



Informationssikkerhedspolitik

Maj 2009



REGION NORDJYLLAND

Informationssikkerhedspolitik for Region Nordjylland

Informationssikkerhedspolitikken er gældende for hele Regionen. Den er tilvejebragt af I-sikkerhedsudvalget og tiltrådt af den Udvidede direktion, Forretningsudvalget og Regionsrådet.

Den gældende version ligger på Region Nordjyllands hjemmeside. Hvis man udskriver eller kopierer en udgave af Informationssikkerhedspolitikken til senere brug, skal man sikre sig, at det er den gældende version, der ageres efter.

Det eneste helt sikre i universet er, at intet er helt sikkert...

Begreber

Informationssikkerhed

Informationssikkerheden inddeles i tre overordnede fokusområder:

Tilgængelighed – Sikring af, at det er muligt at foretage den nødvendige informationsbehandling, når der er behov for det.

Korrekthed – Sikring af, at al information er korrekt, og at informationsbehandlingen ikke forringer indholdet.

Fortrolighed – Sikring af, at ethvert specifikt sæt af information kun kan behandles og kommunikeres af dem, som er berettiget og har fået tildelt adgang til det.

Informationsaktiver

Informationssikkerhed er rettet mod håndteringen og de nødvendige sikringsforanstaltninger knyttet til de tre typer af informationsaktiver: information, it-systemer og teknik.

- Information

Information er oplysninger, der fysisk er repræsenteret som data. Disse kan være på elektronisk form eller på f.eks. bånd og papir. Information til alle formål i regionen er omfattet.

Information klassificeres ud fra indhold i kategorierne:

Almen – information, som stilles til rådighed for offentligheden på alle kanaler og medier med offentlig adgang.

Intern – information, som ikke i sig selv har en nytteværdi eller giver mening for offentligheden. Det kan være materiale som f.eks. er belagt med copyright, arbejdsdokumentation ved udviklingsaktiviteter, interne notater samt detaljerede beskrivelser af sikringsforanstaltninger.

Følsom – personhenførbare information. Følsomme oplysninger om menneskers rent private forhold. Det drejer sig om oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbreds- og seksuelle forhold.

Andre typer af oplysninger om rent private forhold anses også for at være følsomme. Det drejer sig om oplysninger om strafbare forhold, væsentlige sociale problemer og lignende følsomme privatlivsoplysninger, f.eks. om interne familieforhold.

Fortrolig – information som kun er beregnet til behandling af en begrænset og fastlagt persongruppe. I denne kategori kan der være både personhenførbare og andet indhold.

- It-systemer

Systemer er funktionelt afgrænsede programkomplekser. Systemer kan være integrerede med andre systemer via lokalt netværk eller internettet.

Systemer kan være i drift internt i Region Nordjylland eller hos eksterne serviceleverandører og samarbejdspartnere.

Systemer kan inddeles i kategorier ud fra hvor kritiske de er for brugerne samt udbredelsen i regionen.

- Teknik

Teknik er komponenterne i den tekniske infrastruktur i form af fysisk databehandlingsudstyr som f.eks. pc'er, servere og mobile enheder samt kommunikationsudstyr og netværk. Datalagre og mobile databærende medier samt data- og kommunikationsdelen af medicoteknisk apparatur, der er koblet til det fælles netværk, og som behandler patientdata, er også en del af denne gruppe.

1 Formål

Informationssikkerhedspolitikken er den overordnede ramme for håndtering af informationssikkerhed - herefter benævnt i-sikkerhed i Region Nordjylland. For at regionen kan levere ydelser af høj kvalitet til sine borgere og samarbejdspartnere skal et effektivt værn mod i-sikkerhedsmæssige trusler til stadighed udvikles og vedligeholdes. Dette bidrager til, at regionens forretningsområder kan fungere, og at Region Nordjyllands borgere, virksomheder, samarbejdspartnere og ansatte kan være trygge ved regionens behandling af information.

Politikken beskriver styrende principper og mål for i-sikkerhedsindsatsen. Udgangspunktet er Region Nordjyllands strategiske mål, hvor det nødvendige sikkerhedsniveau er en afgørende faktor for, at regionen kan fremstå som en troværdig myndighed.

2 Anvendelse og målgruppe

I-sikkerhedspolitikken skal udmøntes i et sæt retningslinjer, der detaljeret fastlægger rammerne for forretningsgange og sikringsforanstaltninger på i-sikkerhedsområdet.

Til styring af den konkrete adfærd og udformning af sikringsforanstaltninger skal der udarbejdes vejledninger og detaljerede instrukser.

