SYKEHUSINNKJØP

Sak 38/2019

Saksfremlegg til styret i Sykehusinnkjøp

Internkontroll for informasjonssikkerhet

Møtedato:	14.juni 2019	
Tidligere behandlet i styret/saksnr.	sak 77/2017 sak 15/2018 sak 46/2018	
Type sak (orienteringssak, diskusjonssak, beslutningssak, temasak)	Orienteringssak	

Styret i Sykehusinnkjøp inviteres til å treffe følgende vedtak:

1. Styret i Sykehusinnkjøp HF tar informasjon om internkontroll for informasjonssikkerhet til orientering.
2. Styret ber administrerende direktør orientere om status for gjennomføring av plan for internkontroll for informasjonssikkerhet når systemet vurderes implementert i foretaket.

Vadsø, 7.juni 2019

Kjetil M. Istad
Administrerende direktør

1. Hva saken gjelder

Denne saken gjør rede for status og fremdrift for plan for internkontroll for informasjonssikkerhet. Styret bestilte leveransen i sak 59/2017 og ble orientert om status i sak 77/2017, sak 15/2018 og sak 46/2018.

I sak 46/2018 traff styret følgende vedtak:

> *«1. Styret tar plan for internkontroll for informasjonssikkerhet til orientering.*
>
> *2. Styret ber administrerende direktør orientere om status for gjennomføring av plan for internkontroll for informasjonssikkerhet i løpet av 4.kvartal 2018.»*

Denne saken er en oppfølging av vedtakets punkt 2.

Det vises også til oppdragsdokumentet 2019 punkt f) «Informasjonssikkerhet og personvern» hvor det understrekes at helseforetaket skal ha et styringssystem for informasjonssikkerhet og kompetansen om digital sårbarhet skal styrkes blant egne ansatte.

Administrerende direktør legger nå frem saken for styret til orientering.

2. Bakgrunn

Etableringen av internkontroll for informasjonssikkerhet i Sykehusinnkjøp HF er basert på DIFI sitt etablerte rammeverk med veileder som styret sluttet seg til etter administrerende direktørs anbefaling i styresak 15/2018.

DIFI sin veileder inneholder fire faser og 10 etableringsaktiviteter. Disse aktivitetene skal legge til rette for en systematisk og forholdsmessig internkontroll av virksomhetens informasjonssikkerhet støttet av en etablert sikkerhetsorganisasjon.

I sak 46/2018 ble styret informert om at DIFI sin veileder inneholder følgende faser og aktiviteter:

Faser:	Aktiviteter:
1. Avklare behov og lage en plan	1. Analyse og kartlegging 2. Planlegge etablering
2. Få på plass det viktigste	3. Utforme styrende dokumenter 4. Ansvar og roller i sikkerhetsorganisasjonen 4.1 Identifisere nøkkelpersoner 5. Utforme og gjennomføre grunnopplæring 6. Etablere system for hendelses- og avvikshåndtering
3. Skape en god plattform for internkontrollen	7. Etablere fellessikring og synliggjøre tilleggssikring 8. Etablere rammeverk for dokumentasjon
4. Lag et godt grunnlag for sentrale, systematiske aktiviteter	9. Identifisere typiske oppgave- og informasjonstyper 10. Felles analyse av eksterne krav

Styret ble videre orientert om at fase 2 «Få på plass det viktigste» var iverksatt, og at avslutningen av fase 2 ble anbefalt som neste milepælsrapportering.

Arbeidet med internkontroll for informasjonssikkerhet er forsinket i forhold til opprinnelig fremdriftsplan, men er nå tilbake til normal drift.

3. Status for arbeidet

Det er siden siste rapportering jobbet med aktiviteter i både fase 2, fase 3 og fase 4. Rammeverket til DIFI består av både sekvensielle og parallelle aktiviteter slik at aktivitetene nødvendigvis ikke gjennomføres i kronologisk rekkefølge. Hovedfokus i perioden har vært å etablere system for innebygd informasjonssikkerhet og personvern (Information Security Management System - ISMS).

Formålet med systemet er å sikre nødvendig konfidensialitet, integritet og tilgjengelighet på virksomhetens informasjon. Når systemet er implementert (fase 3) vil foretaket kunne oppnå samsvar med regelverk og anbefalt praksis innenfor området, samt gi ledelsen grunnlag for å følge opp dette kontinuerlig.

I tillegg til å vareta konfidensialitet, integritet og tilgjengelighet på virksomhetens informasjon fokuserer systemet også på viktige tilleggsegenskaper omkring sikring av data:

- autentisitet (sikre at informasjon og brukere er ekte)
- sporbarhet/ansvarlighet (kunne spore endringer/holde brukere ansvarlig for sine handlinger)
- pålitelighet (at informasjon og systemer er til å stole på og fungerer som forventet)

Systemet er utviklet og etablert i SharePoint som er en sentral del av felles IKT-plattform.

