Strategi for Persondatabeskyttelse og Cybersikkerhed 2026-2028

- balancen mellem mennesker, teknologi og processer

Nyborg KOMMUNE

IT og Digitalisering
December 2025

Indhold

Indledning

Strategi for Persondatabeskyttelse og Cybersikkerhed udgør Nyborg Kommunes fælles grundlag og forståelse af informationssikkerhed. Den fastlægger ambitionsniveau, ansvar og rammer for de nødvendige sikkerhedstiltag, der skal sikre overholdelse af lovgivning og best practice.

Informationssikkerhed handler om at beskytte alle ressourcer, der indgår i eller understøtter behandling og kommunikation af data – både elektronisk, på papir og i andre former. Dette omfatter såvel teknologiske løsninger som organisatoriske processer.
Persondatabeskyttelse vedrører beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger, herunder indsamling, registrering, videregivelse og sletning, jf. EU's databeskyttelsesforordning (GDPR) og de supplerende bestemmelser i databeskyttelsesloven.

Strategi for Persondatabeskyttelse og Cybersikkerhed er grundlaget for det daglige arbejde med informationssikkerhed inden for Nyborg Kommunes virke, og er en del af den samlede *informationssikkerhedsbeskrivelse* som består af tre dele:

1. Strategi for Persondatabeskyttelse og Cybersikkerhed der ligeledes fastlægger ansvar, organisering og styring. Denne tager udgangspunkt i GDPR og ISO27001 standarden. Godkendes af Byrådet.

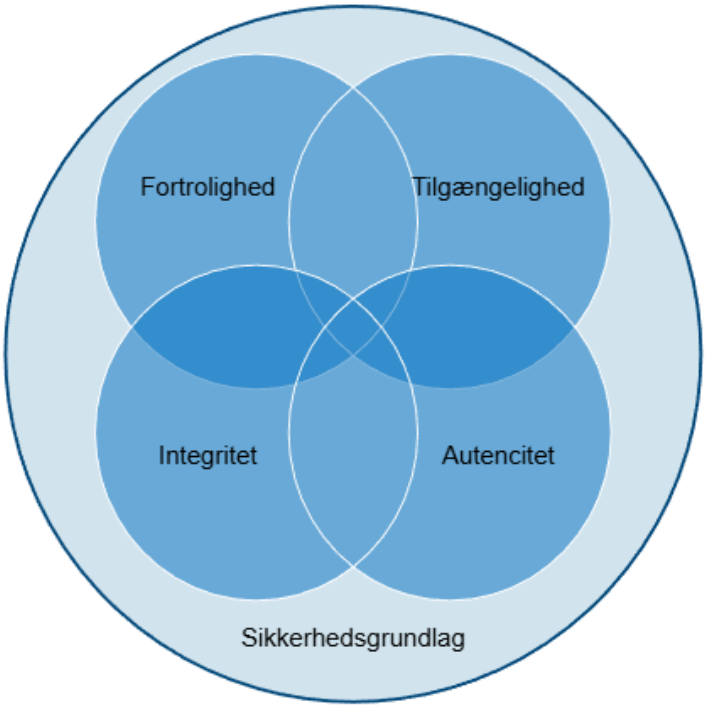
2. IT-sikkerhedsprogrammet, der tager udgangspunkt i CIS18-kontroller og NIS2-loven[1]. IT-sikkerhedsprogrammet suppleres med en handleplan for IT-sikkerhed (fortrolig), hvor konkrete indsatser, der skal styrke Nyborg Kommunes evne til at beskytte systemer, data og processer mod cybersikkerhedstrusler er prioriteret. Godkendes af Direktionen.

3. Konkrete regler og retningslinjer, som skal overholdes i det daglige arbejde. Regler og retningslinjer ajourføres løbende inden for rammerne af Strategi for Persondatabeskyttelse og Cybersikkerhed. Godkendes af Direktionen. Tekniske tilretninger kan løbende ajourføres af IT og Digitalisering.

[1] *CIS18-kontroller* fungerer som en teknisk guide og prioriteringsværktøj, der skal sikre, at Nyborg Kommune arbejder struktureret med de mest kritiske sikkerhedstiltag først.
NIS2-loven er et lovkrav som Nyborg Kommune er pålagt at overholde. Formålet med NIS2 er at forbedre den kritiske IT-infrastruktur til et niveau, der er tilsvarende nutidens risiko- og trusselsbillede.

1. Sikkerhedsgrundlag og lovgivning

Nyborg Kommune fastlægger på baggrund af risikovurderinger et passende sikkerhedsgrundlag på baggrund af den vedtagne risikoaccept.



