Organisering og styring af informationssikkerhed

Juli 2024

Nyborg KOMMUNE

Indhold

1. Indledning

Den overordnede informationsstrategi skaber rammerne for organiseringen af ansvar og styring af informationssikkerhed, der udmøntes i etableringen af fastsatte regler og procedurer for Nyborg Kommunes informationssikkerhedshåndtering.

Dermed etableres der et grundlag for det daglige arbejde med informationssikkerhed inden for kommunens virke.

Den samlede informationssikkerhedsbeskrivelse består af tre dele:

1. Den overordnede informationssikkerhedsstrategi – godkendes af Byrådet.

2. Organisering og styring af informationssikkerhed godkendes af Direktionen - forelægges Chefgruppen til orientering.

3. De konkrete regler og retningslinjer med direkte betydning for ledere og medarbejdere godkendes af Direktionen. Digitalisering og I-sikkerhed har herudover mulighed for at ajourføre samt indføre retningslinjer af teknisk karakter i samarbejde med IT-afdelingen.

Både organisering og styring af informationssikkerhed og konkrete regler revideres ved behov inden for rammerne af den overordnede informationssikkerhedsstrategi.

Dette dokument beskriver organiseringen af ansvar og styring af informationssikkerheden i Nyborg Kommune. Sammen med den overordnede strategi, en løbende risikovurdering, de udarbejdede retningslinjer for informationssikkerhed og selve arbejdet i i-sikkerhedsorganisationen, dannes grundlaget for sikker håndtering af information i Nyborg Kommune.

Dokumentet bygger på principper fra ISO27001.

2. Organisationens kontekst

Nyborg Kommunes administrative organisation kan ses på www.nyborg.dk

Parter, der er relevante for informationssikkerheden:

- Borgere og virksomheder
- Ansatte
- Datatilsynet
- Center for Cybersikkerhed
- Digitaliseringsstyrelsen
- Leverandører og eksterne samarbejdspartnere

Informationssikkerhed er kommunens samlede foranstaltninger til at sikre fortrolighed, tilgængelighed og integritet. Foranstaltninger inkluderer bl.a. organisatoriske, adfærdsmæssige, fysiske og teknologiske kontroller.

Relevant lovgivning vedrørende informationssikkerhed:

- Databeskyttelsesforordningen (nr. 2016/679 af 27. april 2016)
- Databeskyttelsesloven (nr. 502 af 23. maj 2018)
- Forvaltningsloven (nr. 433 af 22. april 2014)
- Arkivloven (nr. 1201 af 28. september 2016)

Kontraktlige forpligtelser, der påvirker informationssikkerheden:

- Kontrakter på løsninger og samarbejde med eksterne parter
- Databehandleraftaler
- Licensstyring
- Ansættelsesbreve (de ansatte bliver allerede ved ansættelsen informeret om kravet om at overholde kommunens regler for informationssikkerhed).

2.1. Anvendelsesområdet for informationssikkerhedsregler

Informationssikkerhedsreglerne gælder alle organisatoriske enheder i Nyborg Kommune: Politikere, administrationen, decentrale enheder og eksterne parter, der har adgang til Nyborg Kommunes informationer.

Reglerne gælder informationer både i digital- og i papirform.

3. Roller, ansvar og beføjelser i organisationen

3.1. Sikkerhedsorganisationen

Informationssikkerhedsstrategien godkendes af Byrådet og varetages af kommunaldirektøren (eller dennes stedfortræder), der er kommunens øverste sikkerhedsansvarlige. Det daglige arbejde udføres i samarbejde med kommunens informationssikkerhedsorganisation, der har ansvaret for at sikre, at strategi, politik og regler er synlige, koordineret og i overensstemmelse med kommunens overordnede principper og mål for informationssikkerhed.

Informationssikkerhedsorganisationen består af følgende:

- Den øverste sikkerhedsansvarlige (kommunaldirektøren eller dennes stedfortræder).
- Direktionen.
- Chefgruppen.

Direktionen skal føre tilsyn med og sikre, at Nyborg Kommune lever op til kravene i lovgivningen vedrørende informationssikkerhed og databeskyttelse, herunder udstikker rammerne for arbejdet mv.

Ansvaret for tilsyn og koordination af sikkerhed på tværs af organisationen bæres af den øverste sikkerhedsansvarlige i samarbejde med direktionen og chefgruppen.

Cheferne skal sikre udbredelsen af informationssikkerhedsbeskrivelsen til egne ledere og medarbejdere – helt ud i de decentrale enheder - og sikre overholdelsen af informations-sikkerheden i de fagspecifikke områder og for systemer inden for deres ansvarsområde.

