Overordnet informationssikkerhedsstrategi

2/2019

Nyborg
KOMMUNE

Indhold

Indledning 3

Mål for sikkerhedsniveau 3

Holdninger og principper 4

Kodeks 5

Gyldighed og omfang 6

Organisering, ansvar og godkendelse 6

Sikkerhedsbevidsthed 6

Overtrædelse 7

Godkendelse 7

Indledning

Det er et krav, at Nyborg Kommune som dataansvarlig myndighed sikrer beskyttelse af personoplysninger.

Byrådet har det endelige politiske ansvar for, at kommunen håndterer borgere, virksomheder og øvrige offentlige myndigheders informationer på betryggende vis.

I forhold til kommunens egen lokale digitaliseringsstrategi, har vi længe selv valgt at digitalisere opgaveløsningen i form af selvbetjeningsløsninger til borgerne og til effektivisering af de interne arbejdsgange. Ydermere er kommunerne i de senere år, fra centralt hold, blevet pålagt at indføre obligatorisk digital selvbetjening og digital kommunikation med borgere, virksomheder og samarbejdspartnere. Digitalisering er således et vilkår og ikke blot et muligt tilvalg.

Dette stiller store krav til vores informationssikkerhed og er dermed en afgørende faktor for kommunens digitaliseringsindsats.

Dette dokument beskriver Nyborg Kommunes overordnede informationssikkerhedsstrategi. Strategien sætter rammerne for operationel organisering og styring af informationssikkerhed, der udmøntes i etableringen af fastsatte regler og procedurer for Nyborg Kommunes informationssikkerhedshåndtering. Hermed etableres grundlaget for det daglige arbejde med informationssikkerhed inden for kommunens virke.

Den samlede informationssikkerhedsbeskrivelse består af tre dele:

1. Den overordnede informationssikkerhedsstrategi – som godkendes af Byrådet.
2. Organisering og styring af informationssikkerhed – der fastlægger ansvar og styring. Denne godkendes af direktionen og tager udgangspunkt i ISO27001 standarden, som KL anbefaler at kommunerne anvender.
3. De konkrete regler og retningslinjer, som vi alle skal overholde i det daglige arbejde. Vi bestræber os på at arbejde efter ISO27002 standarden for informationssikkerhed. Disse regler godkendes af kommunens styregruppe for i-sikkerhed.

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

Mål for sikkerhedsniveau

Nyborg Kommune fastlægger på baggrund af konkrete risikovurderinger et sikkerhedsniveau. Sikkerhedsniveauet og anvendelsen skal til en hver tid være i overensstemmelse med gældende lovgivning.
Ved fastlæggelse af sikkerhedsniveauet, tages der udgangspunkt i tre begreber: *Fortrolighed, Integritet* og *Tilgængelighed*. Disse begreber anvendes til afdækning af risici i samarbejde med afdelingernes system- og dataansvarlige.

Fortrolighed

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

Integritet
Informationssikkerhedsstrategien skal sikre pålidelighed, korrekt brug af løsningerne samt søge at minimere risikoen for ukorrekt datagrundlag fx som følge af menneskelige og systemmæssige fejl eller udefra kommende hændelser.

Tilgængelighed
Informationssikkerhed skal være medvirkende til, at vi opnår høj tilgængelighed og minimerer risikoen for nedbrud på kommunens systemer.

Nyborg Kommune skal dermed træffe de fornødne foranstaltninger for at beskytte oplysninger mod uautoriseret anvendelse, fejl i de registrerede eller behandlede oplysninger og til at sikre den højst mulige "oppetid" for vores løsninger.

Holdninger og principper

Troværdigheden på informationssikkerhedsområdet over for omverdenen, herunder borgere, virksomheder og samarbejdspartnere, må ikke kunne drages i tvivl. På den måde kan kommunen opnå og bibeholde et godt omdømme over for borgere og virksomheder.

