

Politik for Informationssikkerhed

1-16-4-1549-24

Indhold

1 Formål, målgruppe og omfang	2
2 Politikens indhold.....	4
3 Definition af begreber	6
4 Relaterede dokumenter	7
5 Godkendelse og revision.....	8

*Denne politik er udarbejdet af Informationssikkerhed.
Ved spørgsmål kontaktes informationssikkerhed@rn.dk.*

1 Formål, målgruppe og omfang

1.1 Formål

Region Nordjyllands Politik for Informationssikkerhed udgør fundamentet for Regionens fælles forståelse af informationssikkerhed. Formålet med politikken er at fastlægge ambitionsniveauet og sætte klare rammer for de centrale sikkerhedstiltag, som Regionen skal følge for at leve op til gældende lovgivning og håndtere risici effektivt.

Politik for Informationssikkerhed redegør for de centrale mål, prioriterede indsatser, samt roller og ansvar i Regionens informationssikkerhedsarbejde.

Region Nordjylland er en samfundskritisk aktør, og det er dermed afgørende, at Regionen beskytter oplysninger og systemer med høj grad af fortrolighed, integritet, tilgængelighed og autencitet. Region Nordjylland stiller derfor høje krav til cyber- og informationssikkerhed for at sikre lovoverholdelse og en tryk service for borgere og medarbejdere. Informationssikkerhed er højt prioriteret, og der arbejdes løbende med forbedringer, som skal sikre, at informationssikkerhed er en naturlig del af de øvrige kerneaktiviteter, som Regionen udfører.

1.2 Målgruppe

Målgruppen for Politik for Informationssikkerhed er alle Regionens medarbejdere, herunder Regionsrådet, Direktionen, samt informationssikkerhedsorganisationen, de interne stabe og kontorer. Derudover er politikens målgruppe leverandører og eksterne konsulenter, der behandler information på vegne af Region Nordjylland.

Alle medarbejdere har ansvar for at beskytte Regionens informationer og følge gældende politikker, retningslinjer og instrukser.

1.21 Roller og ansvar

Ansvar for informationssikkerheden i Region Nordjylland er entydigt forankret i Regionens Direktion. Dette stadfæster et klart risikoejerskab og sikrer, at det overordnede sikkerhedsniveau i Regionen afstemmes på tværs i hele organisationen, herunder virksomheder, hospitaler og administrationen.

Region Nordjylland har en Informationssikkerhedsledelse, som har til formål at sikre et ledelsesforankret grundlag for sikkerhedsarbejdet i Regionen. Herunder at sikre Regionens drift med en balanceret risikoappetit, samt at træffe risikomitigerende tiltag.

Politik for Informationssikkerhed ejes af Region Nordjyllands Direktion. Implementeringen og efterlevelse sker i et samarbejde mellem IT-direktøren, Informationssikkerhedsledelsen og den øvrige organisation.

Nedenfor i tabellen vises en oversigt over områder og roller og ansvar i sikkerhedsarbejdet.

Område	Rolle og ansvar
Regionsrådet	Fastlægger de overordnede strategiske og økonomiske rammer for Regionens aktiviteter, som danner grundlag for Regionens arbejde med informationssikkerhed.
Direktionen	Overordnet ansvar for, at uddelegeringen af informations-sikkerhedsopgaver er i overensstemmelse med de rammer Regionsrådet har besluttet. Direktionen har det endelige ansvar for Regionens risikostyring. Direktionen ejer og underskriver af Politik for Informationssikkerhed.
IT-Direktøren	Binder Informationssikkerhedsledelsen og Direktionen sammen og sikrer en fornuftig og praktisk beslutningsproces, så eksekvering kan ske i et passende tempo.
Informationssikkerhedsledelsen (ISL)	Består af IT-direktøren, ledelsesrepræsentanter fra Digitalisering og IT, Jura samt sekretariatsbetjening fra Informationssikkerhedsteamet. Informationssikkerhedsledelsen inddrages når der skal træffes beslutninger relateret til cyber- og informationssikkerhed.
Databeskyttelsesrådgiver (DPO)	Rådgivende funktion i arbejdet med informationssikkerhed. DPO'en vejleder og overvåger, at Regionen efterlever regler om databeskyttelse. DPO'en inddrages i sager, hvor det vil være relevant og/eller påkrævet efter GDPR, f.eks. i anskaffelser af it-systemer, hændelser eller auditopfølgninger, hvor der sker eller vil ske behandling af personoplysninger. DPO'en er kontaktled til Datatilsynet og samarbejder med Datatilsynet på vegne af Region Nordjylland.
Informationssikkerhedsteamet	Varetager den daglige drift af informationssikkerhedsarbejdet. Teamets opgaver er at understøtte og drive informationssikkerhedsarbejdet på tværs af hele Region Nordjylland. Teamet udarbejder blandt andet politikker og retningslinjer, foretager risikovurderinger understøtter Regionens overholdelse af gældende lovgivning.
Informationssikkerhedsambassadører	Udpeges på tværs af administration, virksomheder og hospitaler. Har øget fokus på informationssikkerhed og holdes opdateret om tiltag på sikkerhedsområdet, så god og sikker håndtering af følsomme og fortrolige oplysninger kan forankres lokalt.