I forhold til de konkrete punktene i fase 2 er status slik:

Aktivitet 3: Utforme styrende dokumenter – Regulatoriske krav og plikter slik som personvernlovgivning og annen relevant lovgivning er bygget inn i systemet slik at det kan forvaltes systematisk i forhold til virksomhetens rammer og foretakets forretningsmessige risikotilnærming. Det samme gjelder for aktuelle standarder som f.eks. ISO27001: 2013 som er anbefalt standard til dette formålet. Det er foreløpig ikke ferdig utviklet egne styrende dokumenter. Dette vil bli gjort som en forberedelse til implementeringen og man vil da basere seg på DIFI sine maler og tilpasse de til virksomhetens behov, visjon og oppdrag. Et aktuelt dokument som må utarbeides er f.eks. felles retningslinjer for behandling av informasjon i virksomheten.
Aktivitet 4: Ansvar og roller i sikkerhetsorganisasjonen og identifiserte nøkkelpersoner - Rollen som fagansvarlig for informasjonssikkerhet er identifisert og lagt til IKT-leder, og det er utpekt Personvernombud. Ansvar og roller i sikkerhetsorganisasjonen er beskrevet i systemet og følger anbefalinger fra ISO-standard for informasjonssikkerhet (ISO27001:2013). Siden foretaket ikke har etablert alle slike roller tidligere har man funnet det formålstjenlig å identifisere ytterligere nøkkelpersoner i tilknytning til implementeringen av systemet. Dette for å sikre at opplæring er tilgjengelig for nøkkelpersonene.

Aktivitet 5: Utforme og gjennomføre grunnopplæring – Det er bygget opp kompetanse for sentrale ressurser i IKT-avdelingen. For øvrige medarbeidere vil grunnopplæring bli gjennomført i fase 3 da det er naturlig å gjøre dette i nær tilknytning til implementeringen. Grunnopplæringen vil bygge på kursmateriell fra DIFI, men tilpasses til virksomhetens fagområder og organisasjonens behov.
Aktivitet 6: Etablere et system for hendelses- og avvikshåndtering – System for hendelses- og avvikshåndtering inngår i systemet for innebygd informasjonssikkerhet og personvern og er således etablert**.** Systemet legger opp til at avviksrapportering skal oppfattes som innspill til forbedring og ikke nødvendigvis feil. Dette er viktig for å motivere til rapportering Det gjenstår å utarbeide prosedyre for håndtering av hendelser og avvik for informasjonssikkerhet.

I tillegg til de nevnte punktene ovenfor er noen aktiviteter tilhørende fase 3 og fase 4 også gjennomført. Dette gjelder punkt 8 om etablering av rammeverk for dokumentasjon, samt punkt 10 som gjelder felles analyse av eksterne krav som ble gjennomført som en innledende aktivitet.

4. Aktiviteter fremover

Fremover vil fokus være å planlegge og gjennomføre implementering av system for innebygget informasjonssikkerhet og personvern i felles IKT-plattform. En vellykket implementering av system for informasjonssikkerhet betinger egnet plattform med innebygget støtte for datastyring og -vern basert på retningslinjer for klassifisering av lagringsmedier, kommunikasjonskanaler og elementtyper. Foretakets IKT-plattform oppfyller alle krav og behov for å implementere systemet.

Sykehusinnkjøp HF har tjenesteutsatt sentrale oppgaver for forvaltning av konfigurasjon av vår IKT-plattform. Videre arbeid og fremdrift vil derfor måtte skje i tett samarbeid med Helse Nord IKT som er leverandør av driftstjenester på IKT-plattformen. Første aktivitet i den forbindelse vil være å etablere en fremdriftsplan for det videre arbeid i samarbeid med Helse Nord IKT.

Etterlevelse og kultur er en avgjørende faktor for informasjonssikkerhet, og utgjør den egentlige kvaliteten. Dette innebærer tett involvering av linjeorganisasjon og interne tiltak for kompetanseløft, men det må også påregnes at foretaket vil ha behov for støtte fra eksterne fagspesialister på området for å få til en vellykket implementering.

5. Oppsummering

Relevante aktiviteter i fase 2 av DIFI sin veileder er fullført, og det er vurdert at de aktiviteter som gjenstår vil være mest formålstjenlig å gjennomføre i fase 3 på grunn av den nære tilknytningen til implementeringen av systemet.

Avslutningen av fase 3 anbefales som neste milepælsorientering til styret. Systemet for innebygd informasjonssikkerhet og personvern vil da være implementert i foretaket.

6. Anbefaling

Administrerende direktør anbefaler at styret i Sykehusinnkjøp HF tar fremlagt status og fremdrift for plan for internkontroll for informasjonssikkerhet til orientering.