Nyborg Kommune vil fastlægge informationssikkerhedsforanstaltninger som en afvejning mellem de ofte modstridende hensyn, ønsket om høj sikkerhed, hensynet til brugervenlig it-anvendelse og omkostningerne ved investering i sikkerhed.

Sikkerhedsforanstaltninger kan til tider opleves som en barriere for medarbejdernes daglige anvendelse af IT og kan give anledning til besværlige arbejdsgange. Her vil Nyborg Kommune sikre medarbejdernes forståelse for nødvendigheden af disse foranstaltninger, således at sikkerhed bliver en naturlig del af arbejdet i kommunen. Nyborg Kommune vil løbende arbejde med at informere medarbejderne, så de får de nødvendige kompetencer, til at sikre at informationssikkerheden kan overholdes samtidige med, at arbejdet kan udføres så effektivt som muligt.

Følgende tre målsætninger konkretiserer ovennævnte principper:

1. *Fortrolighed i forvaltningen*
   Vi vil i vores it-anvendelse sikre, at behandling af data og informationer sker med fortrolighed og i overensstemmelse med god forvaltningsskik. Informationssikkerhed skal derfor sikre, at informationer om borgerne holdes fortroligt for uvedkommende.

2. *Sikre kommunens medarbejdere, borgere og virksomheder adgang til en stabil og korrekt kommunal service*
   Nyborg Kommune understøtter alle forretningsområder, borgere og virksomheder med digitale løsninger for at sikre en effektiv administration, der medfører hurtig og korrekt service.

Informationssikkerhedsforanstaltninger skal sikre borgere og virksomheder tilgængelighed og pålidelighed i adgang til de eksterne systemer på www.nyborg.dk og selvbetjeningsløsninger.

For de interne systemer skal der sikres stabil drift, således at it-anvendelsen understøtter korrekt service til tiden.

3. *Forebyggende sikkerhed*
   Informationssikkerheden skal implementeres gennem forebyggende tekniske tiltag og informationsaktiviteter, der øger medarbejdernes kompetencer og viden omkring informationssikkerhed.

   Tekniske kontroller er væsentlige, men den menneskelige faktor i form af brugeradfærd ses som den største risikofaktor. Den menneskelige faktor kan ikke kontrolleres og er derfor afhængig af medarbejdernes kompetencer og forståelse for deres rolle i forbindelse med informationssikkerhed.

Kodeks

Hovedudvalget har 14. juni 2019 vedtaget følgende kodeks for informationssikkerhed:

Kodeks for arbejdet med informationssikkerhed

- Vi værner altid om vores oplysninger. Borgerne skal vide, at der passes på deres personfølsomme oplysninger.
- Fejl sker. Det skal være trygt at dele og lære af fejl.
- Kontrol er et arbejdsvilkår, men kontrol skal overholde de etiske spilleregler som åbenhed, respekt, tillid og højt informationsniveau.
- Kontrol af informationssikkerheden skal ske i form af varslet/aftalt tilsyn på den enkelte arbejdsplads.
- Overordnet ansvar er lederens. Men arbejdet med informationssikkerheden er et fælles ansvar og skal ske i gensidig respekt mellem ledere og medarbejdere.
- Brug den sunde fornuft.

Kendetegn i praksis:

- Vi er klædt på i forhold til at håndtere informationssikkerhed. Ved et højt informationsniveau og læring.
- Vi bruger indberetninger om sikkerhedsbrud til læring i afdelingen og hele organisationen.
- Vi er opmærksomme på, at ansatte har forskellige behov i forhold til læring om emnet.
- Vi rydder op inden vi går hjem (makulere, låse af osv.).
- Mine kolleger gør mig opmærksom på det, hvis jeg ikke passer godt nok på borgernes oplysninger.
- Vi afstemmer regelmæssigt informationssikkerhedsniveauet på personalemøder.

Gyldighed og omfang

Alle ansatte, byrådspolitikere og eksterne samarbejdspartnere skal overholde kommunens strategi og retningslinjer omkring informationssikkerhed.