Ved fastlæggelse af et passende sikkerhedsgrundlag, tages der udgangspunkt i begreber: *Fortrolighed, Integritet, Tilgængelighed og Autencitet*. Disse begreber anvendes til afdækning af risici i samarbejde med afdelingernes system- og dataansvarlige.

Fortrolighed skal sikre, at information, som Nyborg Kommune ligger inde med, ikke gøres tilgængelig eller afsløres for uvedkommende.

Integritet 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 skal være medvirkende til, at der opnås høj tilgængelighed og minimerer risikoen for nedbrud på Nyborg Kommunes systemer. Herunder driftskontinuitet, som dækker over foranstaltninger til opretholdelse af vedvarende drift (backup, overvågning og logning) samt gendannelse og test efter katastrofe- og krisesituationer.

Autenticitet skal sikre, at personer og systemer i Nyborg Kommune er legitime og verificeret.

2. Principper og målsætninger

Strategien skal understøtte Nyborg Kommunes virke i forhold til at sikre stabiliteten, fortroligheden samt pålideligheden vedrørende den information, som vi behandler. Det sikres ved, at vi i vores daglige arbejde lever op til grundlæggende principper for persondatabeskyttelse, både som dataansvarlig og databehandler, samt standarder for så vidt angår informationssikkerhed. Herved understøtter strategien, at Nyborg Kommune fortsat vil kunne leve op til forventninger om troværdighed.

Nyborg Kommune vil balancere organisatoriske og tekniske sikkerhedsforanstaltninger som en afvejning mellem de ofte modstridende hensyn til ønsket om høj sikkerhed, hensynet til effektive arbejdsgange og omkostningerne ved investering i sikkerhed.

Sikkerhedsforanstaltninger kan til tider opleves som en barriere for de ansattes daglige arbejdsgange. Her vil Nyborg Kommune sikre medarbejdernes forståelse for nødvendigheden af disse foranstaltninger, således at sikkerhed bliver en naturlig del af arbejdet. Nyborg Kommune vil løbende arbejde med at informere de ansatte, så de får de nødvendige kompetencer, til at sikre, at sikkerheden kan overholdes samtidige med, at arbejdet kan udføres så effektivt som muligt.
Nyborg Kommunes målsætninger for informationssikkerhed skal derudover efterleve kodeks for arbejdet med informationssikkerhed, som blev vedtaget af Hovedudvalget den 14. juni 2019[2].

Kodekset sikrer, at vi værner om borgernes personoplysninger og, at de behandles med respekt og ansvarlighed. Fejl kan ske, og det skal være trygt at dele og lære af dem. Kontrol er en del af arbejdsvilkårene, men skal udføres etisk – med åbenhed, respekt, tillid og tydelig kommunikation. Tilsyn med informationssikkerheden skal være varslet og aftalt lokalt. Det overordnede ansvar ligger hos lederen, men arbejdet med informationssikkerhed er et fælles ansvar, der bygger på gensidig respekt.

3. Omfang og gyldighed

Strategi for Persondatabeskyttelse og Cybersikkerhed gælder for alle ansatte og byrådspolitikere, samt for alle fagsystemer og al information og personoplysninger, som vi behandler. Eksterne samarbejdspartnere, som har adgang til organisationens systemer og data, skal ligeledes efterleve Strategi for Persondatabeskyttelse og Cybersikkerhed.

4. Organisering og ansvar

Ansvaret for tilsyn og koordination af sikkerhed på tværs af organisationen bæres af den øverste sikkerhedsansvarlige (kommunaldirektøren eller dennes stedfortræder) i samarbejde med Direktionen og chefgruppen. Den øverste sikkerhedsansvarlige skal aktivt lede og støtte de medarbejdere, der er ansvarlige for at vedligeholde informationssikkerheden. Det daglige arbejde udføres i samarbejde med Nyborg Kommunes informationssikkerhedsorganisation.

[2] Kodeks for arbejdet med I-sikkerhed i Nyborg Kommune

4.1 Koordinationsgruppe for I-sikkerhed

Der er nedsat en koordinationsgruppe, der forbereder og følger op på punkter til møder i Direktionen. Koordinationsgruppen består af chef for Økonomi og Digitalisering, leder af IT og Digitalisering, leder af Byrådssekretariatet, leder af HR samt relevante medarbejder ad. hoc.

Samarbejdet dækker udarbejdelse af:

- Sikkerhed i IT-systemerne jf. IT-sikkerhedsprogram (fx overvågning, back up og logning), autorisationer og fysisk sikkerhed.
- Regler og retningslinjer samt kommunikation, uddannelse, sagsbehandling og databeskyttelse.
- Databehandleraftaler, standardfortegnelser, risikovurdering, beredskabsplaner og forretningsgange.
- IT-revision og rapportering til den øverste ledelse.

