Politik for informationssikkerhed

nordfyns kommune

Indhold

Dokument nr. D2026-897

Sags nr. 480-2018-9336

Ref til ISO 27002:2022	Ansvarlig for vedligeholdelse	Revisionshyppighed
5.1	Informationssikkerhedskonsulent med kvalificering af Udvalg for Digitalisering og Informationssikkerhed	Årlig
	Godkendt af:	**Godkendt den:**
	Direktionen og Kommunalbestyrelsen	5.11.2025 af direktionen og 18.12.2025 af Kommunalbestyrelsen.
Målgruppe: Alle ansatte i Nordfyns Kommune, samarbejdspartnere og leverandører, politikere		

1. Indledning

Direktionen og Kommunalbestyrelsen har fastlagt denne Politik for Informationssikkerhed som den overordnede ramme for opretholdelse af informationssikkerheden i Nordfyns Kommune.

Politikken skal sikre, at Nordfyns Kommunes informationssikkerhed til stadighed er i overensstemmelse med lovmæssige krav, anerkendte standarder og egne behov. Politikken gælder for alle medarbejdere, ledere, politikere og samarbejdspartnere med adgang til Nordfyns Kommunes informationer og systemer.

Politikken bygger på følgende principper:

- Risikobaseret tilgang til sikkerhed
- Klar ansvars- og rollefordeling
- Forankring i både teknologi, processer og adfærd
- Løbende forbedring gennem opfølgning og læring

Politikken understøttes af emnespecifikke procedurer/retningslinjer, som mere detaljeret fastsætter rammer for de enkelte områder. Nordfyns Kommune fører fortegnelse over disse.

2. Formål

Formålet med politikken er at fastlægge rammerne for arbejdet med informationssikkerhed. Herudover er formålet 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.

Derudover skal politikken være med til at skabe en fælles forståelse af, hvad informationssikkerhed er, herunder beskrive målsætningerne og ansvarsfordelingen for arbejdet med informationssikkerhed i Nordfyns Kommune.

3. Definitioner

Med **informationssikkerhed** forstås beskyttelsen af samtlige aktiver, der indgår i eller bidrager til behandling af data både i elektronisk og fysisk form. Beskyttelsen omfatter alle

relevante foranstaltninger; herunder foranstaltninger der relaterer sig til organisatoriske processer, personorienteret adfærd, fysiske rammer og teknologi.

Med **data** forstås al information der relaterer sig til Nordfyns Kommune myndighedsudøvelse samt information, der relaterer sig til medarbejdere i Nordfyns Kommune.

4. Målsætninger for cybersikkerhed

Kommunens regler for informationssikkerhed skal generelt bygges op omkring den til enhver tid gældende internationale standard (ISO 27001), som også er normsættende for den offentlige forvaltning i Danmark. Der sigtes dog ikke mod en egentlig certificering efter standarden.

Kommunen har desuden som målsætning at sikre en fortsat levering af samfundskritiske tjenester i overensstemmelse med kravene i NIS 2-direktivet.

Cybersikkerhedsarbejdet skal:

- Beskytte Nordfyns Kommunes net- og informationssystemer mod hændelser og angreb, herunder bevare informationers fortrolighed, integritet og tilgængelighed.
- Forebygge og begrænse sårbarheder og konsekvenser af sikkerhedshændelser.
- Styrke ledelsesforankring og ansvarlighed, så cybersikkerhed integreres i den overordnede styring og prioritering.
- Understøtte borgernes og samfundets tillid til kommunens digitale tjenester og informationsbehandling.
- Opfylde gældende lovgivning, herunder NIS 2-krav.

Risiko- og konsekvensvurderinger er et bærende element i kommunens arbejde med informationssikkerheden. Sikkerhedsniveauet i Nordfyns Kommune er fastlagt ud fra en vurdering af de risici, som kommunen ønsker at reducere til et acceptabelt niveau. Grundlaget er kommunens risikotolerance, lovgivning og anerkendte standarder (ISO 27001, NIS2, CIS18).

Risikovurderinger gennemføres løbende på baggrund af systemer og enheders kritikalitetsniveau samt ved ændringer i trusselsbillede, teknologi eller forretningsgange. Metoden følger standarden i ISO 27005. Vurderingerne dokumenteres i Wired Relations og danner grundlag for udvælgelse og justering af kontroller.

