Region Syddanmark

Dato: 21. februar 2021

Notat

Mål for arbejdet med informationssikkerhed 2021

Det fremgår af Region Syddanmarks Digitaliseringsstrategi, at borgerne, patienterne og medarbejderne i Region Syddanmark skal have tillid til, at regionen behandler og opbevarer oplysninger og data forsvarligt.

For at sikre dette mål er det er afgørende, at Region Syddanmark løbende konsoliderer arbejdet med informationssikkerhed. Dette for at sikre, at regionen behandler og håndterer borgeres, patienters og medarbejderes data forsvarligt. Desuden skal sikres, at regionens vitale it-systemer og it-infrastruktur er bedst muligt rustet til at modstå angreb og nedbrud.

It-sikkerhed består af såvel informationssikkerhed som af cybersikkerhed.

Regionsrådet vedtog på mødet den 16. dec. 2019 strategien for Cyber -og informationssikkerhed.

Cyber- og informationsikkerhedsstrategien har primært fokus på cybersikkerhed og allokerer 30 mio. kr. til at styrke Region Syddanmarks evne til at forudse, forebygge, opdage og håndtere sikkerhedshændelser. Gennem målrettede projekter bidrager strategien til at løfte sikkerhedsniveauet på centrale områder som netværkssikkerhed, beredskabsplaner, brugerrettighedsstyring og meget mere. Samtidig bidrager strategien til, at digitale trusler, risikovurderinger og hændelser bliver delt på tværs i sundhedssektoren mellem regioner, kommuner og øvrige aktører. Hvor strategien primært adresserer mål for cybersikkerhed, omhandler nærværende notat mål på informationssikkerhedsområdet.

Informationssikkerhed er en bred betegnelse for de samlede foranstaltninger til at sikre informationers fortrolighed, integritet og tilgængelighed.

Området omfatter helt overordnet den organisatoriske opbygning af regionens arbejde med informationssikkerhed, aktiviteter omkring oplysning og påvirkning af personalets adfærd, processer for personalets behandling af data, styring af leverandører af digitale ydelser samt fysiske sikringsforanstaltninger. Informationssikkerhed hviler i udpræget omfang på lovgivning i forhold til GDPR og NIS, samt ISO 27001-standarderne.

På baggrund heraf har Region Syddanmark udarbejdet 15 overordnede retningslinjer. Retningslinjerne beskriver blandt andet krav til og rammer for informationssikkerhed inden for en lang række centrale områder, herunder sikker håndtering og opbevaring af data samt sikring af regionens it-systemer. Retningslinjerne bliver regelmæssigt opdateret for at imødekomme aktuelle behov og lovkrav.

Retningslinjerne er styrende på informationssikkerhedsarbejdet i regionen.

Det konkrete informationssikkerhedsarbejde handler langt overvejende om praktisk anvendelse af de 15 retningslinjer. Dette er en kompleks opgave. Regionen har mere end 800 it-systemer af forskellig karakter. En række af disse dækker hele regionen (f.eks. EPJ, Blodbank, laboratoriesystemer). Andre er forankret på de enkelte sygehuse og enheder (f.eks. en række systemer til håndtering af fysisk adgang (adgangskort/døråbning), og endelig er der er del systemer, der er forankret på en enkelt afdeling eller i et afgrænset forskermiljø. Det systemmæssige ansvar for de forskellige it-systemer er

udbredt til alle enheder i regionen, som dermed hver især har et særligt ansvar for at sikre et informationssikkerhedsmæssigt forsvarligt niveau i anvendelsen af det enkelte system.

Informationssikkerhed handler ud over it-tekniske forhold også om brugeradfæd. Regionen har mere end 25.000 ansatte. Så det er en væsentlig ledelsesopgave at sikre, at alle medarbejdere har tilstrækkelig viden om og indsigt i it-sikkerhed til at kunne handle i overensstemmelse med regionens retningslinjer og instrukser.

Regionsrådet forelægges årligt en status på informationssikkerhedsarbejdet. Den årlige status er bygget op omkring de 15 retningslinjer.

Det er overordnet vurderingen, at informationssikkerhedsarbejdet er i god gænge, og at regionen er kommet langt i forhold til at anvende de vedtagne retningslinjer

Som det fremgår af de årlige afrapporteringer er alle retningslinjer ikke implementeret i bund. Dette arbejde er et vedvarende fokus. Både fordi det i sig selv er nødvendigt at fasholde et organisatorisk fokus, og fordi retningslinjerne løbende revideres i takt med, at trusselsbilledet og centrale forventninger ændrer sig.