4.2 Byrådets rolle

Byrådet har det overordnede ansvar for Nyborg Kommunes drift herunder, at vi overholder gældende lov i forhold informations- og IT-sikkerhed. Byrådet orienteres løbende om større og væsentlige beslutninger på området, og som minimum 2 gange årligt.

4.3 Direktionens rolle

Direktionen skal sikre, at Nyborg Kommune lever op til kravene i databeskyttelsesforordningen, databeskyttelsesloven og herunder deres juridisk ansvar i henhold til NIS2-loven. Nyborg Kommune arbejder desuden efter KL's anbefalinger, ud fra grundprincipperne i ISO 27001, som skal understøtte arbejdet med at overholde kravene i relevant lovgivning, herunder GDPR og NIS2-loven. 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.

4.4 Chefgruppens rolle

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.

4.5 Decentrale lederes rolle

Ledelsen på alle niveauer skal støtte Nyborg Kommunes informationssikkerhed ved at efterleve vores retningslinjer, udvise synligt engagement og sikre placering af ansvar lokalt.

Det er leders ansvar, at:

- Medarbejderne er tilstrækkeligt informeret om deres roller og ansvar i forbindelse med informationssikkerhed og persondatabeskyttelse.
- Medarbejderne tilegner sig kompetencer og bevidsthed i spørgsmål vedrørende informationssikkerhed, der er i overensstemmelse med deres roller og ansvar i Nyborg Kommune.
- Medarbejderne ved oprettelse 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.
- De personoplysninger medarbejderne behandler i respektive fagsystemer er korrekte.
- Der er udarbejdet relevante lokale procedurer relateret til informationssikkerhed, herunder supplerende nødplaner til Nyborg Kommunes IT-beredskabsplan.

Herudover skal ledere med systemejerskab sikre varetagelsen af sikkerheden for de systemer, som de er ansvarlige for. Oversigten kan ses på Nyborg Kommunes intranet.

5. Relevante aktører og rammer

Nyborg Kommunes administrative organisation kan ses på www.nyborg.dk. Relevante aktører:

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

Relevant lovgivning:

- Databeskyttelsesforordningen
- Databeskyttelsesloven
- Forvaltningsloven
- Arkivloven
- Lov om foranstaltninger til sikring af højt cybersikkerhedsniveau (NIS2-loven)

Kontraktlige forpligtelser, der påvirker informationssikkerheden:

- Kontrakter på løsninger og samarbejde med eksterne parter
- Databehandleraftaler

- Licensstyring
- Ansættelsesbreve
- Fortrolighedserklæring (NDA)

6. Tekniske og organisatoriske sikkerhedsforanstaltninger

Nyborg Kommune gennemfører løbende risikovurderinger af behandlingsprocesser, kritiske IT-løsninger samt teknisk infrastruktur for at identificere hvilke passende og nødvendige foranstaltninger, der skal implementeres. Risici og risikovillighed identificeres på baggrund af *Risikovurderingskonceptet* (godkendt af Direktionen) og munder ud i udarbejdelse af organisatoriske tiltag i form af regler, retningslinjer og uddannelse, samt standard designindstillinger i processer og fagsystemer, som skal sikre behandling efter best practice og dermed understøtte vores overholdelses af gældende lovgivning.

6.1 Regler og retningslinjer

Informationssikkerhed handler ikke kun om teknik i en IT-afdeling, men i lige så høj grad om adfærd i *hele* organisationen. I regler og retningslinjer kan der læses om, hvordan alle medvirker til at sikre Nyborg Kommunes sikkerhed. Alle ansatte har pligt til at kende og overholde de gældende regler og retningslinjer.

Regler og retningslinjer findes på Nyborg Kommunes intranet under IT og Digitalisering, og ajourføres og opdateres løbende. Hvis ændringer af regler og retningslinjer har en større påvirkning på din arbejdsgang, vil dette meldes ud.

6.2 Information og undervisning

Ansatte med adgang til Nyborg Kommunes fagsystemer skal overholde de gældende regler og retningslinjer for håndtering af personoplysninger, der er relevante for deres arbejde. Det er ledelsens ansvar at sikre, at medarbejderne har de nødvendige kompetencer, og at informationssikkerhed integreres i de daglige arbejdsgange.

Derudover skal alle medarbejdere være bekendt med reglerne for behandling af persondata samt de grundlæggende retningslinjer for cybersikkerhed.