1.22 Beslutningsproces

Sager med informationssikkerhedsmæssig karakter behandles i første omgang af Informationssikkerhedsledelsen. Sagerne kan i visse tilfælde have en karakter, som kræver en behandling i et eller flere andre fora i Regionen. Det er f.eks. sager, som omfatter hele Regionen og som omhandler ledelsesgrundlag, det samlede budget og kommunikationsstrategi.

Direktionen

I sager der vedrører informationssikkerhed, der berører hele Regionen, eller hvor der er ønske

om ledelsesmæssig godkendelse på højere niveau, vil sagen blive ført videre til Direktionen. Informationssikkerhedssager, der skal løftes ind i Hovedudvalget, vil normalt blive behandlet i Direktionen forinden.

Hovedudvalget

I sager, som har betydning for arbejds-, personale-, samarbejds- eller arbejdsmiljøforhold, er Hovedudvalget altid/som udgangspunkt en del af sagsgangen. Hovedudvalget indgår typisk i sagsgangen ved at drøfte sagen, inden der træffes endelig beslutning.

1.3 Omfang

Politik for Informationssikkerhed omfatter styring af informationssikkerhed i alle Regionens net- og informationssystemer, herunder både styring af tekniske, organisatoriske og operationelle foranstaltninger.

2 Politikkens indhold

Politik for Informationssikkerhed skal understøtte, at de oplysninger, som Region Nordjylland behandler og kommunikerer til borgere, samarbejdspartnere og offentlige myndigheder, er tilgængelige, forbliver fortrolige og fremstår med korrekt indhold. Dette sikres blandt andet ved, at Regionen i det daglige arbejde lever op til anerkendte principper for informationssikkerhed, herunder standarder, rammeverker og gældende lovgivning. Regionen arbejder risikobaseret med aktiv styring af informationssikkerhedsrisici. Risici rapporteres til ISL og risikoejere jf. Regionens politik for risikostyring.

2.1 Sikkerhedsmål

Region Nordjyllands sikkerhedsmål for informationssikkerhedsområdet er at have et højt informationssikkerhedsniveau under hensyntagen til en effektiv udførelse af Regionens primære opgaver og den økonomiske ramme, som Regionen er underlagt. Det sker via en klar ledelsesforankring, samt en forretningsorienteret og risikobaseret tilgang til sikkerhed.

Sikkerhedsmål realiseres ved:

- at have en klart defineret informationssikkerhedsorganisation, så det er tydeligt, hvor informationssikkerhed er forankret, samt hvordan samarbejdet med resten af organisationen styres, forvaltes og organiseres
- at benytte en ensartet metode til arbejdet med informationssikkerhed på tværs af organisationen
- at sikre en ensartet og kontinuerlig rapportering på risici, igangværende initiativer og efterlevelse af lovgivning og reguleringer.

Informationssikkerhed indebærer blandt andet beskyttelse af oplysninger mod utilsigtede hændelser. Arbejdet med informationssikkerhed tager udgangspunkt i de principper som informationssikkerhedsorganisationen arbejder efter.

Principperne skal sikre:

- fortrolighed – at kun de rette personer har adgang til rette oplysninger
- integritet – at oplysningerne er korrekte, komplette og sikret mod uautoriserede ændringer
- tilgængelighed – at oplysningerne er tilgængelige og brugbare, når der er behov for det
- autencitet – at oplysninger er ægte og stammer fra den kilde, det hævder at være.

2.2 Prioritering af sikkerhedsforanstaltninger

For at nå Region Nordjyllands sikkerhedsmål arbejdes der løbende med modning af en række sikkerhedsforanstaltninger. Sikkerhedsforanstaltningerne prioriteres risikobaseret, og justeres minimum en gang årligt.