Med henblik på at styrke og fokusere det igangværende informationssikkerhedsarbejde – særligt i forhold til de 15 retningslinjer - foreslås i nærværende dokument en række konkrete målsætninger for informationssikkerhedsarbejdet i 2021.

Forslaget til målsætninger hviler på en inddragende proces omkring årsskiftet 2020/21, hvor erfaringer hos regionens sygehuse, øvrige enheder og stabe, bidrag fra regionens databeskyttelsesrådgiver samt erfaringer fra konkrete hændelser, datatilsynsmyndighederne m.fl., er bragt i spil.

Der foreslås en række konkrete mål og indsatser inden for følgende fire temaer:

1) **Risikobaseret tilgang**
2) **Bruger- og adgangsrettigheder**
3) **Databehandler aftaler**
4) **Oplysning, uddannelse og medarbejdernes adfærd (awareness)**

Risikobaseret tilgang

Retningslinje 11.01 (Risikostyring) beskriver rammerne for identifikation, analyse og håndtering af risici i Region Syddanmark. Den risikobaserede tilgang er hjørnestenen i arbejdet med Informationssikkerhed, hvorfor det er vigtigt, at medarbejderne tænker det ind i deres daglige arbejde.

Risikostyring tager udgangspunkt i en endelig liste af trusler, som er identificeret centralt fra. Der skal for prioriterede systemer tages stilling til, hvilke konsekvenser et brud på sikkerheden kan få for Region Syddanmark. Listen af trusler genvurderes årligt.

Risikovurderingen benyttes således til at afklare behovet for løbende kontrol og tilsyn med det enkelte it-system.

I 2020 er der foretaget risikovurdering af i alt 59 systemer, hvor IT-Styring og Informationssikkerhed har bistået processen. I 2019 blev 24 systemer risikovurderet. Herudover er der foretaget risikovurdering på et ganske betydende antal systemer på de enkelte enheder. Det vurderes uhensigtsmæssigt, at der ikke er et samlet overblik over hvilke systemer, der er risikovurderede. Det

foreslås derfor, at der i 2021 etableres et samlet overblik herover. Med udgangspunkt i dette overblik foreslås endvidere, at der udarbejdes en samlet plan for risikovurderinger og en samlet plan for opfølgning.

Risikovurdering vil også fremover foregå ved de systemansvarlige med bistand fra regionens fælles støttefunktion: IT- styring og informationssikkerhed. Retningslinjen for risikostyring udgør en fælles ramme herfor. Det anbefales, at målarbejdet suppleres med yderligere detaljeret præcisering af roller og ansvarsfordeling på tværs af regionen.

Et væsentligt element i arbejdet med risikovurderinger er – foruden den fælles forståelse – fælles skabeloner. De hidtidige skabeloner (fra 2019) er derfor opdateret til et nyt fælles værktøj, der ibrugtages i 2021. Det foreslås, at der i 2021 sikres, at risikovurderinger sker ved anvendelse af det nye opdaterede værktøj. Forudsætningen herfor er selvsagt kendskab til værktøjet, hvorfor der tillige opstilles et mål om uddannelse/træning af nøglemedarbejdere i brugen af det nye fælles værktøj.

Opsummeret anbefales følgende mål for temaet risikobaseret tilgang for 2021:

1. Etablering af fælles overblik over risikovurderinger
2. Plan for fremadrettede risikovurderinger og opfølgninger
3. Præcisering af rolle- og ansvarsfordeling i forhold til risici på tværs af regionen
4. Anvendelse af nyt fælles værktøj for risikovurderinger
5. Uddannelse og træning i brug af nyt fælles værktøj for risikovurderinger

Bruger- og adgangsrettigheder

Retningslinje 11.04 (Brugeradgange og adgangsrettigheder) omhandler styring og løbende opfølgning på brugeres retmæssige adgange og rettigheder til regionens it-systemer og it-udstyr. Formålet er at sikre, at kun de brugere, der har et arbejdsbetinget behov for adgang til systemer eller oplysninger, kan tilgå disse.

Der har gennem flere år været stort fokus på brugeradgange og adgangsrettigheder, og der er gennem årene opbygget en god systematisk opfølgning på bruger- og adgangsrettigheder, særligt for de tværgående it-systemer. De enkelte enheder har i 2020 – med udgangspunkt i retningslinjerne – haft til opgave at sikre:

1. Opfølgning på brugeradgange og adgangsrettigheder
2. Ledelsesmæssig godkendelse af opfølgningen
3. Håndtering af brugere med administratorrettigheder, herunder tidsbegrænsning af disse rettigheder
4. Overvejelser om muligheder for automatisering af kontroller på området
5. Kontroller af robotbrugere (RPA-brugere) og servicekonti

Der er fortsat er behov for fokus på dette område. Brugeradgang og kontrol har flere gange været underlagt ekstern revision. Og dette har tidligere resulteret i bemærkninger om utilstrækkelig dokumentation og systematik.

