, som udarbejdes efter principperne i ISO27001. Reglerne beskriver det ønskede niveau for informationssikkerheden i Mariagerfjord Kommune og fastlægges af informationssikkerhedsudvalget.

Ud fra Håndbogen for informationssikkerhed skal fagchefer, system- og dataejere udarbejde relevante procedurebeskrivelser, så det daglige arbejde med kommunens informationer sker i overensstemmelse med det ønskede sikkerhedsniveau.

Informationssikkerhedsudvalget udarbejder i samarbejde med relevante fagchefer, system- og dataejere løbende risikovurderinger af de væsentligste informationsaktiver og infrastruktur. Kommunens risikobillede danner afsæt for eventuelle indsatser for at styrke informationssikkerheden.

Hvor det er relevant, udarbejder fagchefer, system- og dataejere beredskabsplaner, som træder i kraft, hvis vigtige informationsaktiver bliver utilgængelige, kompromitteres eller lækkes.

I henhold til EU databeskyttelsesforordningen udpeges der endvidere en databeskyttelsesrådgiver. Databeskyttelsesrådgiveren underretter og rådgiver organisationen, om forpligtelserne efter forordningen, og fører tilsyn med, om kommunen overholder reglerne.

Sikkerhedsbevidsthed

Ledelsen har ansvar for, at medarbejderne forstår, hvorfor regler og procedurer er nødvendige og kan agere herefter, samt vigtigheden af, at sikkerhed skal være en naturlig del af opgaveløsningen.

Hvis en medarbejder, politiker, samarbejdspartner eller leverandør opdager trusler eller brud, der kan kompromittere informationssikkerheden, skal de straks kontakte nærmeste leder eller kommunens informationssikkerhedskoordinator, som så vurderer, hvordan hændelsen skal håndteres.

Gyldighed og omfang

Politikken, regler og procedurer gælder alle ansatte, politikere, eksterne samarbejdspartnere og leverandører, som har adgang til kommunens informationer. Hertil kommer alle lokaliteter, hvor informationer anvendes og bearbejdes, såsom rådhus, institutioner, hjemmearbejdspladser mv.

Alle, der har adgang til kommunens informationer, skal kende relevante regler for informationssikkerheden og har pligt til at overholde dem.

Hvis der konstateres en overtrædelse, er det et ledelsesansvar at håndtere dette.

Godkendt af Byrådet 29.04.2021