Sikkerhedsindsatsen prioriteres ud fra foranstaltninger på fire niveauer med udgangspunkt i ISO 27002:2022 og relevante risikovurderinger:

- **Organisatoriske foranstaltninger**: vedrører, at Nordfyns Kommune har beskrevne procedurer på relevante sikkerhedsområder og sikrer forankring i fagområderne. Procedurerne er vedtaget af Direktionen og revideres årligt eller ved ændring i trusselsbilledet.

- **Personorienterede foranstaltninger**: vedrører, at alle ansatte gøres bevidst om deres sikkerhedsansvar ved ansættelse samt løbende modtager rollebaseret awareness-træning. Hertil følger ansvar ved distancearbejde, brug af mobile enheder mv.

- **Teknologiske foranstaltninger**: vedrører, at systemer, enheder, netværk og data er beskyttet i henhold til kritikalitet, leverandørsikkerheden, trusler og sårbarheder, fx via logning og logkontrol, adgangsrettigheder, beredskabsstyring og håndtering af sikkerhedshændelser.

- **Fysiske foranstaltninger**: vedrører beskyttelse af it-udstyr og lokationer, som er vitale for opretholdelse af sikker drift. Her skal der etableres tilstrækkelige fysisk sikkerhed mod eksempelvis brand, vandskade, tyveri og hærværk.

5. NIS 2-overholdelse

Nordfyns Kommune er omfattet af kravene i NIS 2-direktivet (EU-direktiv 2022/2555) og NIS 2 loven (LOV nr. 434 af 06/05/2025), som har til formål at styrke cybersikkerheden og sikre et højt fælles niveau for cybersikkerhed i organisationer, der varetager den kritiske samfundsinfrastruktur i EU.

NIS 2-overholdelsen er baseret på en risikobaseret tilgang som grundlag for sikring af et passende sikkerhedsniveau omkring kommunens aktiviteter. I valget af sikkerhedsforanstaltninger inddrages hensyn til det aktuelle tekniske niveau, gennemførelsesomkostninger og risiciene mod sikkerheden i enhedens net- og informationssystemer.

ISO 27001 anvendes som overordnet ramme til at sikre, at kommunen overholder NIS 2 og understøtter de tre centrale krav i NIS 2 direktivet:

- Ledelsespligter
- De 10 minimumskrav til foranstaltninger for styring af cybersikkerhed
- Krav om hændelsesunderretning

NIS 2-overholdelsen er integreret i kommunens informationssikkerhedsarbejde, der også sikrer overholdelse af øvrige lovkrav som f.eks. GDPR og AI-forordningen. Dette vil regelmæssigt blive revideret og indarbejdet i takt med ændringer i lovgivning, teknologi og trusselsbillede. Læring fra hændelser, f.eks. sikkerhedsbrud, anvendes desuden til at forbedre både politikken og de tilhørende procedurer.

Nordfyns Kommunes tilgang til styring af sikkerhed i net- og informationssystemer er herunder:

- **Ledelse og governance:** Direktionen fastsætter mål der sikrer et passende cybersikkerhedsniveau, godkender og prioriterer foranstaltninger, fører tilsyn med NIS 2 implementeringen og modtager undervisning og oplæg. Informationssikkerhedsudvalget og -konsulenten støtter Direktionen i opfyldelse af NIS 2-kravene, følger løbende op og koordinerer indsatsen.

- **Risikostyring:** Der er implementeret risikostyring som sikrer passende tekniske, personorienterede, fysiske og organisatoriske foranstaltninger til håndtering af risici, som truer sikkerheden i net- og informationssystemer. Disse foranstaltninger er risikobaserede og proportionelle i forhold til de identificerede trusler og sårbarheder.

- **Forsyningskædesikkerhed:** Der stilles sikkerhedskrav til leverandører og samarbejdspartnere, der leverer kritiske IT-tjenester. Kravene omfatter tekniske sikkerhedsforanstaltninger, hændelseshåndtering, og rapportering – samt sikrer, at leverandører underlægger sig tilsvarende sikkerhedsprincipper som kommunen.