Med udgangen af 2020 har Region Syddanmark ibrugtaget en fælles brugerhåndteringsløsning (SYDID), der med yderligere modning understøtter arbejdet med at oprette, ændre og nedlægge brugere.

Det foreslås, at SydID udbygges i 2021 og bredes ud til regionens tværgående it-systemer. I sammenhæng hermed kan SydID konfigureres til at bistå i opgaven med opfølgning på brugere- og adgangsrettigheder.

Udgangspunktet for kontrol med bruger- og adgangsrettigheder er retvisende oplysninger, derfor foreslås en opdatering af oplysningerne i regionens centrale dokumentationssystem for it-systemer (CMDB), så det sikres at informationerne fortsat er korrekte.

Med afsæt i den risikobaserede tilgang foreslås det at gennemføre en prioritering af regionens systemer med henblik på at gennemgå bruger- og adgangsrettigheder. Herefter anbefales etableret en samlet plan for gennemgangen, samt etablering af standardiserede procedurer for opfølgning på tværs af regionen. Derved søges revisionens kritik af utilstrækkelig dokumentation og mangelfuld systematik imødegået.

Opsummeret anbefales følgende mål for temaet bruger- og adgangsrettigheder for 2021:

1. Udbygning af SydID til at omfatte regionens tværgående it-systemer.
2. Etablering af muligheder for opfølgning på bruger- og adgangsrettigheder i SydID
3. Opdatering af dokumentationen for regionens it-systemer i det centrale dokumentationssystem for IT systemer (CMDB)
4. Etablering af prioriteringsplan for gennemgang af bruger- og adgangsrettigheder
5. Fælles proces for opfølgning på bruger- og adgangsrettigheder på tværs af regionen

Databehandleraftaler

Et vigtigt element i regionens arbejde med at sikre, at data opbevares og håndteres sikkert, er de aftaler, som regionen indgår med leverandører. Retningslinje 11.11 (Leverandørstyring i relation til informationssikkerhed og databehandling) beskriver krav til håndtering af de data, som eksterne leverandører har adgang til. På basis af risikovurderinger afgøres, hvorvidt der er behov for indgåelse af en databehandlingsaftale, fortrolighedserklæring eller anden form for kontrakt med eksterne leverandører.

Databehandleraftaler og implementering af retningslinjen om leverandørstyring har været et indsatsområder i de seneste ca. tre år. Regionen har i hvert enkelt tilfælde vurderet behovet for at indgå databehandleraftaler med leverandøren. Regionen har i skrivende stund indgået 337 databehandleraftaler, og yderligere 43 er under udarbejdelse. I de resterende tilfælde har risikovurderingerne peget på alternativer til databehandleraftaler – f.eks. fortrolighedserklæringer eller omhandlet systemer uden følsomme data.

Det vurderes, at der fortsat er behov for at fastholde fokus på området. Dels skal aftalerne løbende revideres på baggrund af fornyede risikovurderinger, ligesom regionen gennem sin opfølgning på aftalerne sikrer, at leverandørerne lever op til kravene i aftalen.

Som det fremgår, er der indgået et stort antal databehandleraftaler, og der er fortsat også et antal aftaler i proces. I forlængelse af målet om opdatering af oplysningerne i regionens centrale dokumentionssystem for it-systemer (CMDB) foreslås det, at der sker en stillingtagen til *alle* regionens systemer, i forhold til behovet for databehandleraftaler og opfølgning.

En række af de databehandleraftaler, der er indgået, er indgået for flere år siden, og disse er indgået med afsæt i den daværende viden og (tværregionale) skabeloner. Skabelonerne er løbende revideret, og der er også sket en ny fortolkning af lovgivning på området. Endvidere har Rigsrevisionen

anbefalet, at databehandleraftalerne skal hvile på en risikovurdering. På den baggrund anbefales et mål om at gennemføre eller opdatere de eksisterende risikovurderinger og på den baggrund genvurdere behovet for allerede indgåede databehandleraftaler.

Når regionen har indgået en databehandleraftale, skal der følges op på denne. Der foreligger en central skabelon for opfølgningen. Det foreslås, at der udarbejdes et samlet overblik og en samlet plan for opfølgning på de indgåede databehandleraftale.

