Ramme for informations-sikkerhed

REGION NORDJYLLAND
– i gode hænder

INDHOLD

1 Indledning

I denne ramme fastsættes ambitionsniveauet for informationssikkerhed i Region Nordjylland, og der redegøres for prioriteterne i informationssikkerhedsarbejdet. Rammen indeholder de overordnede sikkerhedsmål, og danner grundlaget for driftsmodellen for informationssikkerhed (operating model) (bilag 1).

Retningslinjer, som understøtter rammens hovedmål skal sikre, at alle medarbejdere arbejder med Informationssikkerhed og relaterer til informationssikkerhed i deres daglige arbejde. Region Nordjylland kræver et højt niveau af sikkerhed. Ikke kun for at overholde lovkrav og reguleringer, men også for at yde en sikker service til borgere og medarbejdere. Informationssikkerhed er højt prioriteret, og det skal være en naturlig del af de øvrige aktiviteter.

2 Målgruppe

Målgruppen for Region Nordjyllands ramme for informationssikkerhed er Regionsrådet, Region Nordjyllands direktion, samt Informationssikkerhedsorganisationen, herunder de interne stabe og kontorer (leverandører), som bidrager til arbejdet med informationssikkerhed.

3 Roller og ansvar

I Region Nordjylland er det vigtigt med en korrekt identificering af nøgleroller, som er ansvarlige for informationssikkerheden i regionen. Ansvaret for informationssikkerheden i Region Nordjylland er entydigt forankret i regionens ledelse. Dette stadfæster et klart risikoejerskab samt sikrer, at det overordnede sikkerhedsniveau i regionen afstemmes på tværs af virksomheder og i forhold til den samlede økonomiske ramme.

Region Nordjylland har etableret en informationssikkerhedsorganisation, som har til formål at skabe et ledelsesforankret grundlag for, at kunne drive regionens kerneområder med en balanceret risikoappetit, samt træffe rette risikominimerende tiltag rettidigt.

Dette dokument ejes af Region Nordjyllands direktion. Implementering og efterlevelse sker i et samarbejde mellem IT-direktøren, Informationssikkerhedsledelsen og organisationen.
I bilag 1, operating model, ses en liste over rollefordelingen.

Nedenfor følger en skitse over Region Nordjyllands sikkerhedsorganisation samt en beskrivelse af de enkelte led:

Regionsrådet
Regionsrådet er den øverste besluttende myndighed i informationssikkerhedsarbejdet. Regionsrådet træffer beslutning om sikkerhedsniveauet gennem den overordnede sikkerhedspolitik, og sørger for, at der stilles en afstemt økonomisk ramme til rådighed for informationssikkerhedsarbejdet.

Direktionen
Direktionen har det overordnede ansvar for at uddelegeringen af informationssikkerhedsopgaver i regionen, er i overensstemmelse med de rammer Regionsrådet har besluttet.

Direktionen skal sikre, at der er etableret en række målrettede politikker, som opfylder gældende informationssikkerhedskrav, at der årligt sker en opfølgning på, om politikkerne overholdes, samt støtte op om forbedringer efter behov.

Ejer og underskriver af dette dokument ' Ramme for informationssikkerhed' er dermed Direktionen.

IT Direktøren
I Region Nordjylland binder IT-direktøren Informationssikkerhedsledelsen og Direktionen sammen, samt sikrer et fornuftigt og praktisk beslutningsflow, så der kan eksekveres i et passende tempo.

Informationssikkerhedsledelsen (ISL)
ISL består af IT-direktøren samt ledelsesrepræsentanter fra Jura, IT og Informationssikkerhed. ISL varetager og koordinerer den daglige ledelse af informationssikkerhedsarbejdet på taktisk plan og inddrages hvor der skal træffes hurtige beslutninger.

Databeskyttelsesrådgiver DPO
Regionens Databeskyttelsesrådgiver (DPO) har en rådgivende funktion i arbejdet med informationssikkerhed. DPO´ens funktion består i at rådgive, vejlede og overvåge at organisationen efterlever regler om databeskyttelse. DPO´en er kontaktled til Datatilsynet og samarbejder med Datatilsynet på vegne af Region Nordjylland.

