SYKEHUSINNKJØP

Sak 46/2018

Saksfremlegg til styret i Sykehusinnkjøp HF

Orientering om plan for internkontroll for informasjonssikkerhet

Møtedato:	14. juni 2018	
Tidligere behandlet i styret/saksnr.	59/2017, 77/2017	15/2018
Type sak (orienteringssak, diskusjonssak, beslutningssak, temasak)	Orienteringssak	

Styret i Sykehusinnkjøp HF inviteres til å treffe 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.

Vadsø, 7. juni 2018

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 og sak 15/2018.

Viser videre til oppdragsdokumentet 2018 punkt 3G «Etablering av sikkerhetsorganisasjon», brev fra Helse- og omsorgsdepartementet av 19. desember 2014 samt brev fra de regionale helseforetakene av 15. november 2017 om «etablering av sikkerhetsorganisasjon».

Administrerende direktør legger nå frem status i arbeidet for styret.

2. Hovedpunkter i orientering av status

Etableringen av internkontroll for informasjonssikkerhet 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 sikkehetsorganisasjon. Resultatene fra etableringen vil inngå i den generelle internkontrollen.

Hvis det blir påvist at virksomhetens forvaltning av tjenester og informasjon omfatter skjermingsverdige objekter og sikkerhetsgradert informasjon, slik det er definert i lov om forebyggende sikkehetstjeneste (sikkerhetsloven), vil sikkerhetsorganisasjonen tilpasses eventuelle nye krav til tiltak.

Planen har også tatt høyde for at virksomheten må oppfylle grunnleggende krav i ny personopplysningslov (GDPR) som er forespeilet å tre i kraft 1. juli 2018. Fagansvarlig for informasjonssikkerhet og stabsdirektør har deltatt på GDPR-kurs og har identifisert aktiviteter i etableringsplanen som samsvarer med grunnleggende krav i ny personvernsforordning.

Her følger en oversikt over faser og aktiviteter i DIFI sin veileder:

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.

Status på etableringsplanen:

Fase 1 «Avklare behov og lage en plan» er allerede gjennomført og har sikret viktige forutsetninger for planleggingen og videre gjennomføring.

Med fase 1 som grunnlag, er fase 2 «Få på plass det viktigste» iverksatt. Fasens aktiviteter har som formål å skape et styrende rammeverk for arbeidet og forankre prosjektet i organisasjonen. Aktivitet 10 "felles analyse av eksterne krav" er fremskyndet for å ivareta sentrale krav i ny personopplysningslov.

Avslutningen av fase 2 anbefales som neste milepælsrapportering til ledergruppen. På dette tidspunktet vil det være etablert et rammeverk, en sikkerhetsorganisasjon og identifiserte nøkkelpersoner som er nødvendig for gjennomføring av aktiviteter i fase 3 og 4.

Her følger en oppsummert oversikt over status på aktivitetene:
Fullstendig etableringsplan ligger vedlagt. Merk at nummerering avviker fra kronologien fordi det er både sekvensielle og parallelle aktiviteter:

Uke 16-20. Ferdige aktiviteter:

- **Aktivitet 1: Analyse og kartlegging –** Det er gjennomført kartlegging og analyser, og man har opprettet en konfigurasjonsoversikt som er tilstrekkelig for å fortsette etableringen. Oversikten skal holdes ved like og danner grunnlag for videre klassifisering av tjenester og informasjonselementer.

- **Aktivitet 2: Planlegge etablering -** Stab ved IKT-leder har planlagt etableringen i samsvar med DIFI sin veileder for internkontroll for informasjonssikkerhet. Etableringsplanen viser hvilke konkrete oppgaver som må utføres for å oppnå målet om internkontroll.

Uke 20-27. Påbegynte aktiviteter:

- **Aktivitet 3: Utforme styrende dokumenter -** Utforming av styrende dokumenter baserer seg på DIFI sine maler og tilpasses virksomhetens behov, visjon og oppdrag. Aktiviteten er påbegynt og man har skissert de første dokumentene.