Den tekniske overvågning af systemer foretages af IT-afdelingen, der bl.a. kan udtrække logs af systemerne.

Den daglige kontakt vedrørende informationssikkerhedshændelser varetages af Digitalisering og I-sikkerhed i samarbejde med databeskyttelsesrådgiveren.

3.2. Ledelsens rolle og engagement

Den øverste sikkerhedsansvarlige skal aktivt lede og støtte de medarbejdere, der er ansvarlige for at vedligeholde informationssikkerheden.

Ledelsen på alle niveauer skal støtte kommunens informationssikkerhed ved at udlægge klare retningslinjer, udvise synligt engagement og sikre præcis placering af ansvar.

Det er ledelsens ansvar:

- At ansatte er tilstrækkeligt informeret om deres roller og ansvar i forbindelse med informationssikkerhed.

- At ansatte tilegner sig kompetencer og opmærksomhedsniveau i spørgsmål vedrørende informationssikkerhed, der er i overensstemmelse med deres roller og ansvar i kommunen.

- At medarbejderne kun har adgang til de IT-systemer og rettigheder, som de har et arbejdsbetinget behov for, herunder ændring af rettigheder, hvis medarbejderen får andre arbejdsopgaver.

- At der føres tilsyn med at data i de anvendte systemer er korrekte.

- At der er udarbejdet relevante lokale procedurer relateret til informationssikkerhed.

Herudover skal ledelsen sikre varetagelsen af sikkerheden for de systemer, som de er systemejere og ansvarlige for. Oversigten kan ses på Nyborg Kommunes intranet.

Ledelsen skal endvidere:

- Kommunikere betydningen af at overholde kravene til informationssikkerhed.
- Aktivt fremme og støtte løbende forbedringer af informationssikkerheden.

3.3. Direktionens rolle

Direktionen skal sikre, at Nyborg Kommune lever op til kravene i databeskyttelsesforordningen, databeskyttelsesloven, NSIS samt tilstræbes ISO27001.

Der er nedsat en koordinationsgruppe, der forbereder og følger op på punkter til møder i direktionen. Koordinationsgruppen består af direktør, sekretariatschef, IT-chef, leder af Digitalisering og I-sikkerhed, leder af Personale og HR samt relevante medarbejdere ad. hoc. Arbejdet dækker områderne:

- Informationssikkerhedspolitik, vejledninger, kommunikation, uddannelse, sagsbehandling og databeskyttelse.

- Sikkerhed i IT-systemer, autorisationer og fysisk sikkerhed.

- Systemansvarlige, databehandleraftaler, standardfortegnelser, risikovurdering, beredskabsplaner og forretningsgange.

- IT-revision og rapportering til den øverste ledelse.

Koordinationsgruppen drøfter emnerne og indstiller forslag til direktionen.

3.4. IT-afdelingens rolle

IT-afdelingen er ansvarlig for den samlede IT-infrastruktur i kommunen, herunder serverplatform, kommunikationslinjer og tværgående systemer.

IT-afdelingen er ansvarlig for oprettelse af autorisationer og ændring af rettigheder til systemer efter godkendelse hos nærmeste leder eller systemansvarlig. Tildeling af autorisationer skal følge autorisationsproceduren.

Godkendelse og oprettelse af autorisation skal ske indenfor 14 dage.

Håndtering af nedbrud på tværgående IT-løsninger varetages af IT-afdelingen.

Ved kritiske IT-nedbrud indkaldes kriseberedskabet, jf. beredskabsplanen "Nødberedskab for it-anvendelsen".

Det er IT-chefen, der i de enkelte tilfælde beslutter, hvorvidt kriseberedskabet skal igangsættes.

3.5. Digitalisering og I-sikkerhed

Digitaliserings- og I-sikkerhedsenheden under Økonomi og Digitalisering varetager opgaver vedrørende både digitaliseringsprojekter samt opgaver vedrørende I-sikkerhed og databeskyttelse. Enheden bistår med konsulentbistand vedrørende bl.a. følgende opgaver:

- Sekretariatsbetjening af direktionen(kommunaldirektør formand).
- Implementering og efterlevelse af Strategi for Informationssikkerhed.
- Vedligeholdelse af Organisering og styring af informationssikkerhed.
- Skriftlige forretningsgange, vejledninger og interne kontroller.
- Retningslinjer for brugeradgang til IT-systemer og autorisationer.
- Implementering af kvalitetsstandard ISO 27001 for I-sikkerhed.
- Udarbejdelse af risikovurderinger og beredskabsplaner.
- Ajourføring af oversigt med systemejere og systemansvarlige.
- Indgåelse af databehandleraftaler med eksterne leverandører.
- Kontrol af revisorerklæringer fra eksterne leverandører.
- Fortegnelse over databehandlingsaktiviteter i kommunen.
- Løbende afrapportering til den øverste ledelse i kommunen.
- Sagsbehandling i forhold til databeskyttelsesretlige problemstillinger.
- Uddannelse af ledere og medarbejdere i persondatalovgivningen og I-sikkerhed.
- Deltagelse i diverse digitaliseringsprojekter og udbud af IT-systemer.
- Opfølgning på ekstern IT-revision.