Informationssikkerhedsteamet
Teamet består af jurister, IT-sikkerhedskonsulenter, databeskyttelsesmanagere samt informationssikkerhedskonsulenter. Teamet varetager den daglige drift af informationssikkerhedsarbejdet. Teamets opgave er at understøtte og drive informationssikkerhedsarbejdet på tværs af hele organisationen. Teamet udarbejder blandt andet politikker, retningslinjer og instrukser og foretager løbende risikovurderinger.

Informationssikkerhedsambassadører
For at fremme og fastholde budskabet om at passe bedst muligt på borgernes oplysninger, har regionen udpeget ambassadører i alle sektorer og enheder. Ambassadørerne vil i samarbejde med databeskyttelsesrådgiveren sikre, at viden om en god og sikker håndtering af borgernes oplysninger når ud i alle hjørner af organisationen.

Beslutningsproces
Sager af informationssikkerhedsmæssig karakter behandles i første omgang af Informationssikkerhedsledelsen (ISL). Sagerne kan i visse tilfælde have en karakter, som kræver en behandling i et eller flere andre fora i regionen. Det er f.eks når sager omfatter hele regionen og som omhandler ledelsesgrundlag, det samlede budget, kommunikationsstrategi, økonomi og IT-dækning.

Direktionen
I sager der berører hele regionen eller hvor der er ønske om ledelsesmæssig godkendelse på højere niveau vil sagen blive ført videre til Direktionen. Sager, 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. Alle ledere er derudover ansvarlige for at inddrage MED-udvalg på de relevante niveauer.

4 Sikkerhedsmål og -målsætninger

Region Nordjyllands strategiske målsætning for informationssikkerhedsområdet er at have et højt informationssikkerhedsniveau under hensyntagen til en effektiv udførelse af regionens primære opgaver og den økonomiske ramme, som Region Nordjylland er underlagt. Opnåelse af det ønskede informationssikkerhedsniveau sker via en klar ledelsesforankring, samt en forretningsorienteret og risikobaseret tilgang til sikkerhed. Denne målsætning realiseres ved:

- At have en klart defineret informationssikkerhedsorganisation, så det bliver tydeligt, hvor informationssikkerhed er forankret, hvem der har den daglige ledelse, samt hvordan samarbejdet med resten af organisationen styres, forvaltes og organiseres-
- At benytte en ensartet og generisk metode til arbejdet med informationssikkerhed, som skal anvendes i relation til informationssikkerhed på tværs af organisationen. Metoden er beskrevet i bilag 1.
- At sikre ensartet og kontinuerlig rapportering på risikoappetit, igangværende initiativer såvel som compliance-efterlevelse.

informationssikkerhed indebærer beskyttelse af oplysninger mod utilsigtede hændelser. Arbejdet med informationssikkerhed tager udgangspunkt i de værdier, som informationssikkerhedsorganisationen arbejder efter.

Værdierne skal sikre:

- Fortrolighed – dvs. at kun rette personer har adgang til rette oplysninger.
- Integritet – dvs. at oplysningerne er korrekte, komplette og sikret mod uautoriserede ændringer.
- Tilgængelighed – dvs. at oplysningerne er tilgængelige og brugbare, når der er behov for det.

Centrale mål

For at nå Region Nordjyllands strategiske målsætning arbejdes der løbende med modning af en række sikkerhedsforanstaltninger. Sikkerhedsforanstaltningerne prioriteres for en valgperiode og justeres én gang årligt. De sikkerhedsforanstaltningerne, der er prioriteret i den kommende periode findes i bilag 2.

