Politik for informationssikkerhed

nordfyns kommune

Indhold

Dokument nr. 2022-156584

Sags nr. 480-2018-9336

1. Indledning

Kommunalbestyrelsen har fastlagt denne Politik for Informationssikkerhed som den overordnede ramme for opretholdelse af informationssikkerheden i kommunen.

Politikken skal sikre, at kommunens informationssikkerhed til stadighed er i overensstemmelse med lovmæssige krav og egne behov.

Politikken suppleres af en Håndbog for Informationssikkerhed, som mere detaljeret fastsætter rammer og procedurer for de enkelte områder.

2. Formål

Formålet med politikken er at beskytte informationer og systemer, uanset hvor Nordfyns Kommune opbevarer og behandler disse, så borgernes og virksomhedernes tillid og retssikkerhed på området opretholdes, og så kommunens egen forvaltning har velfungerende systemer og valide informationer.

3. Mål

Kommunens regler for informationssikkerhed skal generelt bygges op omkring den til enhver tid gældende internationale standard (ISO 2700X), som er også er normsættende for den offentlige forvaltning i Danmark. Der sigtes dog ikke mod en egentlig certificering efter standarden.

Risiko- og konsekvensvurderinger skal være et bærende element i kommunens arbejde med informationssikkerheden.

Sikkerhedsindsatsen skal opfylde nedenstående mål:

- Overensstemmelse med lovgivning og eksterne krav
  - Databeskyttelsesforordningen med deraf afledt dansk lovgivning.
  - Anden relevant lovgivning.
  - Kontraktuelle krav

- Sikker drift
  - Der skal sikres et driftsmæssigt stabilt niveau, hvor data er beskyttet i forhold til en risikovurdering og i overensstemmelse med lovgivningen.

- Fysisk sikkerhed
  - For lokationer, som er vitale for opretholdelse af sikker drift, skal der etableres tilstrækkelige fysisk sikkerhed mod eksempelvis brand, vandskade, tyveri, hærværk.
  - Sikkerhedsforanstaltningerne etableres i henhold til relevante risikovurderinger.

- Adgang og rettigheder til data og systemer
  - Data og systemer skal beskyttes mod uautoriseret adgang jf. en risikovurdering.
  - Adgangen til systemer og data skal overvåges. Autorisationer og brugen af systemerne skal kontrolleres stikprøvevis.

- Anskaffelse af systemer
  - Følgende procedure skal følges ved anskaffelse af nye systemer:
    - Nordfyns Kommunes IT-arkitekt skal inddrages før ethvert tilkøb af nye It-systemer.

    - Er der tale om køb af et koncernsystem, skal digitaliseringsudvalget også inddrages forud for købet.

- Håndtering af sikkerhedshændelser
    - Sikkerhedshændelser skal løbende registreres og behandles ved DPO´s foranstaltning.
    - Såfremt der er tale om personoplysninger skal databeskyttelsesrådgiveren omgående inddrages, så den vedtagne procedure for sådanne hændelser kan blive fulgt.

- Beredskabsstyring
    - Der skal på baggrund af en risikovurdering etableres et tilstrækkeligt nødberedskab, så kommunens kritiske opgaver hurtigst muligt kan videreføres ved systemnedbrud og lignende situationer, som påvirker kommunens behandling og beskyttelse af personoplysninger.

- Sporbarhed
    - Der skal sikres den nødvendige registrering af adgang til og ændring af følsomme eller kritiske systemer, så det kan spores hvem der har foretaget handlingen.

- Evaluering
    - Der foretages løbende en revurdering af regler og procedurer for kommunens informationssikkerhed.

Informationssikkerhedsudvalget udpeger, hvem der for de enkelte områder af Håndbogen for informationssikkerhed er ansvarlig for udarbejdelse, vedligeholdelse og implementering af regler og procedurer.

4. Dækningsområde

Politik for Informationssikkerhed dækker alle områder af kommunens administration. Efter konkret aftale og i et nærmere defineret omfang kan den også omfatte eksterne parter (selvejende virksomheder m.m.) som kommunen måtte udføre services for.

Politikken dækker informationsaktiver i bredest mulig forstand, dvs.:

- It-infrastrukturen
    - Bl.a. netværk, kommunikationsudstyr, servere, personlige computere af forskellig slags

- Fagsystemer, informationssystemer
    - De forskellige systemer, som understøtter kommunens administration af diverse opgaver.
    - De systemer, som danner, opsamler og organiserer information til forskellige formål, herunder kommunens hjemmesider og sider på sociale netværk.

- Digitale teknologier i øvrigt
    - Diverse teknologier, som opsamler og behandler informationer, herunder elektronisk overvågning, velfærdsteknologier, Internet of Things.

- Papirbaserede arkiver og dokumenter
    - Disse kan have stor værdi og kan også rumme fortrolige og følsomme oplysninger, herunder personoplysninger.

5. Organisation og ansvar

Kommunen har valgt at organisere arbejdet med informationssikkerheden ud fra nedenstående roller:

- Kommunalbestyrelsen
  - Vedtager større og væsentlige ændringer af Politik for Informationssikkerhed.
  - Behandler årligt statusrapport fra Databeskyttelsesmedarbejderen (DPO).