Målgruppen for i-sikkerhedspolitikken er alle, der skal udmønte den i retningslinjer og instrukser for indretning og håndtering af i-sikkerheden.

I-sikkerhedspolitikken skal offentliggøres på Region Nordjyllands hjemmeside. Retningslinjer, instrukser og vejledninger er til intern brug.

3 Omfang

Politikken gælder for:

- alle informationsaktiver inden for grupperne: information, systemer og teknik
- al intern informationsbehandling og den informationsbehandling, som foretages for regionen, hos samarbejdspartnere og leverandører
- alle typer af information, ligegyldigt i hvilken form de behandles, opbevares og kommunikeres. Dette gælder for information, som regionen enten selv er ansvarlig for, eller som stammer fra samarbejdspartnere
- alle ansatte, både fastansatte og personer, som midlertidigt udfører arbejdsopgaver for Region Nordjylland
- ansatte hos samarbejdspartnere og leverandører med adgang til regionens informationsaktiver.

4 Ansvar

Det overordnede ansvar for i-sikkerheden i Region Nordjylland påhviler den Udvidede direktion. Ansvarret varetages gennem den etablerede i-sikkerhedsorganisation.

Alle med ledelsesansvar i regionen har et aktivt og udførende ansvar for, at i-sikkerhedspolitikken overholdes i forbindelse med de daglige processer og arbejdsopgaver. Ledere skal sikre, at

ansatte kun har de absolut nødvendige adgange til at anvende og administrere de relevante informationsaktiver ud fra principperne behov og funktionsadskillelse.

Det er ledernes ansvar, at ansatte i Region Nordjylland har det nødvendige kendskab til og forståelse for regionens i-sikkerhedsregler. Endelig er det ledernes ansvar at sikre sig, at de ansatte efterlever reglerne, og at informere om konsekvenserne af bevidste brud på i-sikkerheden.

Det er en afdelings ledelse, som har ansvar for, at der er de nødvendige informationsaktiver til understøttelse af afdelingens arbejdsopgaver. Ligeledes er afdelingsledelsen ansvarlig for, at der er indrettet et beredskab, når teknik eller systemer svigter, således at den nødvendige og aftalte informationsbehandling er umulig.

Nogle af regionens informationsaktiver kan være fysisk placeret i eller serviceret af andre organisationer. Dette ændrer ikke regionens grundlæggende ansvar, som varetages af rollerne tilknyttet disse aktiver.

5 Mål

Aktiviteter og håndtering af i-sikkerheden i Region Nordjylland skal indrettes, så følgende mål tilfredsstilles:

Generelt:

- Håndtering af I-sikkerhed skal integreres i alle forretningsgange, der involverer informationsbehandling.
- I-sikkerhed skal vurderes og indarbejdes i alle Region Nordjyllands udviklingsaktiviteter, som resulterer i ændringer i bestående eller helt ny informationsbehandling.
- Ingen sikringsforanstaltninger må forringe patientsikkerheden.
- I-sikkerheden skal håndteres og sikringsforanstaltninger indrettes, så der tages hensyn til de ansattes sikkerhed og rettigheder.
- Medarbejderne skal orienteres om væsentlige hændelser eller ændringer, der har indflydelse på i-sikkerheden.
- Såfremt der indtræffer en alvorlig i-sikkerhedshændelse, skal den berørte ledelse foretage en vurdering af årsagen til den givne hændelse og en vurdering af, om dette giver anledning til nødvendige i-sikkerhedsmæssige tiltag.
- Alle i-sikkerhedshændelser skal registreres for at kunne vurdere, om der er ændringer i det trusselsbillede, som benyttes i risikovurderinger.
- Kompetencer om i-sikkerhed skal ajourføres og fastholdes gennem videndeling og andre aktiviteter hos alle, der beskæftiger sig med indretning og overvågning af i-sikkerheden.