5 Lovgivning og standarder

Region Nordjylland vil oprette et ISMS under hensyntagen til følgende lovgivningsmæssige krav og industristandarder:

- Databeskyttelsesforordningen (GDPR)
- Databeskyttelsesloven
- Regionsloven
- Offentlighedsloven
- Forvaltningsloven
- Arkivloven

- Net- og informationssikkerhed (NIS-loven)
- Lov om elektroniske kommunikationsnet og –tjenester
- Sundhedsloven*
- Journalføringsbekendtgørelsen*
- 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 - Risikoledelse i tilknytning til informationssikkerhed

* Eksempler på relevant særlovgivning. Listen er ikke udtømmende.

6 Plan for behandling af informationssikkerhedsricisi

Som risikoejer skal Direktionen sikre, at de problemstillinger og risici, som potentielt kan påvirke regionens evne til at nå de ønskede mål for informationssikkerhed bliver adresseret. Risici skal identificeres og foranstaltninger skal integreres og evalueres løbende.
Konkret skal der udarbejdes en dokumenteret proces for risikovurdering, som identificerer, analyserer og evaluerer de risici, som regionen står over for.
Der skal udarbejdes en dokumenteret proces for behandling af risici. Herunder ligger, at der skal udarbejdes en plan for behandling af identificerede risici.
I planen fastsættes

- hvem der ejer de pågældende risici
- hvilke kontroller, der er nødvendige at indføre for at imødegå risici
- passende behandlingsmuligheder for risici
- hvilke ressourcer der er nødvendige
- en tidsplan for implementering
- en metode til evaluering af resultater og
- risikoappetit i forhold til en eventuel tilbageværende risiko.

Risikoejer godkender plan og restrisiko.

7 Vurdering og forbedring af informationssikkerhed

Arbejdet med Informationssikkerhed skal være effektivt og det kræver løbende forbedringer. For at sikre dette, er det skal direktionens ansvar, at der udvikles et dokumenteret program for udførelse af audit i organisationen. I auditprogrammet fastsættes

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

Direktionen beslutter på baggrund af rapportering hvilke forbedringer der skal iværksættes.

8 Afvigelser og dispensationer

Informationssikkerhedsledelsen er ansvarlig for at afvigelser fra rammen, dokumenteres, vurderes og i nødvendig grad håndteres. Afvigelser fra rammen identificeres ved forespørgsler, audit eller tilsyn.
Risikoen ved afvigelse fra rammen skal vurderes og forelægges for Direktionen, som træffer beslutning om hvorvidt der kan dispenseres fra afvigelsen. Beslutning om dispensation skal dokumenteres.
Hvis risikoen overstiger regionens risikovillighed, bør der ikke dispenseres fra afvigelsen.

Hvis der ikke kan dispenseres, skal afhjælpning af afvigelsens risiko planlægges.

9 Vedligeholdelse

Rammen og dens understøttende dokumenter skal løbende evalueres. Det kan f.eks. ske ved større tekniske eller organisatoriske forandringer samt efter væsentlige sikkerhedshændelser forårsaget af afvigelser fra rammen. Rammen skal dog som minimum evalueres årligt.
Alle nye revisioner af rammen sendes til høring hos rammens målgrupper for at sikre, at den kan implementeres og ikke er i modstrid med lovgivning, interne regler eller andet. Herefter godkendes rammen af Direktionen. Nye versioner af rammen er gyldig fra godkendelsesdatoen.

10 Versionshistorik

Dato	Version	Udarbejdet af	Godkendt af	Beskrivelse
25-10-2018	0.1	Deloitte		Dokument oprettet.
28-02-2019	0.2	Nicolai Jørgensen, Brian Stenskrog Hansen	Direktionen 23. apr. 2019	Revideret version
30-11-2022	1.0	Grethe Kristensen	ISL 5. dec. 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	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. Det tidligere bilag 3 med sikkerhedsinitiativer bibeholdes og omdøbes til bilag 2, men er ikke opdateret i 2024. Emnerne afspejler mål for 2023.
07-03-2024	1.1	Jens Halgaard	ISL	Version 1.1 er godkendt af ISL

Ramme for informationssikkerhed

Informationssikkerhed
Niels Bohrs Vej 30
9220 Aalborg Øst

2. december 2022

REGION NORDJYLLAND
– i gode hænder