Politik for informationssikkerhed

nordfyns kommune

Indhold

Dokument nr. 480-2022-3929

Sags nr. 480-2018-9336

1. Indledning

Kommunalbestyrelsen har fastlagt denne Informationssikkerhedspolitik 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 Informationssikkerhedshåndbog, som mere detaljeret fastsætter rammer og procedurer for de enkelte områder.

2. Formål

Formålet med politikken er at beskytte informationer og systemer, uanset hvor disse findes og behandles, så borgernes og virksomhedernes tillid og retssikkerhed på området bevares, og så kommunens egen forvaltning kan basere sig på fungerende systemer og valide informationer.

3. Mål

Kommunens regler for informationssikkerhed skal generelt bygges op omkring den internationale standard ISO 27001, 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
  - Datasikkerhedsforordningen med tilhørende 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 sikker drift, skal der etableres tilstrækkelige fysisk sikkerhed mod eksempelvis brand, vandskade, tyveri, hærværk.
  - Sikkerhedsforanstaltningerne etableres på baggrund af en risikovurdering.

- 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 og såvel anvendelsen som de givne autorisationer skal stikprøvevis kontrolleres.

- Anskaffelse af systemer
  - Før anskaffelse af systemer skal der foretages en vurdering af behovet for informationssikkerhed i forbindelse med systemet og dets anvendelse i kommunen (Databeskyttelse gennem design og standardindstillinger).

- Håndtering af sikkerhedshændelser
  - Sikkerhedshændelser skal løbende registreres og behandles.
  - Såfremt der er tale om personoplysninger skal Informations-sikkerhedsudvalget og Databeskyttelsesmedarbejderen 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 efter et nedbrud.

- 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 hvert år en revurdering af regler og procedurer for kommunens informationssikkerhed.

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

4. Dækningsområde

Informationssikkerhedspolitikken dækker alle områder af kommunens forvaltning. 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 forvaltning 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 Informationssikkerhedspolitikken.
  - Behandler årligt statusrapporter fra Informationssikkerhedsudvalget og Databeskyttelsesmedarbejderen (DPO).

- Direktionen
  - Godkender Informationssikkerhedspolitikken og sørger for, at denne forelægges til behandling i Kommunalbestyrelsen.
  - Udpeger medlemmerne af i Informationssikkerhedsudvalget, herunder en repræsentant fra direktionen, som er formand for udvalget.

- Informationssikkerhedsudvalget
  - Koordinerer kommunens arbejde med informationssikkerhed, mødes fast 4 gange årligt samt ad hoc efter behov.
  - Godkender ændringer til Informationssikkerhedshåndbogen.
  - Håndterer sikkerhedsbrud, herunder brud på persondatabeskyttelsen.

- Databeskyttelsesmedarbejderen
  - Rådgivende og kontrollerende opgaver, som nærmere er reguleret af Databeskyttelsesforordningen.
  - Udarbejder årligt en rapport til Kommunalbestyrelsen over det foregående års arbejde med Persondatabeskyttelsen.
  - Medlem af Informationssikkerhedsudvalget, men kan ikke deltage i beslutninger, som konflikter med kravet om uafhængighed.

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

- System- og dataansvarlige
  - Er for det enkelte system ansvarlig for styring af kontrakter med systemleverandører og driftsleverandører, herunder indgåelse og kontrol af data-behandleraftaler.
  - Ansvarlig for design og implementering af effektive arbejdsgange og kontroller for det forvaltningsområde, systemet understøtter.

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

- Medarbejdere
  - Alle – herunder ledere og folkevalgte - efterlever i det daglige de krav og forventninger omkring informationssikkerheden, som er defineret i lovgivningen, i kommunens regler og procedurer, eller som kendetegner ”god og sikker adfærd” på området.

- Samarbejdsparter
  - Samarbejdsparter, som har adgang til kommunens informationssystemer, skal i det daglige respektere de 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 derefter tilpasser sikkerhedsniveauet i overensstemmelse hermed.

Et andet bærende princip er, at der på relevante områder udføres interne kontroller til sikring af, at regler og procedurer også efterleves i det daglige.

Hvert år foretager Informationssikkerhedsudvalget en revurdering af regler og procedurer for kommunens informationssikkerhed.

I forbindelse hermed vurderes det, hvorvidt der er behov for at foretage ændringer i Informationssikkerhedspolitikken. Ændringer fremsendes gennem direktionen til behandling i kommunalbestyrelsen.

Redaktionelle ændringer kan foretages uden behandling i Kommunalbestyrelsen. De skal fortsat godkendes i direktionen.

7. Godkendelse

Denne Informationssikkerhedspolitik er godkendt i Kommunalbestyrelsen den 26/4 2018.

Nordfyns Kommune
www.nordfynskommune.dk