- **Håndtering og rapportering af hændelser:** Der er etableret proces for registrering og håndtering af sikkerhedshændelser. Som led i NIS2-overholdelsen er der defineret interne processer og tidsfrister for rapportering af væsentlige hændelser til relevante myndigheder, herunder SAMSIK, inden for de fastsatte tidsrammer

(indenfor 24 timer ved væsentlige hændelser). Der iværksættes forebyggende tiltag som awareness-træning og teknisk sikring på baggrund af læring fra hændelser.

- **Overvågning og kontrol:** Der foretages løbende intern kontrol, evaluering og test af cybersikkerhedsforanstaltninger, herunder sårbarhedsscanning, awarenesstræning og gennemgang af beredskabsplaner. Udvalget for Digitalisering og Informationssikkerhed fører løbende tilsyn og sikrer dokumentation for overholdelse.
- **Træning og awareness:** Alle relevante medarbejdere uddannes i god cybersikkerhedspraksis og opmærksomhed på trusler, som en del af den årlige awarenesstræning. Særlige målgrupper, herunder ledelse, udsatte jobroller, informationssikkerhedskonsulent og Digitalisering og Teknologi modtager målrettet uddannelse i forhold til funktion.
- **Anskaffelse af systemer**: Nye it-systemer skal gå igennem Digitalisering og Teknologi, hvor de vurderes ift. It-arkitektur, risikoprofil og kritikalitet inden indkøb.
- **Dokumentation og rapportering:** Alle krav i NIS2, som er relevante for kommunen, dokumenteres i kommunens ISMS-system, Wired Relations, og indarbejdes i procedurer, politikker, beredskabsplaner og kontroller. På dette grundlag udføres regelmæssig vurdering af foranstaltningernes effektivitet og ajourføring af dokumentationen.
- **Evaluering:** Der foretages løbende en revurdering af procedurer for kommunens informationssikkerhed. Udvalget for Digitalisering og Informationssikkerhed udpeger, hvem der for de enkelte procedurer er ansvarlig for udarbejdelse, vedligeholdelse og implementering.

6. Dækningsområde

Politik for Informationssikkerhed dækker alle fagområder i kommunen. 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.

7. Organisation, roller 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 Databeskyttelsesrådgiveren (DPO).

- Direktion
  - Har det overordnede ansvar for, at kommunen lever op til kravene i NIS 2
  - 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 Udvalg for Digitalisering og Informationssikkerhed, herunder en repræsentant for direktionen, som er formand for udvalget.
  - Godkender foranstaltninger til styring af cybersikkerhedsrisici og fører tilsyn med implementeringen
  - Sætter mål, regelmæssigt orienteres om status og tager stilling til kommunens cybersikkerhed og foranstaltningers effektivitet
  - Tilskynder til awareness-træning af alle kommunens medarbejdere

- Udvalg for Digitalisering og Informationssikkerhed
  - Koordinerer og kvalificerer 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 kritikalitet)
  - Godkender ændringer og kvalificerer procedurer for informationssikkerhed, inden de forelægges Direktionen og følger op på implementeringen
  - Opdragsgiver til Informationssikkerhedsteamet og -konsulenten, som er den udførende enhed.
  - Godkender organisatorisk årshjul for informationssikkerhed og statusrapporter, der udarbejdes af informationssikkerhedskonsulenten

- Databeskyttelsesrådgiveren (DPO)
  - 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 forgangne år på informationssikkerhedsområdet
  - Er født medlem af Udvalg for Digitalisering og Informationssikkerhed, men kan ikke deltage i beslutninger, som konflikter med kravet om uafhængighed.
  - Indberetter brud på persondatasikkerheden til Datatilsynet på vegne af Nordfyns Kommune.
  - Inddrages i konsekvensanalyser

- Informationssikkerhedskonsulent
  - Rapporterer til Direktion på status for informationssikkerhed generelt i Nordfyns Kommune, herunder NIS 2 og GDPR
  - Koordinator for Informationssikkerhedsteamet, som er udførende enhed i forhold til opgaver udstukket af Udvalg for Digitalisering og Informationssikkerhed.
  - Central styring med opgaver relateret til informationssikkerhed, fx udarbejdelse og revision af politikker og procedurer og udrulning af awareness-træning
  - Faglig bistand og sparring til systemejere og systemansvarlige i fagområderne, fx ifm. risikovurderinger, tilsyn med leverandører, indgåelse af databehandleraftaler, udarbejdelse af konsekvensanalyser og TIA'er.
  - Løbende compliance-opgaver relateret til informationssikkerhed.
  - Dokumentation af compliance i ISMS-system og etablering af governance-strukturer, der sikrer kontinuerlig indsats, genbesøg og justering.

