# Informationssikkerhedspolitik

# Morsø Kommune

April 2026

**Morsø Kommune**

Jernbanevej 7 • 7900 • Nykøbing Mors
Telefon 9970 7000 • www.mors.dk

# Indholdsfortegnelse



## Indledning

Morsø Kommunes informationssikkerhedspolitik beskriver rammerne for informationssikkerhedsarbejdet i Morsø Kommune. Formålet med politikken er at tilkendegive over for alle som har relation til Morsø Kommune, at anvendelse af informationer sker efter gældende lovgivning, anerkendte standarder og fastlagte regler.

Informationssikkerhed er en bred betegnelse for de samlede foranstaltninger til at sikre informationer i forhold til fortrolighed[1], integritet[2] og tilgængelighed[3].

Morsø Kommunes informationssikkerhedspolitik bygger på principperne i den internationale standard for informationssikkerhed, ISO27001/2 i henhold til aftale mellem kommunerne og regeringen. Politikken er opdateret i henhold til kravene i NIS2-direktivet, som er implementeret i dansk lovgivning og gælder for kommuner som væsentlige enheder. Morsø Kommune forpligter sig til at overholde direktivets krav om risikostyring, hændelseshåndtering og ledelsesforankring.

Informationer i såvel elektronisk som papirbaseret form er omfattet.

Politikken gælder for alle ansatte i Morsø Kommune, samt for politikere og eksterne samarbejdspartnere med adgang til Morsø Kommunes informationsaktiver.

## Målsætning for sikkerhedsniveauet

Det samlede arbejde med informationssikkerhed skal sikre at borgere, virksomheder og samarbejdspartnere som medarbejdere og politikere kan være trygge ved at Morsø Kommune håndterer informationer på lovlig og betryggende vis.

---

[1] Fortrolighed: Informationssikkerhed skal sikre fortrolig behandling, transmission og opbevaring af informationer, hvor kun autoriserede brugere har adgang.

[2] Integritet: Informationssikkerhed skal sikre korrekt og pålidelig brug af aktiver og minimere risiko for ukorrekt datagrundlag, fx pga. menneskelige eller systemmæssige fejl.

[3] Tilgængelighed: Informationssikkerhed skal være medvirkende til, at vi opnår høj tilgængelighed og minimere risiko for systemnedbrud.

Sikkerhedsniveauet fastlægges med udgangspunkt i fortrolighed, integritet og tilgængelighed og udmøntes i en informationssikkerhedshåndbog og et understøttende sæt af informationssikkerhedsregler og -procedure, der gælder for alle dele af informationssikkerhedsarbejdet i Morsø Kommune, og som skal understøtte det ønskede sikkerhedsniveau i Morsø Kommune. Sikkerhedsniveauet skal derudover leve op til kravene i NIS2-direktivet, herunder krav om dokumenteret risikostyring, hændelseshåndtering og beredskab. Kommunen skal sikre, at informationssikkerheden understøtter kontinuitet og robusthed i kritiske tjenester.

Procedurekataloget skal understøtte den praktiske udførelse af informationssikkerhedsarbejdet og skal forankres hos lederne.

Informationssikkerhedshåndbogen, regler og procedure underlægges en kontrolfunktion, der sikrer at regler og procedure løbende er opdateret og overholdt.

Informationssikkerhedsaktiviteterne styres gennem et ledelsessystem for informationssikkerhed (ISMS).

## Organisering og ansvar

Kommunaldirektøren er den øverste sikkerhedsansvarlig i Morsø Kommune. Kommunaldirektøren har desuden det overordnede ansvar for, at Morsø Kommune lever op til kravene i NIS2-direktivet, herunder at cybersikkerhed er forankret på ledelsesniveau og indgår som en integreret del af kommunens strategiske risikostyring.

Direktionen har nedsat et informationssikkerhedsudvalg, som skal varetage den overordnede styring og kontrol af informationssikkerheden og har det overordnede ansvar for implementeringen af de fastsatte informationssikkerhedsregler og -procedure. Informationssikkerhedsudvalget består af Styregruppen for Informationssikkerhed, informationssikkerhedskonsulent og databeskyttelsesrådgiveren.

Udover deltagelse i informationssikkerhedsudvalget er databeskyttelsesrådgiverens rolle at servicere borgerne ift. informationssikkerhed, understøtte at den dataansvarlige overholder persondataforordningen, samt varetage rådgivning og kontrol internt i organisationen. Databeskyttelsesrådgiveren kan rapportere direkte til kommunaldirektøren, hvis der er behov herfor.

Informationssikkerhedsudvalget har nedsat et tværfagligt forum med lokale sikkerheds-agenter, som er nøglepersoner fra forvaltningerne. Forums opgaver er at understøtte fagområderne i arbejdet med GDPR og informationssikkerhed.