2.3 Lovgivning og standarder

Region Nordjylland arbejder med at systematisere og opretholde et Information Security Management System (ISMS) under hensyntagen til gældende lovgivning og industristandarder, herunder:

- Databeskyttelsesforordningen (GDPR)
- Databeskyttelsesloven
- Offentlighedsloven
- Forvaltningsloven
- Net- og Informationssikkerhedsdirektivet (NIS2-loven)
- Lov om elektroniske og kommunikationsnet og -tjenester
- Sundhedsloven*
- Serviceloven*
- ISO/IEC 27000 – Ledelsessystemer for informationssikkerhed – Oversigt og ordliste
- ISO/IEC 27001 – Ledelsessystemer for informationssikkerhed – Krav
- ISO/IEC 27002 – Regelsæt for styring af informationssikkerhed
- ISO/IEC 27005 – Risikoledeelse i tilknytning til informationssikkerhed
- ISO/IEC 27701 – Ledelsessystem for beskyttelse af personoplysninger (privacy/PIMS)
- CIS18 – Et kontrolkatalog til tekniske og organisatoriske foranstaltninger
- ISO / IEC 62443 – Standard for cybersikkerhed i industrielle kontrolsystemer
- AI Forordning – EU-forordning til udvikling og anvendelse af kunstig intelligens
- CRA – EU-forordning til cybersikkerhedskrav til digitale produkter og software
- CER – EU-direktiv til krav til modtanddygtighed, både fysiske og digitale
- URIS – Dansk ramme for cybersikkerhed i samfundskritiske sektorer

*Eksempler på relevant særlovgivning. Listen er ikke udtømmende.

2.4 Plan for behandling af informationssikkerhedsrisici

Som risikoejer, skal Direktionen sikre, at de risici, som potentielt kan påvirke Regionens evne til at levere samfundskritiske tjenester, bliver adresseret og behandlet.

Risici skal identificeres, og foranstaltninger skal integreres, rapporteres og evalueres løbende. Der er udarbejdet en dokumenteret politik og proces for risikostyring som analyserer, evaluerer og håndterer identificerede risici.

2.5 Vurdering og forbedring af informationssikkerhed

Arbejdet med informationssikkerhed skal være effektivt, og det kræver løbende forbedringer. For at sikre dette, etablerer Informationssikkerhedsteamet et auditprogram som godkendes af Direktionen. I auditprogrammet fastsættes:

- hvilke kontroller der skal gennemføres
- frekvens og metode for audit
- ansvar for gennemførelse af audit, analyse, evaluering og rapportering.

Direktionen forelægges løbende auditresultater og handlingsplaner og på baggrund heraf træffer Direktionen beslutning om, hvilke foranstaltninger Regionen skal implementere, og hvornår beskyttelsen er tilstrækkelig.

2.6 Afvigelser og dispensationer

Informationssikkerhedsledelsen er ansvarlig for, at eventuelle afvigelser fra Politik for Informationssikkerhed registreres, vurderes og håndteres på en passende måde. Afvigelser kan identificeres gennem forespørgsler, audits og øvrige tilsynsaktiviteter.

3 Definition af begreber

I nedenstående tabel indskrives begreber, som vurderes at skulle forklares yderligere, for at målgruppen af dokumentet har en fuld forståelse for indholdet.

Begreb	Definition
ISMS	Information Security Management System (Ledelsessystem for Informationssikkerhed)
NIS2	Fastlægger foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU

4 Relaterede dokumenter

Retningslinjer, som understøtter Informationssikkerhedspolitikens formål skal sikre, at alle medarbejdere er bevidste om informationssikkerhed og ved, hvordan de arbejder sikkert i deres daglige arbejde.

Relaterede dokumenter kan ajourføres løbende uden godkendelse af ISL og Direktionen.

I nedenstående tabel indskrives interne retningsgivende dokumenter (f.eks. politikker og retningslinjer), hvis indhold har relation til indholdet i dette dokument.