Kommunens strategi og retningslinjer omkring informationssikkerhed gælder for alle lokaliteter, hvor kommunens informationer bliver anvendt og bearbejdet; Rådhuset, institutioner, hjemmearbejdspladser, eksterne adgange, adgange via mobil, Ipad mv.

For leverandører, der 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. Desuden skal Nyborg Kommune have mulighed for at sikre sig, at leverandører reelt lever op til det påkrævede sikkerhedsniveau.

Ansatte, byrådsmedlemmer og samarbejdspartnere med fysisk[1] eller logisk[2] adgang til kommunens systemer skal være bekendt med sikkerhedsreglerne og skal forpligte sig til at overholde reglerne.

Organisering, ansvar og godkendelse

Informationssikkerhedsstrategien godkendes af Byrådet og varetages af kommunaldirektøren, der er den øverste sikkerhedsansvarlige. Det daglige arbejde udføres i samarbejde med kommunens i-sikkerhedsorganisation.

I-sikkerhedsorganisationen består af den øverst sikkerhedsansvarlige, en i-sikkerhedsstyregruppe og chefgruppen.

Kommunaldirektøren er formand for i-sikkerhedsstyregruppen, der mødes hver 2. måned – og straks i forbindelse med alvorlige i-sikkerhedshændelser. I-sikkerhedsstyregruppens kommissorium er vedhæftet som bilag.

I-sikkerhedsstyregruppen sikrer, i samarbejde med den øverste sikkerhedsansvarlige, vedligeholdelse af den samlede informationssikkerhedsbeskrivelse: Den overordnede informationssikkerhedsstrategi, Organisering og styring af Informationssikkerhed og de konkrete regler og retningslinjer. Ligeledes sikrer styregruppen den løbende risikovurdering og information til ledelsen omkring informationssikkerhed.

Chefgruppen er ansvarlig for udbredelsen af informationssikkerhedsregler til egne medarbejdere og for overholdelse af informationssikkerheden på de fagspecifikke områder og systemer inden for deres ansvarsområde.

Sikkerhedsbevidsthed

Medarbejdere med adgang til kommunens systemer skal overholde de informationssikkerhedsregler, der er relevante for deres arbejde. Her er det ledelsens ansvar at sikre, at medarbejderne får de fornødne kompetencer, og at informationssikkerhed bliver en del af kulturen og indarbejdes i arbejdets tilrettelæggelse.

[1] Fysisk computeradgang betyder evnen til at se, røre og ændre computerens installationer.
[2] Logisk computeradgang er netadgang evt. via intranet eller internettet

I-sikkerhedsstyregruppen arbejder kontinuerligt med information i form af forskellige oplysningsmaterialer, e-learnings mv., der kan understøtte ledelsens arbejde med udvikling af medarbejdernes kompetencer omkring informationssikkerhed.

Det skal til en hver tid være muligt for medarbejderne at få adgang til den overordnede informationssikkerhedsstrategi, informationssikkerhedsregler og de underliggende procedurer via kommunens intranet.

Overtrædelse

Bevidst eller ubevidst overtrædelse af kommunens informationssikkerhed kan medføre, at borgernes oplysninger kompromitteres, og 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.

Sikkerhedsbrud skal indberettes til kommunens databeskyttelsesrådgiver (DPO) med det samme. Det er den daglige leders ansvar. I tilfælde af alvorlige overtrædelser vurderes overtrædelsen af kommunaldirektøren og kan få ansættelsesretlige konsekvenser.

Databeskyttelsesrådgiveren orienterer I-sikkerhedsstyregruppen om indberetningerne i form af statistik på styregruppens møder. I-sikkerhedsstyregruppen vurderer på baggrund heraf, om der skal igangsættes tiltag.

Godkendelse

Den overordnede informationssikkerhedsstrategi skal godkendes af Nyborg Byråd.

Godkendt af Nyborg Byråd den 28.4.2018. Strategien er efterfølgende konsekvenstilrettet efter organisationsændring i april 2019 med godkendelse i Nyborg Byråd 17.09.2019.