- **Aktivitet 4: Ansvar og roller i sikkerhetsorganisasjonen og identifiserte nøkkelpersoner -** Ansvar og roller i sikkerhetsorganisasjonen vil følge linjen og det vil etableres tilstrekkelige med støttefunksjoner, eksempelvis personvernombud. Rollen som fagansvarlig for informasjonssikkerhet er identifisert og lagt til IKT-leder. Videre identifisering av roller og ansvar vil avklares underveis i prosjektets fremdrift.

- **Aktivitet 10: Felles analyse av eksterne krav -** Risikoeiere (systemeiere) vil jobbe med å identifisere konkrete krav om sikkerhetstiltak i overordnet regelverk og avtaler innenfor sine ansvarsområder. Det ble gjennomført en analyse av eksterne krav november 2017 som vil være grunnlaget for videre arbeid.

Fra uke 30. Fremtidige aktiviteter:

- **Aktivitet 5: Utforme og gjennomføre grunnopplæring -** Grunnopplæringen vil være sammensatt av DIFI sitt kursmateriell og vil blant annet bestå av rollespill, nettkurs og diskusjoner med dilemmatrening. Sikkerhetsorganisasjonen vil tilpasse DIFI sine opplæring- og informasjonspakker etter virksomhetens fagområder og organisasjonens behov. Første grunnopplæringen vil gjennomføres for stab/fellesfunksjoner innen uke 30.

- **Aktivitet 6: Etablere et system for hendelses- og avvikshåndtering -** Sikkerhetsorganisasjonen vil opprette prosedyre for håndtering av hendelser og avvik for informasjonssikkerhet.

- **Aktivitet 7: Etablere fellessikring og synliggjøre tilleggssikring -** Etablering av fellessikring og synliggjøre tilleggssikring innebærer å kartlegge og potensielt forbedre eksisterende sikkerhetstiltak, og etablere nye der hvor det er nødvendig.

- **Aktivitet 8: Etablere rammeverk for dokumentasjon -** Sikkerhetsorganisasjonen vil opprette et rammeverk for dokumentasjon som er tilpasset virksomhetens generelle internkontroll og virksomhetsstyring.

- **Aktivitet 9: Identifisere typiske oppgave- og informasjonstyper -** Organisasjonens systemeiere vil opprette en samling eksempler over typiske oppgave- og informasjonstyper. Samlingen vil benyttes som et oversiktsbilde ved senere internkontrollsaktiviteter.

Veien videre og systematiske aktiviteter:
Når etableringen er gjennomført og ansvar og roller i sikkerhetsorganisasjonen er fordelt, beskrevet og dokumentert, vil produktene overleveres Kvalitet. Kvalitet vil dermed overta ansvaret for å integrere internkontroll for informasjonssikkerhet som systematiske aktiviteter i virksomhetens øvrige internkontroll.

3. Oppsummering

Fase 1 av DIFI sin veileder er fullført i henhold til bestilling og videre gjennomføring er iverksatt. Neste milpælsorientering til ledergruppen anbefales lagt ledermøtet i august 2018 i forbindelse avslutning av fase 2, aktivitet 6. Dette begrunnes med at fase 3 og 4 er mest krevende både teknisk og ressursmessig, fordi risikoeiere i linjeorganisasjonen skal jobbe med å identifisere interne og eksterne risikoer for sine fagfelt.

Man planlegger å gjennomføre de siste aktivitetene i etableringen i løpet av november 2018 og har som mål at ledergruppen og styret kan orienteres desember samme år. Dette er en foreløpig dato ettersom flere aktiviteter må gjennomføres av ansatte i linjeorganisasjonen.

4. Anbefaling

Etableringen av internkontroll for informasjonssikkerhet er planlagt i henhold til bestilling. Administrerende direktør direktør anbefaler at styret i Sykehusinnkjøp HF tar fremlagt status av etableringsplanen til orientering.

Trykte vedlegg

- Etableringsplan for internkontroll for informasjonssikkerhet

Utrykte vedlegg

- DIFI sin veileder: ***http://internkontroll.infosikkerhet.difi.no***
- Brev fra Helse- og omsorgsdepartementet av 19. Desember 2014
- Brev fra de regionale helseforetakene ved Helse Nord RHF. "Etablering av sikkerhetsorganisasjon". 15. November 2017.