Nyborg Kommune har i henhold til databeskyttelsesforordningen udpeget en særlig databeskyttelsesrådgiver (DPO), som skal understøtte, at kommunen overholder de databeskyttelsesretlige regler. Databeskyttelsesrådgiveren er advokatfirmaet Bech-Bruun, der samarbejder med Digitalisering og I-sikkerhed, men rapporterer til direktionen og Byrådet.

3.6. Distribution af informationssikkerhedsbeskrivelsen

Informationssikkerhedsbeskrivelsen skal kommunikeres ud i organisationen. Dette sker via SPOTS/mails, intranettet, undervisning, via behandling i MED-organisationen, på ledergruppemøder, afdelingsmøder mv.

Informationssikkerhedsbeskrivelsen skal være tilgængelig for alle relevante parter. Beskrivelsen publiceres på kommunens intranet for medarbejdere og på kommunens hjemmeside for borgere og virksomheder.

I forbindelse med indgåelse af samarbejdsaftaler med IT-leverandører og eksterne parter henvises der til informationssikkerhedsbeskrivelsen for at sikre, at deres sikkerhedsniveau som minimum svarer til kommunens niveau.

4. Risikovurdering og håndtering

Der skal udføres en risikovurdering på alle kritiske behandlingsaktiviteter og understøttende IT-systemer. Risikovurderingerne skal opdateres når systemer/infrastruktur/behandlings-aktiviteter ændrer sig og fast minimum en gang årligt.

Risikohåndtering har betydning for hvilke krav vi stiller til bl.a.:

- Beredskabsplaner.
- Uddannelse.
- Databehandleraftaler og tilsyn.
- Håndtering af sikkerhedsbrud.

Konsekvensanalyse, både i forhold til ISO 27001 og GDPR, udarbejdes på alle behandlings-aktiviteter og understøttende IT-systemer med høj risiko.

Risikovurdering og konsekvensanalyse skal udføres efter den af direktionens godkendte metode.

4.1. Ejerskab

Systemanskaffelser skal altid forelægges IT-afdelingen til en teknisk afklaring og Digitaliseringsstyregruppen i forhold til økonomi og godkendelse af systemejer.

Databeskyttelsesrådgiveren (DPO) skal inddrages i alle væsentlige spørgsmål vedrørende beskyttelse af personoplysninger, herunder indkøb af nye IT-systemer og indgåelse af databehandler-aftaler med eksterne leverandører af IT-systemer m.v.

IT-kontrakter og databehandleraftaler underskrives af systemejeren.

Der udpeges altid en systemejer af alle kommunens systemer.

I Nyborg Kommune ejes fagsystemerne altid af chefen for den afdeling, som er primære udfører på opgaven, der løses via systemet. Hvis fagsystemet anvendes af flere afdelinger,

så tildeles ansvaret til chefen af den afdeling, som har flest brugere af løsningen, eller hvor systemet logisk bør være forankret.

IT-afdelingen er systemejer af infrastruktur som serverplatform, kommunikationslinjer og fællessystemer (fx Outlook).

Digitalisering og I-sikkerhed sørger løbende for at holde systemejer og -ansvarlig -oversigten opdateret.

Systemejerne kan uddelegere opgaver til de systemansvarlige som f.eks. drift af systemet, uddannelse af brugerne, information til brugerne, kontakt til IT-afdeling eller ekstern IT-leverandør i forbindelse med driftsforstyrrelser eller systemnedbrud. Brugerne kan tilmelde sig løbende orienteringer vedrørende driftsforstyrrelser o. lign. via SMS-service eller driftssupport på hjemmeside.

5. Sikkerhedsbevidsthed

5.1. Uddannelse i informationssikkerhed

Ved introduktion af nye medarbejdere præsenteres de for kommunens informations-sikkerhedsregler.

Det er ligeledes obligatorisk, at alle nye medarbejdere i løbet af den første tid gennemgår et e-learningsforløb i informationssikkerhed. Dette kursus gentages derefter en gang årligt.

Alle IT-brugere skal læse og sætte sig ind i kommunens informationssikkerhedsregler.