Opsummeret anbefales følgende mål for databehandleraftaler for 2021:

1. Stillingtagen til *alle* regionens systemer, i forhold til behovet for databehandleraftaler og opfølgning
2. Indgåelse af nye databehandleraftaler eller der er igangsat processer herfor jf. punkt ovenfor
3. Vurdering af eksisterede databehandleraftaler på baggrund af fornyet risikovurdering.
4. Samlet overblik over og plan for opfølgning af databehandleraftaler.

Oplysning, uddannelse og medarbejdernes adfærd (awareness)

Retningslinje 11.03 (Personaleforhold i relation til informationssikkerhed) beskriver vigtigheden af, at alle medarbejdere oplyses om og uddannes i håndteringen af informationssikkerhed, også kaldet awareness. Formålet er, at den enkelte medarbejder er opmærksom på og kan tage et ansvar for, at data behandles og opbevares trygt.

Regionen løser denne opgave ved brug af forskellige oplysningsaktiviteter, herunder kampagner, video- og tegnefilm og skriftligt materiale. Dertil tilbyder regionen en række uddannelsesaktiviteter for de forskellige medarbejdergrupper.

Det vurderes, at der er et kontinuerligt behov for oplysnings- og uddannelsesaktiviteter i lyset af, at der sker en løbende udskiftning i medarbejderstaben. Dertil skal aktiviteterne tilpasses løbende for at imødegå nye former for trusler og risici. Dette gælder både for centrale tiltag, men ikke mindst tiltag på den enkelte enhed og i den enkelte afdeling.

Regional IT har en central støttefunktion i forhold til dette arbejde, som er organiseret i IT Styring og Informationssikkerhed. Enheden bistår med at udvikle materialer (plakater, video, skriftligt materiale) og at koordinere aktiviteter og facilitere valg af fælles indsatser. Fælles indsatser kan være kampagner, sikre at nyansatte introduceres til informationssikkerhed, uddannelseskurser mv.
De enkelte enheder har ansvar for at sikre ledelsesmæssig forankring af oplysnings- og uddannelelsesaktiviteter, herunder kommunikation med medarbejderne og formidling af relevante indsatser.

For at understøtte oplysnings- og uddannelsesarbejdet foreslås gennemført en målgruppeanalyse, så initiativerne kan målrettes mod forskellige faggrupper: f.eks. lægesekretærer, sygeplejersker, administrative medarbejdere eller it-ansatte.

Det foreslås også, at nye medarbejdere gives basisviden om informationssikkerhed i forbindelse med introduktionen til regionen som arbejdsplads, herunder hvilke forventninger dette indebærer til den enkelte som medarbejder.

For yderligere at styrke uddannelsesarbejdet afprøves et nyt E-læringsmodul. Hvis resultaterne er gode, kan modulet udbredes til it-ansatte og medarbejdere med et særligt ansvar i forhold til informationssikkerhed.

Blandt regionens nøglepersoner, systemansvarlige og informationssikkerhedsansvarlige i de enkelte afdelinger tilbyder IT Styring og Informationssikkerhed kurser i informationssikkerhed. Disse kurser foreslås gjort mere tilgængelige via regionens kursuskatalog.

Opsummeret anbefales følgende mål for temaet om oplysning, uddannelse og medarbejdernes adfærd (awareness) for 2021:

1. Gennemførsel af målgruppeanalyse for at sikre at regionens initiativer rammer de relevante medarbejdergrupper
2. Basisviden om informationssikkerhed indarbejdes i introduktionsprogrammet for nye medarbejdere
3. Afprøvning og udbredelse af regionens E-læringmodul i Informationssikkerhed
4. Udbredelse af centrale kurser i informationssikkerhed

Oversigt over retningslinjer for informationssikkerhed:

- Informationssikkerhedsbrud
- Leverandørstyring
- Brugeradgange og rettigheder
- Netværksstyring
- Nød-, beredskabs- og re-etableringsstyring
- Audit
- Driftssikkerhed
- Klassifikation
- Risikostyring
- Personaleforhold
- Styring af databærende systemer og udstyr
- Password
- Fysisk sikring og miljøsikring
- Initiativer til at imødekomme kravene i GDPR
- Organisering af informationssikkerhedsarbejdet

Retningslinjerne kan læses i deres helhed i regionens dokumenthåndteringsværktøj Infonet:

https://infonet.regionsyddanmark.dk/D4Doc/book/bookcontentHieraki.asp?BookID=174&DokID=0&HGruppeID=0#Afs39997