- Indberetter brud på persondatasikkerheden til Datatilsynet på vegne af Nordfyns Kommune, hvis Databeskyttelsesrådgiveren er forhindret.
- Ansvarlig for organisatorisk implementering af sikkerhedsforanstaltninger

- Stabschef for Strategi og Politik
  - Ansvarlig for informationssikkerheden i og omkring de dele af kommunens infrastruktur og systemer, som ikke er outsourcet til andre.
  - Er født formand for Udvalg for Digitalisering og Informationssikkerhed.

- System- og risikoejer
  - Ansvarlig for styring af kontrakter med systemleverandører og driftsleverandører, herunder at sikre efterlevelse af procedurer for indgåelse af og kontrol med databehandleraftaler, tilsyn og evaluering af leverandører mm.
  - Ansvarlig for udarbejdelse og implementering af effektive arbejdsgange og kontroller ift. informationssikkerhed for det fagområde, som systemet understøtter.
  - Sikrer at nye IT-løsninger implementeres og visiteres via Digitalisering og Teknologi
  - Sikrer at risikovurderingerne og evt. konsekvensanalyser genbesøges med passende interval. Systemejer er i udgangspunktet risikoejer for systemets risici
  - Ansvarlig for systemers overholdelse af minimumskrav via fx stikprøvekontrol, fx funktionsadskillelse, adgangsrettigheder, adfærdslog og sletteprocedurer
  - Orienterer direktion og informationssikkerhedskonsulent ved alvorlige fejl, som har eller kan have konsekvens for driften

- Systemansvarlig
  - Kan være udførende på opgaver relateret til systemejeren, fx udarbejdelse af risikovurderinger og opgaver relateret hertil

- Lederforum (chefer og ledere)
  - Kommunens ledere har inden for eget ledelsesområde ansvaret for tilsynet med, at lovgivningen og informationssikkerhedsbestemmelserne efterleves i det daglige arbejde, fx kendskab til procedurer
  - Adgangs- og rettighedsstyring og generel cyberhygiejne i egne teams
  - Tilskyndelse til awareness-træning i egne teams
  - Sikre at fagområdets behandlingsaktiviteter løbende er dokumenteret og opdateret i kommunens ISMS-system via informationssikkerhedskonsulenten
  - Ansvar for at It-adgange lukkes samt at udleveret udstyr og adgangsbrik til medarbejdere og besøgende afleveres tilbage ifm. ophør

- Informationssikkerhedsteam
  - Udførende enhed i forhold til opgaver, som udstikkes af Udvalget for Digitalisering og Informationssikkerhed
  - Gennemgår løbende regler og procedurer for informationssikkerhed.

- Alle ansatte
  - Efterlever i det daglige krav og forventninger omkring informationssikkerheden, som er beskrevet i Nordfyns Kommunes Politik for informationssikkerhed, informationssikkerhedshåndbog og relevante procedurer
  - Deltager aktivt i den awareness-træning, Nordfyns Kommune udbyder
  - Indberetter sikkerhedshændelser hurtigst muligt til Digitalisering og Teknologi
  - Indberetter persondatabrud til Databeskyttelsesrådgiveren hurtigst muligt

- Digitalisering og Teknologi
  - Ansvarlig for teknisk implementering af sikkerhedsforanstaltninger
  - Vurdering, koordinering og indberetning af væsentlige sikkerhedshændelser til relevante myndigheder jf. NIS 2

- 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.

8. Dokumentation og 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 systemejerne.

Udvalget for Digitalisering og Informationssikkerhed 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 Udvalg for Digitalisering og Informationssikkerhed, inden den godkendes af Direktionen. 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.

Nordfyns Kommune dokumenterer arbejdet med informationssikkerhed samt efterlevelsen af de databeskyttelsesretlige regler i Nordfyns Kommunes ISMS-system, Wired Relations.

9. Revisionslog

Årsag til revision	**Dato**	**Initialer**
Revideret og tilpasset til NIS 2	20-10-2025	niccl

Nordfyns Kommune
www.nordfynskommune.dk