Overordnet I-sikkerhedspolitik for Hjørring Kommune

Indledning
Informationssikkerhedspolitikken (I-sikkerhedspolitikken) udgør den overordnede ramme for I-sikkerheden i Hjørring Kommune. Byrådet har det endelige politiske ansvar for, at kommunen håndterer borgeres, virksomheders og øvrige offentlige myndigheders informationer på betryggende vis.

Politikken bygger på kommunens vision og strategi, blandt andet udtrykt gennem MED-aftalen samt ledelsesgrundlaget. Værdierne tillid, dialog og arbejdsglæde skal udgøre rammen for efterlevelsen af nærværende politik.

Hjørring Kommune løser en lang række opgaver, hvori der indgår personhenførbare oplysninger. Disse oplysninger skal sikres i henhold til gældende lovgivning, således at kommunen fremstår troværdig over for såvel borgere, virksomheder andre myndigheder og øvrige samarbejdsparter.

Hjørring Kommunes direktion har det øverste administrative ansvar for I-sikkerhedsarbejdet. Der er i administrationen nedsat et I-sikkerhedsudvalg, som skal sikre den overordnede koordinering og efterlevelse af politikken. I-sikkerhedsudvalgets vigtigste opgave er, at opbygge og sikre en hensigtsmæssig ramme for sikkerhedsarbejdet i alle kommunens forvaltninger og driftsenheder. Målet er, at niveauet af I-sikkerheden skal være højt uden at det opleves som en hæmsko i det daglige arbejde, sikkerhedstiltagene skal således stå mål med den konkrete risiko. Direktionen godkender kommissoriet for I-Sikkerhedsudvalget. Til at understøtte I-sikkerhedsudvalgets opgavevaretagelse, råder Hjørring Kommune over en I-sikkerhedskoordinator.

Byrådet har i henhold til EU Persondataforordning udpeget en databeskyttelsesrådgiver (DPO). Opgaverne for DPO er:

- Rådgivning om:
  - Hvorvidt en given behandling overholder de generelle behandlingsregler.
  - Indkøb af nyt IT-system inklusiv Kravsspecifikationer.
  - Underretning om sikkerhedsbrister.
  - Udarbejdelse af konsekvensanalyser.

- Overvågning:
  - Indsamling af oplysninger til identifikation af behandlingsaktiviteter.
  - Analysere og kontrollere behandlingsaktiviteter.

- Komme med anbefalinger.

- Underretning af og statusrapportering til Byrådet vedr. Hjørring Kommunes overholdelse og efterlevelse af gældende lovgivning vedr. databeskyttelse
- Kontaktpunkt for og samarbejde med Datatilsynet og borgerne.

Omfang og organisation
I-sikkerhedspolitikken omfatter den samlede informationsanvendelse i Hjørring Kommune, og gælder også behandling af eksterne informationer, som kommunen kan gøres ansvarlig for. Dette inkluderer data om kommunens borgere, virksomheder og personale, data om finansielle forhold, administrative data, produktionsdata og anlægsdata. Informationer, som videregives til kommunen af andre, ligegyldigt i hvilken form de opbevares og formidles, er ligeledes omfattet af politikken.

Overholdelse af kommunens informationssikkerhed er gældende for alle ansatte, byrådspolitikere og eksterne samarbejdspartnere. Kommunens informationssikkerhed gælder for alle lokaliteter hvor der sker en anvendelse og bearbejdning af kommunens informationer – Rådhus, institutioner, hjemmearbejdspladser, eksterne adgange, adgang via mobile enheder mv.

For leverandører, som har adgang til kommunens systemer, gælder det, at de skal have implementeret et sikkerhedsniveau, der mindst svarer til kommunens niveau. Dette sikres ved indgåelse af databehandleraftaler og gennem løbende kontrol med leverandører, således at Hjørring Kommune sikrer sig, at leverandører reelt lever op til det påkrævede sikkerhedsniveau.

Ansatte, byrådsmedlemmer og samarbejdspartnere med fysisk eller logisk adgang til kommunens systemer skal være bekendt med sikkerhedsreglerne og skal forpligte sig til at overholde reglerne.

Den overordnede informationssikkerhedsbeskrivelse består af 4 dokumenter:

1. Den overordnede I-sikkerhedspolitik, som godkendes af Byrådet (dette dokument).

2. Styring og organisering af I-sikkerhedsarbejdet, som godkendes af Direktionen

3. Hjørring Kommunes I-Sikkerhedsregler, som godkendes af I-sikkerhedsudvalget. Regelsættet tager udgangspunkt i Informationssikkerhedspolitikken, gældende lovgivning samt ISO 27001 & 27002 sikkerhedsstandarderne.

4. Proceduresamling, som opdateres løbende. I-sikkerhedsudvalget godkender nye procedurer.

Mål
I-sikkerhedspolitikken skal sikre, at Hjørring Kommune overholder gældende lovgivning, overenskomster og andre udefrakommende krav, samt understøtter og overholder kommunens IT-strategi. Relevante love, cirkulærer og vejledninger, der har indvirkning på udformningen og håndhævelsen af I-sikkerhedspolitikken skal omtales i mere detaljerede retningslinjer herfor. Hjørring Kommunes I-sikkerhedspolitik tager udgangspunkt i den til enhver tid aktuelle version af ISO Standarderne 27001 og 27002.