Det er ligeledes obligatorisk, at alle nye ansatte i løbet af den første tid gennemgår e-learningsuddannelse i GDPR og IT-sikkerhed. Dette kursus gentages derefter en gang årligt.

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 IT og Digitalisering.

Den enkelte leder har ansvaret for den løbende kompetenceudvikling og tilmelding af medarbejderne til relevante og obligatoriske kurser, der udbydes. Ledelsens arbejde kan understøttes af jævnlige informationer og produkter fra IT og Digitalisering, der formidler disse på forskellige måder: SPOT-mails, nyhedsbreve, opslag på intranettet, møder, kampagner mv.

Der skal til en hver tid være muligt for de ansatte at få adgang til den overordnede Strategi for Persondatabeskyttelse og Cybersikkerhed, samt regler og retningslinjer der ligger tilgængeligt på intranettet.

6.3 IT-sikkerhedsprogram og standardindstillinger

I Nyborg Kommune er der udarbejdet et IT-sikkerhedsprogram, som via en konkret handleplan har til formål at styrke sikkerheden på vores tekniske infrastruktur og governance. Som en del af denne indsats tages der udgangspunkt i NIS2 og CIS18. NIS2-loven pålægger blandt andet omfattede organisationer, herunder Nyborg Kommune, at implementere 10 minimumsforanstaltninger til styring af cybersikkerhedsrisici.

NIS2 og CIS18 overlapper og komplementerer hinandens standarder og krav, og skaber dermed et effektivt grundlag for at opfylde både juridiske og tekniske forpligtelser. Mens NIS2 lægger vægt på Nyborg Kommunes ansvar og ledelsens involvering, hjælper CIS18 med at fokusere på de vigtigste sikkerhedstiltag og sikre, at indsatsen bliver prioriteret efter de største risici – og dermed understøtter overholdelsen af kravene.

Tekniske minimumskrav
IT og Digitalisering har udarbejdet en række minimumskrav til tekniske løsninger. Disse minimumskrav skal understøtte Nyborg Kommunes – og dermed Direktionens – overholdelse af NIS2-loven. Kravene til systemer, IT-løsninger mv. baseres på en risikobaseret tilgang.

Direktionen har ansvaret for at sikre, at relevante dele af disse minimumskrav formidles videre til

organisationen. I den forbindelse er der et særligt fokus på indkøbsprocessen, der indebærer, at Nyborg Kommunes afdelinger:

1) Altid skal kontakte IT og Digitalisering forud for indkøb software og hardware.
2) Ikke køber software eller hardware, der ikke opfylder de tekniske minimumskrav til IT-løsninger samt de 10 NIS2-lovbestemte minimums foranstaltninger, der beskrives i IT-sikkerhedsprogrammet[3] .

Privacy by design og Privacy by default
Herudover skal vi sikre, at IT-løsninger implementeres i overensstemmelse med GDPR-principperne om *Privacy by Design* og *Privacy by Default*. Disse principper understøtter blandt andet dataminimering og opbevaringsbegrænsning i vores IT-systemer og arbejdsgange.

IT og Digitalisering er garant for, at disse principper overholdes, forudsat at indkøb og implementering af IT-løsninger sker gennem afdelingen. Det er derfor ledelsens ansvar at sikre, at alle indkøb af software og hardware koordineres med IT og Digitalisering.

7. Brud og hændelser

Bevidst eller ubevidst overtrædelse af Nyborg Kommunes informationssikkerhed kan medføre brud på fortrolighed, integritet og tilgængelighed anses som sikkerhedsbrud, og skal indberettes med det samme.

I Nyborg Kommune håndteres brud og hændelser af IT og Digitalisering.

Brud og hændelser kan skyldes en menneskelig fejl, fx en medarbejder, der ved en fejl har videregivet personoplysninger til en forkert modtager eller et IT-nedbrud hos kommunen eller leverandøren af et fagsystem hvor også persondata bliver kompromitteret.
IT og Digitalisering håndterer brud og hændelser fra konstatering til afslutning, herunder bl.a. sagsoprettelser, vurdering af bruddet og dokumentation. Derudover foretager IT og Digitalisering selve anmeldelse til Datatilsynet under Justitsministeriet og Forsvarets Efterretningstjeneste CSIRT under Styrelsen for Samfundssikkerhed, såfremt det er påkrævet.

[3] IT-sikkerhedsprogram 2025-2027 (fortroligt)

IT og Digitalisering evaluerer på konstaterede brud og hændelser på persondatasikkerheden og rapporterer løbende om relevant brud på persondatasikkerheden til Direktion og Økonomiudvalget.

8. Godkendelse

Godkendt af Byrådet den 16. December 2025