Informationsaktiver:

- Alle informationsaktiver skal registreres.
- Alle informationsaktiver skal klassificeres ud fra:
 - hvor kritiske de er for udførelsen af arbejdsopgaver og for patientsikkerheden
 - indhold

- deres betydning for Region Nordjylland
 - krav fra lovgivning
 - deres relation til eller direkte afhængighed af andre informationsaktiver.
- Alle væsentlige informationsaktiver skal risikovurderes med jævne mellemrum. Risikovurderingen skal fastlægge det ønskede i-sikkerhedsniveau med udgangspunkt i aktivets brug i forhold til tilgængelighed, korrekthed og fortrolighed. Der skal der foretages fornyede risikovurderinger ved:
 - væsentlige ændringer i trusselsbilledet
 - større organisatoriske forandringer i regionen
 - væsentlige forandringer i it-arkitekturen
 - ved indgåelse af eksterne serviceaftaler
 - ved outsourcing af driftsopgaver.
 - Ejerskabet til hvert informationsaktiv skal fastlægges. Ejere skal løbende udarbejde aktuelle risiko- og konsekvensvurderinger af deres informationsaktiver, og bevirke at de pågældende aktiver er sikret i forhold til trusselsbilledet, og hvor kritiske aktiverne er.
 - For informationsaktiver, som teknisk og driftsmæssigt håndteres af en leverandør af drift og serviceydelser, skal ejeren af aktivet indgå en aftale i form af en kontrakt eller service niveauaftale - SLA - med leverandøren om betingelserne for håndteringen. I aftalen skal de specifikke i-sikkerhedsmæssige krav indgå. Der skelnes ikke her mellem interne eller eksterne leverandører. Aftaler skal omhandle alle faser af informationsaktivets livscyklus.
 - Der kan hos en leverandør af drift og serviceydelser – såvel internt som eksternt - være ansatte, som har omfattende adgang til at se information og mulighed for at slette denne. Region Nordjylland forbeholder sig ret til om fornødent at sikkerhedsgodkende disse ansatte ud fra en konkret risikovurdering.

Beredskab:

- Beredskabsstyring skal udføres i en kontinuerlig proces, som sikrer, at regionens forretningsområder kan fungere ved manglende tilgængelighed og tab af informationsaktiver, når der er beredskabssituationer forårsaget af nedbrud, i-sikkerhedshændelser eller katastrofer.
- Der skal foretages en nøjagtig kortlægning af samtlige afdelingers afhængighed af informationsbehandling ved brug af information, systemer og teknik. Ved denne kortlægning skal informationsaktivernes vigtighed prioriteres ud fra en afdelings følsomhed i situationer hvor systemer og teknik svigter, så den nødvendige og aftalte anvendelse er umulig.
- Der skal udarbejdes planer for kommunikation samt forberedelse, vedligeholdelse og reetablering af forretningsaktiviteter før, under og efter en beredskabssituation.
- Beredskabsplaner skal etableres, så der er sammenhæng med andre krav og beredskabsplaner vedrørende drift, personale, forsyning, materiel, transport og øvrige faciliteter. Koordineringen udøves af den instans, som har det overordnede ansvar for beredskabsplanlægningen i Region Nordjylland.
- Beredskabsplanerne skal afprøves og om nødvendigt ajourføres løbende, dog minimum en gang om året.

6 Sikkerhedsniveau

Regionen er forpligtet til at etablere sikringsforanstaltninger og håndtere i-sikkerheden ud fra:

- love og afledte forskrifter
- obligatoriske standarder
- krav fra samarbejdspartnere
- internt vedtagne regler og valgte standarder.

Konkrete sikringsforanstaltninger skal etableres og dimensioneres ud fra risikovurderinger. Med udgangspunkt i risikovurderingen sammenholdt med de forretningsmæssige prioriteringer af informationsaktiverne fastlægger og prioriterer ledelsen de nødvendige sikringsforanstaltninger til opretholdelse af det for regionen nødvendige og tilstrækkelige i-sikkerhedsniveau.

Som reference for det basale sikkerhedsniveau benytter regionen Dansk Standard for informationssikkerhed DS484:2005.

7 I-sikkerhedsorganisation

Den Udvidede direktion har nedsat regionens I-sikkerhedsudvalg og besluttet principperne for sammensætningen. Udvalget er normgivende og fastsætter på grundlag af i-sikkerhedspolitikken de principper og aktiviteter, der skal sikre målopfyldelsen.

Udvalget behandler alle i-sikkerhedsspørgsmål af principiel karakter. For hvert spørgsmål vurderes, om der er særlige hensyn, om spørgsmålet skal behandles på et andet niveau i organisationen, og om andre relevante fora skal involveres.

