SYKEHUSINNKJØP

Sak 56/2022

Saksfremlegg til styret i Sykehusinnkjøp HF

Status informasjonssikkerhet og personvern

Møtedato:	16. juni 2022	
Tidligere behandlet i styret/saksnr.	77/2017 15/2018 46/2018 38/2019 72/2021	
Type sak (orienteringssak, diskusjonssak, beslutningssak, temasak)	Orienteringssak	

Styret i Sykehusinnkjøp HF inviteres til å treffe følgende vedtak:

1. Styret tar saken til orientering.

Vadsø, 9. juni 2022

Bente Hayes
administrerende direktør

1. Hva saken gjelder

Denne saken redegjør for status og fremdrift i plan for internkontroll for informasjonssikkerhet. Styret har tidligere bedt om dette, ref. sak 59/2017, og det ble orientert om status i sak 77/2017, sak 15/2018, sak 46/2018, sak 38/2019 og sak 72/2021.

I sak 72/2019 traff styret 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.*

Administrerende direktør legger nå frem saken for styret til orientering.

2. Hovedpunkter og handlingsalternativer

Som det er gjort rede for i tidligere saksfremlegg, baserer arbeidet med informasjonssikkerhet i Sykehusinnkjøp HF seg på DIFI, nå Digitaliseringsdirektoratet (Digdir) sitt etablerte rammeverk med veileder som styret sluttet seg til etter administrerende direktørs anbefaling i styresak 15/2018.

Sykehusinnkjøp HF er kommet langt i arbeidet med å etablere et helhetlig ledelsessystem for informasjonssikkerhet og personvern i foretaket. Gjenstående arbeid omfatter beslutninger omkring ansvarlige roller i organisasjon, samt analyse av virksomhetens leveranser og tjenesters avhengighet til teknologiske ressurser.

Prioritering av vitale forretningsfunksjoner og krav til sikkerhetsnivå for disse skal ferdigstilles i løpet av høsten 2022. Identifiserte avhengigheter til IKT-funksjoner, IKT-tjenester og IKT-systemer vil danne grunnlaget for krav til tjenestenivå, gjenopprettelsestid, og beskyttelse av data. Det er særlig forhold mellom eierskap til prosess og system at mål om å sikre at IKT-systemer understøtter prosesser innen foretakets ulike virksomhetsområder.

Prosesseier skal kunne stille krav til systemstøtten basert på fagmessige vurderinger og prioritering til kontinuerlig forbedring gjennom foretakets prosess for endringsstyring av IKT-tjenesteportefølje. Systemeier skal på sin side sikre merkantile forhold, herunder budsjettrammer, tilfredsstillende organisering og bemanning omkring bruk og forvaltning av systemet.

Samråd mellom disse to rollene skaper grunnlag for et helhetlig perspektiv både med hensyn til virksomhet, informasjonssikkerhet og digitaliseringsgevinster. Samarbeid om videreutvikling av prosesser og IKT-systemportefølje med forankring i foretakets virksomhetsarkitektur bidrar til forsvarlig endringsstyring innenfor både teknologiske og økonomiske rammer.

I ledermøtesak 58/2021 ble styrende dokumenter for System for informasjonssikkerhet og personvern vedtatt, men på grunn av større endringer i de samme dokumentene gjennomførte ledergruppen en ny gjennomgang og godkjenning av dokumentene i sak 38/2022. Mandatene til IKT-utviklingsråd og IKT-sikkerhetsråd ble videre godkjent i sak 46/2022.

Fordeling av systemeierroller i foretakets IKT-tjenesteportefølje er planlagt vedtatt i ledermøtet 28. juni 2022.

Foretakets avtalte tjenestenivå og forpliktelser skal følges opp av både ansatte i egen organisasjon og innleide ressurser. Forretnings- og personopplysninger skal behandles i samsvar med de krav som er gitt i lov og avtaler. Informasjonssikkerhetsnivå skal etableres og opprettholdes ved kontinuerlig:

- Identifisere og kartlegge virksomhetens leveranser og tjenester
- Beskytte og opprettholde en sikker tilstand for IKT-systemer og på denne måte motstå eller begrense skaden fra dataangrep
- Oppdage sårbarheter og trusler ved å overvåke avvik fra sikker tilstand
- Håndtere hendelser og gjenopprette normaltilstand basert på kontroll og evaluering. Kontinuerlig oppfølging av sikkerhetstiltak basert på erfaring
- Kommunisere kunnskap, holdninger og forventinger til ansatte på alle nivå for å skape bevissthet omkring risiko og opprettholde god sikkerhetskultur

Internrevisjonen i Sykehusinnkjøp HF meldte 08.04.2022 oppstart av fase én for revisjonstema «Informasjonssikkerhet og personvern», i henhold til vedtatt revisjonsplan for 2022/2023.

Revisjonens formål er å bekrefte at foretaket har etablert en egnet internkontroll for informasjonssikkerhet og personvern. Følgende dokumentasjon ble oversendt i henhold til frist 28.04.2022:

- Foretakets styrende dokumenter for informasjonssikkerhet og personvern
- En oversikt over IKT-arkitektur (Infrastruktur, IKT-systemer, integrasjoner og digitale tjenester)
- En oversikt over foretakets inngåtte databehandleravtaler
- Databehandleravtaler med de regionale helseforetakene og/eller deres underliggende IKT-foretak
- Protokoll over behandling av personopplysninger

3. Anbefaling

Internrevisjonen vil i neste fase etterse implementering av sikkerhetstiltak for deretter, i avsluttende fase, avdekke om ønskede effekter er oppnådd. Gjennomføring av plan for internkontroll for informasjonssikkerhet er fullført. Ledelsessystem for informasjonssikkerhet og personvern er etablert og underlagt internrevisjon.

Administrerende direktør anbefaler styret å ta saken til orientering.