Dokumenttitel	Identifikationsnummer
Politik for risikostyring	SBSYS: 1-31-82-39-24
Politik for leverandørstyring	Identifikationsnummer påføres efter endelig godkendelse
Procedure for leverandørstyring	Identifikationsnummer påføres efter endelig godkendelse
Politik for databackup og -gendannelse	SBSYS: 1-16-4-3153-24
Politik for kryptering	SBSYS: 1-16-00-622-24
Politik for Incident Management	SBSYS: 1-16-4-3158-24
IT Asset Politik	SBSYS: 1-16-4-3158-24
Politik for administration af konto og legitimationsoplysninger	SBSYS: 1-16-4-3154-24
Politik for passwords og pinkoder	SBSYS: 1-16-4-933-24
Politik for awareness	SBSYS: 1-16-4-2852-24
Politik for håndtering af auditlogs	SBSYS: 1-16-4-3130-24
Politik for revision og opfølgning	Identifikationsnummer påføres efter endelig godkendelse
Retningslinje for dokumenthåndtering	SBSYS: 1-16-00-617-24
Retningslinje for opbevaring og flytning af personoplysninger i fysisk form	Identifikationsnummer påføres efter endelig godkendelse
Politik for tilsyn med databehandlere	SBSYS: 1-16-4-2876-24

5 Godkendelse og revision

Politik for Informationssikkerhed og understøttende dokumenter skal løbende evalueres og revideres minimum én gang årligt. Ajourføring sker i forbindelse med større tekniske eller organisatoriske ændringer, ved væsentlige sikkerhedshændelser samt ved ændringer i Regionens forretningsmæssige mål eller i det aktuelle trusselsbillede.

Region Nordjylland forpligter sig til løbende forbedring af cyber- og informationssikkerheden baseret på risikovurderinger, auditresultater, hændelser og ændringer i trusselsbilledet.

Nye versioner af Politik for Informationssikkerhed skal sendes til høring hos relevante interessenter for at sikre, at den kan implementeres og ikke er i modstrid med lovgivning, interne regler eller andet. Politik for Informationssikkerhed godkendes af Direktionen.

Nye versioner er gyldige fra godkendelsesdatoen.

Politikken er, efter indstilling fra Informationssikkerhedsledelsen, godkendt af Direktionen den 07.04.2026

Gældende version af politikken er journaliseret i Region Nordjyllands ESDH-system 1-16-4-1549-24.

Dato	Version	Udarbejdet af	Godkendt af	Beskrivelse
25.10.2018	0.1	Deloitte		Dokument oprettet.
28.02.2019	0.2	Nicolai Jørgensen, Brian Stenskrøg Hansen	Direktionen 23.03.2019	Revideret version.
30.11.2022	1.0	Grethe Kristensen	ISL 05.12.2022	Der er foretaget mindre ændringer, som afspejler den nuværende organisering af informationssikkerhedsarbejdet. Afsnittet om 'udvidet i-sikkerhedsledelse' er fjernet og repræsentanter af ISL er præciseret. Afsnittet om 'involvering af Driftsledelsen' er fjernet. Der er tilføjet et afsnit om 'involvering af Direktionen'. Bilag omkring dokumentregister er fjernet. Bilag omkring prioriterede indsatser er opdateret.

12.02.2024	1.1	Jens Halgaard	Afventer ISL	<p>Bilag 1 opdateret således at det også afspejler den nuværende organisering af informationssikkerhedsområdet. Desuden er det tidligere bilag 2 med dokumentstruktur fjernet, da det ikke vurderes relevant længere.</p> <p>Det tidligere bilag 3 med sikkerhedsinitiativer bibeholdes og omdøbes til bilag 2, men er ikke opdateret i 2024. Emnerne afspejler mål for 2023.</p>
07.03.2024	1.1	Jens Halgaard	ISL	Version 1.1 godkendt af ISL
26.08.2025	1.2	Informationssikkerhed (MCO)	Jane Bak	Redaktionelle ændringer. Tilføjet til nye skabelon.
07.04.2026	2.0	Informationssikkerhed (MCO)	Direktionen	<p>Gennemgribende strukturel og sproglig opdatering.</p> <p>”Ramme for Informationssikkerhed” ændret til ”Politik for Informationssikkerhed”.</p> <p>Øget fokus på risikobaseret tilgang og aktiv risikostyring.</p> <p>Tydelig forankring af Direktionen som risikoejer.</p> <p>Sikkerhedsmål og foranstaltninger prioriteres risikobaseret.</p> <p>Tydeligere kobling til Regionens samfundskritiske funktion og aktuelle trusselsbilleder.</p> <p>Lovgivning og standarder er opdateret og udvidet.</p> <p>Governance- og ledelsesmæssig forankring præciseret og styrket.</p> <p>Opdatering og strukturering af relaterede dokumenter.</p>

Region Nordjylland
Cyber- og Informationssikkerhed
Hadsundvej 190
9000 Aalborg

april 2026