Det daglige ansvar for udbredelsen og overholdelsen af regelsættet og procedurekataloget i Morsø Kommune ligger hos lederne. Den enkelte leder på et fagområde er ansvarlig for, at der udpeges en systemejer, som er ansvarlig for sikkerheden i de fagsystemer, der anvendes på eget fagområde. Dette indbefatter bl.a. leverandørstyring, brugerstyring, risikostyring, beredskab og uddannelse af medarbejdere. Disse ansvarsområder er samtidig centrale elementer i NIS2-direktivet, som stiller krav om dokumenteret styring af cybersikkerhed og forsyningskæder.

Implementeringen af regelsættet, understøttes i de enkelte centre af informationssikkerhedsteamet, som også vejleder og hjælper fagområderne med udarbejdelsen og vedligeholdelsen af procedurekataloget.

## Sikkerhedsbevidsthed

Det er den enkelte leder, direktør eller chef, som er ansvarlig for at egne medarbejdere og eksterne samarbejdspartnere har de nødvendige kompetencer og viden til at overholde persondataforordningen og at relevante informationssikkerhedsregler, procedure og uddannelse bliver indarbejdet i de daglige arbejdsrutiner.

I henhold til NIS2-direktivet har ledelsen desuden ansvar for, at medarbejdere og samarbejdspartnere har tilstrækkelig cybersikkerhedskompetencer til at kunne identificere og håndtere relevante trusler og risici. Dette omfatter løbende awareness-aktiviteter og målrettet træning, som understøtter en stærk sikkerhedskultur i organisationen.

Informationssikkerhedsudvalget skal løbende stille nødvendig viden, information og materiale til rådighed, der kan understøtte ledernes og systemejers arbejde.

Informationssikkerhedspolitikken og de relevante informationssikkerhedsregler og -procedure skal til enhver tid være tilgængelige for lederne og medarbejderne.

Lederen og den enkelte medarbejder kan til en hver tid søge vejledning og rådgivning hos databeskyttelsesrådgiveren.

## Risikovurdering og sikkerhedsbrud

Morsø Kommune forholder sig aktivt til trusler mod informationssikkerheden og iværksætter løbende nødvendige sikkerhedsforanstaltninger for at sikre et tilstrækkeligt sikkerhedsniveau.

Der gennemføres løbende risikovurderinger på de vigtigste aktiver, herunder systemer og arbejdsprocesser i forhold til tab af fortrolighed, integritet og tilgængelighed. Desuden skal der foretages en risikovurdering ved større ændringer i fx fysiske forhold, arbejdsgange og it-systemer. Informationssikkerhedsudvalget fastlægger metode til risikovurdering.

I overensstemmelse med NIS2-direktivet skal risikovurderingerne dokumenteres og danne grundlag for prioritering af sikkerhedsforanstaltninger, herunder beredskabsplaner og genopretning af kritiske funktioner. Kommunen skal kunne dokumentere, at relevante cybersikkerhedsrisici er identificeret og håndteret, og at der er etableret passende tekniske og organisatoriske foranstaltninger.

Med udgangspunkt i risikovurderingen prioriterer informationssikkerhedsudvalget mulige sikkerhedsforanstaltninger og iværksætter de nødvendige tiltag.

Alle sikkerhedshændelser skal rapporteres til nærmeste leder og databeskyttelsesrådgiveren, som vurderer om de berørte parter skal orienteres, og om hændelsen skal rapporteres til datatilsynet.

Skulle der ske et alvorligt sikkerhedsbrud er det informationssikkerhedsudvalgets ansvar at vurdere bruddet og iværksætte de nødvendige sikkerhedsforanstaltninger.

## Overtrædelse

Overtrædelse af informationssikkerheden skal rapporteres til informationssikkerhedsudvalget og kan i alvorlige tilfælde få ansættelsesmæssige konsekvenser.

## Godkendelse og opfølgning

Informationssikkerhedspolitikken godkendes i informationssikkerhedsudvalget og revideres årligt.

| Dato | Ændring | Version | Udført af |
|---|---|---|---|
| 08.07.2022 | Opdateret | 1.5 | Informationssikkerhedskoordinator |
| 26.09.2022 | Godkendt | 1.5 | Direktionen |
| 28.11.2023 | Opdateret:<br>Tilrettet ift. ny Styregruppe for Digitalisering og Informationssikkerhed, som er det nye informationssikkerheds-udvalg | 2.0 | Informationssikkerhedskoordinator |
| 23.01.2024 | Godkendt | 2.0 | Informationssikkerhedsudvalget |
| 09.12.2024 | Opdateret: | 2.1 | Informationssikkerhedskoordinator |
| 28.03.2025 | Opdateret | 2.2 | Informationssikkerhedskonsulent |
| 03.04.2025 | Godkendt | 2.2 | Informationssikkerhedsudvalget |
| 16.03.2026 | Opdateret | 3.0 | Informationssikkerhedskonsulent |
| 29.04.2026 | Godkendt | 3.0 | Informationssikkerhedsudvalget |