Den enkelte leder har ansvaret for den løbende kompetenceudvikling og træning af medarbejderne i kommunens informationssikkerhedsbeskrivelse. Ledelsens arbejde kan understøttes af jævnlige informationer og produkter fra Digitalisering og I-sikkerhed, der formidler disse på forskellige måder: e-mail, video, plakater, opslag på intranettet, møder, kampagner mv.

Ud over E-learning skal alle ansatte i løbet af hhv. 1 år for ledere og administrative og 2 år for andre fagområder, have deltaget i særligt tilrettelagt fysisk undervisning afholdt af Digitalisering og I-sikkerhed.

5.2. Kommunikation om informationssikkerhed

Kommunikationsplan for informationssikkerhed er følgende:

Ved indførelse af nye regler orienteres relevante dele af organisationen.

Chefgruppen har efterfølgende ansvaret for udbredelse og implementering af nye tiltag, der retter sig mod deres del af organisationen.

Den løbende kommunikation varetages af Digitalisering og I-sikkerhed.

For hver udmelding omkring informationssikkerhed skal følgende vurderes:

- Hvornår skal der kommunikeres?
- Modtagere?
- Hvem, der skal kommunikere?
- Hvordan kommunikationen skal foretages (medie/form)
- Hvad der skal kommunikeres?

6. Evaluering, tilsyn og opfølgning

Direktionen fører løbende tilsyn med I-sikkerheden i Nyborg Kommune.

Databeskyttelsesrådgiveren og Digitalisering og I-sikkerhed rapporterer til Direktionen og Økonomiudvalget i alt to gange årligt.

To gange årligt udføres der ledelsestilsyn i forhold til overholdelse af informations-sikkerheden i Nyborg Kommune. Resultatet rapporteres til Direktionen, der tager stilling til eventuelle tiltag på baggrund af ledelsestilsynet.

Den interne kontrol skal sikre, at sikkerhedsbeskrivelsen er velimplementeret i organisationen, og at ansvar og regler overholdes (så vi er trygge ved, at "det virker", og at vores indsats giver resultater). Denne kontrol forventes at ske i forbindelse med ledelsestilsynet, og bør omfatte beskrivelsen af evt. årsag til afvigelser og handlingsplan, der er nødvendig for at håndtere afvigelserne (korrigerende handlinger).

Kontrollen af sikkerhed for fagsystemerne foretages stikprøvevist for de fagsystemer, der udvælges af Digitaliserings- og I-sikkerhedsenheden og/eller databeskyttelsesrådgiveren.

Borgerservice følger særskilte retningslinjer for logning.

Outsourcede informationssikkerhedsprocesser styres via databehandleraftaler og revisionserklæringer.

Digitaliserings- og I-sikkerhedsenheden gennemgår og vurderer behov for revision af informationssikkerhedsbeskrivelsen en gang om året. Den revideres altid når de forretningsmæssige behov eller kommunens mål ændres.

7. Håndtering af sikkerhedshændelser

7.1. Informationssikkerhedshændelser

Nyborg Kommune har oprettet et team til håndtering af informationssikkerhedshændelser, også kaldet et "information security incident response team" (ISIRT), som har til formål at håndtere og vurdere informationssikkerhedshændelser.

Teamet til håndtering af informationssikkerhedshændelser består af én ansvarlig, som enten er lederen af Digitalisering og I-sikkerhed eller IT-chefen. Derudover består den af to medlemmer fra IT-afdelingen og to medlemmer fra Digitalisering og I-sikkerhed.

Teamet håndterer informationssikkerhedshændelser fra konstatering til afslutning, herunder bl.a. sagsoprettelse, vurdering af hændelsen og dokumentation. Teamet evaluerer på konstaterede informationssikkerhedshændelser og rapporterer løbende om relevante informationssikkerhedshændelser til ledelsen.

7.2. Brud på persondatasikkerheden

I Nyborg Kommune håndteres brud på persondatasikkerheden af Digitalisering og I-sikkerhed.

Digitalisering og I-sikkerhed håndterer brud på persondatasikkerheden fra konstatering til afslutning, herunder bl.a. sagsoprettelse, vurdering af bruddet og dokumentation. Derudover foretager Digitalisering og I-sikkerhed anmeldelse til Datatilsynet, såfremt det er påkrævet.

Digitalisering og I-sikkerhed evaluerer på konstaterede brud på persondatasikkerheden og rapporterer løbende om relevante brud på persondatasikkerheden til ledelsen.

8. Godkendelse

Organisering og styring af informationssikkerhed er godkendt i Direktionen 20. september 2022. Teknisk tilrettet af Digitalisering og I-sikkerhed juli 2023

Nyborg
KOMMUNE
Torvet 1
5800 Nyborg
www.nyborg.dk