I-sikkerhedsudvalget fastsætter selv forretningsgangen og varetager opgaverne kontinuerligt. Udvalgets aktiviteter skal som udgangspunkt omfatte:

- At der igangsættes initiativer, der løbende skal sikre, at Region Nordjylland har et for regionen acceptabelt i-sikkerhedsniveau.
- At sikre, at der gennemføres en løbende kontrol af om i-sikkerhedspolitikens mål er nået.
- At der indsamles oplysninger om i-sikkerhedshændelser og tilstande med et uacceptabelt højt risikoniveau.
- At der løbende på baggrund af de udførte kontroller og de indsamlede oplysninger igangsættes aktiviteter til ajourføring af i-sikkerheden, således at i-sikkerhedsniveauet svarer til det aktuelle trusselsbillede.
- At i-sikkerheden integreres i alle relevante forretningsgange, driftsopgaver og udviklingsaktiviteter.
- At iværksætte aktiviteter, som udbygger og fastholder de ansattes bevidsthed om i-sikkerhed.
- At der årligt foretages afrapportering af i-sikkerhedsniveauet til den Udvidede direktion.

Al håndtering af i-sikkerhed i Region Nordjylland skal koordineres centralt. Til at varetage koordineringsaktiviteterne er der ansat en I-sikkerhedskoordinator. Ud over koordineringen yder vedkommende konsulentbistand og deltager i løsning af konkrete opgaver på i-sikkerhedsområdet. Endelig deltager koordinatoren i aktiviteter, til styrkelse af i-sikkerheden nationalt og i regionerne. Koordinatoren er sekretær for I-sikkerhedsudvalget.

8 Sikkerhedsbevidsthed

Alle ansatte i Region Nordjylland skal i deres løsning af de daglige opgaver bidrage til at beskytte information mod uautoriseret adgang, ukorrekt ændring og ødelæggelse. En høj sikkerhedsbevidsthed er derfor forudsætningen for, at de ansatte aktivt kan medvirke til at håndtere i-sikkerheden.

Regionens ansatte skal kende principperne for i-sikkerhed. De skal have kendskab til hvilke instrukser og vejledninger, der er aktuelle i en bestemt sammenhæng. Der skal derfor hos hver enkelt ansat være en forståelse for, at der er et behov for at efterleve reglerne for i-sikkerhed.

9 Brud på i-sikkerheden

Såfremt en ansat opdager potentielt alvorlige trusler mod i-sikkerheden eller brud på denne, skal dette straks rapporteres til I-sikkerhedskoordinatoren og nærmeste leder. Hvis det skønnes, at det observerede er så alvorligt, at der skal foretages en omgående teknisk indgriben, kontaktes It-afdelingens ServiceDesk.

Hvis ansatte bevidst bryder i-sikkerheden, vil der blive anvendt disciplinære forholdsregler i overensstemmelse med gældende regler og personalepolitik i Region Nordjylland.

10 Kontrol

Der skal periodisk, dog mindst en gang årligt, udføres kontroller til verifikation af kvaliteten og relevansen af de gennemførte sikringsforanstaltninger. Kontrollerne skal også bruges til at registrere i hvilken udstrækning håndteringen af i-sikkerheden opfylder kravene.

Nogle kontroller foretages af den eksterne revision efter aftale med Region Nordjylland.

Kontrollerne vedrører alle områder, underlagt I-sikkerhedspolitikken, herunder også de områder, der måtte være outsourcet. Kontrollerne tilrettelægges, så de omfatter selv-kontrol af overholdelse af instrukser og vejledninger samt central opfølgning. Udgangspunktet for kontrol af basisniveauet er DS484:2005.

Resultatet af foretagne kontroller indgår i den årlige rapport til den Udvidede direktion.

11 Dispensation

Hvis der opstår tilstande, hvor der er væsentlige forretningsmæssige interesser, særlige krav til patientsikkerhed eller væsentlige samfundsmæssige interesser, kan der ansøges om midlertidig dispensation fra regler, instrukser og vejledninger baseret på I-sikkerhedspolitikken.

Ansøgninger forelægges I-sikkerhedskoordinatoren, som sammen med I-sikkerhedsudvalget vurderer ansøgningen. Afhængig af det ansøgte omfang og ændring af risikobilledet kan ansøgningen afgøres af enten I-sikkerhedsudvalget eller af den Udvidede direktion.

12 Ajourføring

I-sikkerhedspolitikken skal på grundlag af den løbende overvågning og rapportering revideres og om nødvendigt ajourføres og godkendes som udgangspunkt én gang om året, eller hvis der er markante ændringer i forudsætningerne for informationsbehandlingen. I-sikkerhedsudvalget har denne opgave.

INFORMATIONSSIKKERHEDSPOLITIK

Maj 2009

Udgivet af
I-sikkerhedsudvalget.

Regionssekretariatet
Region Nordjylland
Niels Bohrs Vej 30
9220 Aalborg Ø
9635 1000

www.rn.dk