- Direktionen
  - Vedtager redaktionelle og mindre ændringer af Politik for Informationssikkerhed. Godkender større og væsentlige ændringer i politikken, og sørger for, at disse forelægges til behandling i Kommunalbestyrelsen.
  - Udpeger medlemmerne af Informationssikkerhedsudvalget, herunder en repræsentant for direktionen, som er formand for udvalget.

- Informationssikkerhedsudvalget
  - Koordinerer kommunens arbejde med informationssikkerhed, mødes fast 4 gange årligt samt ad hoc efter behov.
  - Udpeger systemansvarlige (chef eller leder, dog minimum niveau 4 leder. Rette niveau afhænger af systemets kriminalitet)
  - Godkender ændringer i Håndbog for Informationssikkerhed.
  - Godkender risikovurderinger, udarbejdet af den systemansvarlige i organisationen.
  - Opdragsgiver til Informationssikkerhedsteamet, som er det udførende enhed.

- Databeskyttelsesrådgiveren
  - Rådgiver og påser efterlevelsen af regler på informationssikkerhedsområdet, som fremgår af Databeskyttelsesforordningen og den deraf afledte nationale lovgivning.
  - Udarbejder årligt en rapport til Kommunalbestyrelsen over det forgangene år på informationssikkerhedsområdet.
  - Er født medlem af Informationssikkerhedsudvalget, men kan ikke deltage i beslutninger, som konflikter med kravet om uafhængighed.
  - Indberetter brud på persondatasikkerheden til Datatilsynet på vegne af Nordfyns Kommune.
  - Koordinater for Informationssikkerhedsteamet, som er udførende enhed i forhold til opgaver udstukket af Informationssikkerhedsudvalget.

- It-chefen
  - Ansvarlig for informationssikkerheden i og omkring de dele af kommunens infrastruktur og systemer, som ikke er outsourcet til andre.
  - Er født medlem af Informationssikkerhedsudvalget.

- System- og dataansvarlige
  - Ansvarlig for styring af kontrakter med systemleverandører og driftsleverandører, herunder at sikrer efterlevelse af procedurer for indgåelse af og kontrol med databehandleraftaler.
  - Ansvarlig for udarbejdelse og implementering af effektive arbejdsgange og kontroller for det fagområde, som systemet understøtter.

- Lederforum
  - Kommunens ledere har inden for eget ledelsesområde ansvaret for tilsynet med, at lovgivningen og informationssikkerhedsbestemmelserne efterleves i det daglige arbejde.

- Informationssikkerhedsteamet
  - Udførende enhed i forhold til opgaver, som udstikkes af Informationssikkerhedsudvalget.

    - Kontaktenhed for systemansvarlige, ledere og medarbejdere i forhold til spørgsmål om informationssikkerhed generelt.
    - Gennemgår løbende regler og procedurer for informationssikkerhed.

- Medarbejdere
    - Alle, som er omfattet af kommunens administration, efterlever i det daglige krav og forventninger omkring informationssikkerheden, som er beskrevet i Håndbog for Informationssikkerhed.

- Samarbejdsparter
    - Samarbejdsparter, som har adgang til kommunens informationssystemer, skal i det daglige efterleve de samme krav, som stilles til kommunens medarbejdere, herunder specielle krav, som måtte være stillet i en databehandler-aftale.

6. Evaluering

Et bærende princip for kommunens informationssikkerhed er, at de ansvarlige løbende udfører risiko- og konsekvensvurderinger og sikrer den nødvendige tilpasning af sikkerhedsniveauet i overensstemmelse hermed.

Et andet bærende princip er, at der udføres interne kontroller til sikring af, at regler og procedurer efterleves i det daglige. Ansvaret for dette påhviler den systemansvarlige.

Informationssikkerhedsteamet forestår løbende en gennemgang af regler og procedurer for kommunens informationssikkerhed, med henblik på at sikre nødvendig opdatering heraf. I tilfælde af indholdsmæssige forandringer, som påvirker den specifikke opgaveløsning, skal opdateringen godkendes af Informationssikkerhedsudvalget. Dette for at sikre den nødvendige forankring af ansvaret for, at Nordfyns Kommune efterlever korrekte arbejdsgange i organisationen.

I samme forbindelse vurderes det, om ændringerne giver anledning til ændringer i Politik for Informationssikkerhed. Eventuelle ændringer af denne fremsendes via direktionen til behandling i kommunalbestyrelsen.

Mindre eller redaktionelle ændringer samt konsekvensændringer som følge af ændringer i lovgivningen kan foretages uden behandling i Kommunalbestyrelsen. Disse ændringer skal dog fortsat godkendes i direktionen. Direktionen vurderer, om Kommunalbestyrelsen bør orienteres herom.

7. Godkendelse

Denne udgave af Politik for Informationssikkerhed er godkendt i Kommunalbestyrelsen den 27/10-2022, og erstatter Nordfyns Kommunes Informationssikkerhedspolitik, godkendt den 26. april 2018.

Nordfyns Kommune
www.nordfynskommune.dk