DAGSORDEN Direktionen d. 23-06-2026

Mødedato	Tirsdag d. 23. juni 2026 kl. 09:00
Mødested	Mødelokale 1.14
Mødedeltagere	Lars Holte, Anya Krogh Manghezi, Rasmus Vanggaard Knudsen (Afbud), Jakob Lynge Lind

Indholdsfortegnelse

Punkt 1: Lukket

21/12763

Afbud Rasmus Vanggaard Knudsen

Punkt 2: 2. Ny cyber og informationssikkerheds politik og håndbog

26/9096

Baggrund

Høje-Taastrup Kommune har en informationssikkerhedspolitik som politisk ramme for arbejdet med beskyttelse af borgernes data og IT-sikkerhed. Den nuværende politik blev godkendt af økonomiudvalget den 23-08-2022. Dertil har Høje-Taastrup Kommune en informationssikkerhedshåndbog, som sætter de administrative rammer for området. Den nuværende håndbog er senest opdateret i 2023.

I løbet af de senere år er omfanget af krav og regler på IT-området øget betydeligt og samtidig har den teknologiske udvikling sat turbo på hvordan teknologien på mange områder griber ind i de kommunale kerneopgaver. På den baggrund forelægges Direktionen forslag til ny cyber- og informationssikkerhedspolitik samt ny informationssikkerhedshåndbog for Høje-Taastrup Kommune. Cyber- og Informationssikkerhedspolitikken skal politisk behandles.

Sagen til direktionen præsenterer hovedlinjerne i både politikken og håndbogen. CBA foreslår, at Direktionen godkender cyber- og informationssikkerhedspolitikken og informationssikkerhedshåndbogen som kommunens samlede styringsgrundlag for cyber- og informationssikkerhed. Politikken forelægges efterfølgende Økonomiudvalget og Byrådet til politisk behandling, mens håndbogen udgør den administrative ramme for den daglige efterlevelse af politikken og relevante krav på området. CBA foreslår desuden, at Direktionen godkender initiativer til kommunikation og udbredelse af viden om cyber- og informationssikkerhed.

På mødet vil Rune Thomsen, Christina Skov og Klaus Fisker præsentere hovedlinjerne i politikken og håndbogen.

Indstilling

Det indstilles, at Direktionen

1. godkender cyber- og informationssikkerhedspolitikken som kommunens overordnede ledelsesmæssige ramme for cyber- og informationssikkerhed

2. godkender, at politikken forelægges Økonomiudvalget og Byrådet til politisk behandling

3. godkender informationssikkerhedshåndbogen som kommunens administrative ramme for implementering og efterlevelse af cyber- og informationssikkerhed

4.godkender initiativer til kommunikation og udbredelse af viden om cyber- og informationssikkerhed

Sagsfremstilling

Cyber- og informationssikkerhed handler om kommunens evne til at opretholde den daglige opgaveløsning og levere kerneydelser til borgere og virksomheder på en stabil, sikker og lovlig måde. Det gælder også i situationer, hvor kommunen rammes af digitale hændelser, fejl, nedbrud, leverandørsvigt eller cyberangreb. Cyber- og informationssikkerhed er derfor ikke alene et teknisk eller administrativt område, men en forudsætning for, at kommunen kan levere ydelser som hjemmehjælp, plejehjem, skole, myndighedsbehandling og øvrige borgerrettede funktioner.

Kommunens opgaveløsning er i dag afhængig af digitale løsninger, data, netværk, leverandører og faste arbejdsgange på tværs af organisationen. Hvis disse ikke fungerer, kan det få direkte betydning for borgernes hverdag, medarbejdernes mulighed for at løse deres opgaver og kommunens evne til at opretholde normal drift.

Formålet med politikken og håndbogen er at fastlægge en fælles ramme for kommunens arbejde med cyber- og informationssikkerhed. Dokumenterne skal understøtte, at kommunen beskytter oplysninger, systemer og digitale services, så de er fortrolige, korrekte og tilgængelige, når der er behov for dem. Samtidig skal dokumenterne være med til

at sikre, at kommunen er bedre forberedt, hvis der indtræder en hændelse eller beredskabssituation, hvor digitale systemer, data eller kritiske arbejdsgange påvirkes.