Hjørring Kommune fastlægger på baggrund af konkrete risikovurderinger et sikkerhedsniveau, som svarer til betydningen af de pågældende informationer og systemer. Informationssikkerhedsforanstaltningerne tilrettelægges altid i en konkret afvejning af de ofte modstridende hensyn mellem ønsket om høj sikkerhed, hensynet til øget brugervenlighed og omkostningerne ved investering i sikkerhed. Sikkerhedsniveauet og anvendelsen skal til en hver tid være i overensstemmelse med gældende lovgivning.

Ved fastlæggelse af sikkerhedsniveauet tages der udgangspunkt i 3 nøglebegreber: Fortrolighed, Integritet og Tilgængelighed. Disse begreber anvendes til afdækning af risici i samarbejde med afdelingernes system- og dataansvarlige.

<u>Fortrolighed</u>
Borgerne skal til enhver tid kunne stole på, at de trygt kan overlade deres fortrolige data til Hjørring Kommune. Informationssikkerhed skal sikre fortrolig behandling, transmission og opbevaring af data, hvor kun autoriserede brugere har adgang.

<u>Integritet</u>
Informationssikkerhed skal sikre pålidelig og korrekt brug af løsningerne og minimere risici for ukorrekt datagrundlag, f.eks. som følge af menneskelige og systemmæssige fejl eller udefra kommende hændelser.

<u>Tilgængelighed</u>
Informationssikkerhed skal være medvirkende til, at vi opnår høj tilgængelighed og minimere risiko for nedbrud på vore systemer.

Sikkerhedsniveau
Hjørring Kommune skal sikre, at der er truffet de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at persondata hændeligt eller bevidst tilintetgøres, mistes eller forringes. Endvidere skal der træffes

foranstaltninger mod, at disse kommer uvedkommende til kendskab, misbruges eller på anden måde behandles i strid med gældende lovgivning og myndighedskrav.

Der skal etableres regler for funktionsadskillelse, idet dette princip er en grundlæggende forudsætning for forebyggelse og begrænsning af konsekvenser hidrørende fra fejl, uheld og bevidst negative handlinger foretaget af enkeltpersoner.

Kommunikation af I-sikkerhed
Det er ledelsens opgave at orientere deres medarbejdere om I-sikkerhedspolitikkens regler og procedurer, herunder om ansvarlighed i forhold til Hjørring Kommunes informationer og systemdata. Medarbejderne skal løbende holdes orienteret om væsentlige ændringer, der har indflydelse på I-sikkerhedspolitikken.

Der er medarbejdernes ansvar at holde sig orienteret om I-sikkerhedspolitikkens regler og procedurer, og på baggrund heraf udvise omhu i den daglige anvendelse af informationsaktiverne.

I-sikkerheden vedrører Hjørring Kommunes samlede informationsanvendelse. Alle ansatte har et ansvar for at bidrage til at beskytte informationer mod uautoriseret adgang, ændring og ødelæggelse.

Den gældende I-sikkerhedspolitik vil være tilgængelig på Hjørring Kommunes medarbejderweb.

<u>Brud på I-sikkerheden</u>
Såfremt en ansat opdager trusler mod I-sikkerheden eller brud på denne, skal dette straks rapporteres til I-sikkerhedskoordinatoren eller nærmeste leder.

<u>Regelsæt</u>
I-sikkerhedspolitikkens bestemmelser skal udmøntes i et regelsæt, der detaljeret fastlægger kravene til I-sikkerheden. Der skal endvidere udarbejdes detaljerede procedurer og standarder, hvor det er relevant ud fra et sikkerhedsmæssigt synspunkt, samt sikkerhedsvejledninger til samtlige kommunens ansatte.

Politikken, regler, procedurer, driftsafviklingsprocedurer og sikkerhedsvejledninger samles i en I-sikkerhedshåndbog, der efter nærmere fastsatte regler skal være helt eller delvist tilgængelig for ansatte, samarbejdspartnere, borgere og virksomheder.

<u>Efterlevelse af I-sikkerhedspolitikken</u>
Der skal periodisk, dog mindst en gang årligt, udføres kontroller til afprøvning af de gennemførte sikringsforanstaltningers evne til at imødegå trusler. Dette sker ved hjælp af ISMS-systemet, som gennem kontroller udarbejder rapporter for de enkelte

fokusområder. I-sikkerhedsudvalget vurderer det aktuelle sikkerhedsbillede ud fra rapporterne. Direktionen forelægges en gang årligt resultaterne af ISMS-systemets afrapportering.

Overtrædelse af Hjørring Kommunes I-sikkerhed

Bevidst eller ubevidst overtrædelse af kommunens informationssikkerhed kan medføre, at borgernes oplysninger kompromitteres, at kommunens brugere, samarbejdspartnere, borgere mv. oplever ustabilitet, uregelmæssigheder og uhensigtsmæssigheder i anvendelse og bearbejdning af kommunens informationer. Dette kan medføre økonomisk tab og forringelse af den kommunale service og kommunens omdømme.

Overfor medarbejdere, som bevidst bryder I-sikkerhedspolitikken eller deraf afledte retningslinjer, kan der anvendes disciplinære forholdsregler i overensstemmelse med gældende regler og personalepolitik i Hjørring Kommune.

Godkendelse

Denne politik er godkendt af Byrådet 25. april 2018.