Politikken og håndbogen er udarbejdet i samarbejde med BDO. Arbejdet er både en modernisering af kommunens hidtidige politik og håndbog og en tilpasning til det aktuelle trusselsbillede, gældende lovgivning, relevante standarder og myndighedernes forventninger. Kravene følger blandt andet af NIS 2-loven, databeskyttelsesforordningen (GDPR), databeskyttelsesloven og de krav til kommunens beredskab og fortsatte opgaveløsning, som følger af kommunens ansvar som offentlig myndighed.

Det centrale formål med det nye materiale er at sikre et samlet styringsgrundlag, der gør det tydeligt, hvad kommunen vil sikre, hvem der har ansvar, og hvordan arbejdet skal understøttes i praksis. Cyber- og informationssikkerhedspolitikken fastlægger den overordnede ledelsesmæssige ramme for arbejdet. Politikken beskriver de principper, målsætninger og ansvarsforhold, der skal gælde for arbejdet med at beskytte kommunens informationer, systemer og digitale services.

Informationssikkerhedshåndbogen omsætter politikken til mere konkrete rammer, krav og arbejdsgange. Håndbogen skal understøtte den daglige efterlevelse i organisationen og beskriver blandt andet, hvordan kommunen arbejder med risikovurderinger, adgangsstyring, leverandørstyring, beredskab, hændelseshåndtering, logning, fysisk sikkerhed, sikker drift og beskyttelse af oplysninger. Tilsammen udgør politikken og håndbogen den fælles ramme for, at kommunen kan arbejde systematisk, risikobaseret og dokumenteret med cyber- og informationssikkerhed.

Håndbogen er opbygget med henblik på at strømline og forenkle de mange krav, der stilles til kommunen. Det betyder, at krav fra forskellige lovgivninger, standarder og myndighedsforventninger er samlet og omsat til én fælles ramme, hvor der så vidt muligt ikke stilles flere parallelle krav, der i praksis handler om det samme. Formålet er at gøre det lettere for organisationen at efterleve kravene i hverdagen og samtidig sikre en mere ensartet og dokumenterbar tilgang til cyber- og informationssikkerhed.

Dokumenterne understøtter samtidig kommunens beredskab. Et velfungerende beredskab handler ikke kun om at kunne reagere, når en hændelse er indtruffet, men også om at have klare roller, kendte arbejdsgange, dokumenterede sikkerhedsforanstaltninger og et fælles grundlag for prioritering, inden en hændelse opstår. Politikken og håndbogen skal derfor være med til at sikre, at kommunen hurtigere kan opdage, vurdere, håndtere og komme videre efter en hændelse.

Kommunikation

Efter Direktionens behandling er det relevant at cyber- og informationssikkerhedspolitikken og informationssikkerhedshåndbogen formidles til relevante ledelsesfora og bredere til Høje-Taastrup Kommune. Formidlingen skal understøtte, at dokumenterne ikke alene opfattes som styringsdokumenter, men som en praktisk ramme for den daglige opgaveløsning og kommunens samlede beredskab.

Der påbegyndes samtidig et arbejde med at udarbejde målrettet materiale til henholdsvis medarbejdere og ledere. Formålet er at omsætte politikken og håndbogen til kortere og mere tilgængelige pixi-udgaver, der giver de enkelte målgrupper netop de informationer, de har brug for i deres funktion. For medarbejdere vil fokus være på de vigtigste krav og handlemåder i hverdagen. For ledere vil fokus være på ansvar, prioritering, opfølgning og håndtering af risici og hændelser inden for eget område.

Bilag

Bilag 1 - ØU sag - Cyber- og informationssikkerhedspolitik for Høje-Taastrup

Bilag 2 -Cyber- og Informationssikkerhedspolitik

Bilag 3 -Informationssikkerhedshåndbog i Høje-Taastrup Kommune 2026

Afbud Rasmus Vanggaard Knudsen