Saksfremlegg til styret i Sykehusinnkjøp HF

Sak 28/2023

Møtedato:	30. mars 2023
Saksbehandler:	Geir Arne Eriksen
Divisjon/fellesfunksjon:	Økonomi og virksomhetsstyring
Sakstype:	☒ Beslutningssak ☐ Orienteringssak ☐ Temasak
Offentlighetsvurdering:	☒ Offentlig sak ☐ Unntatt offentlighet etter §__
Tidligere behandlet i styret/saks-nr.:	

Handlingsplan for oppfølging av internrevisjonsrapport 01/2022

Styret i Sykehusinnkjøp HF inviteres til å treffe følgende vedtak:

1. Styret godkjenner handlingsplan for oppfølging av anbefalinger fra internrevisjonen.
2. Styret ber administrerende direktør rapportere på status i arbeidet i fjerde kvartal 2023.

Vadsø, 23. mars 2023

Bente Hayes

administrerende direktør

1. Hva saken gjelder

I denne saken legger administrerende direktør frem forslag til handlingsplan for oppfølgingsarbeidet knyttet til internrevisjonens anbefalinger i *Internrevisjonsrapport 01/2022 - Internkontroll for informasjonssikkerhet og personvern – Fase 1.* Styret ba i møte 26. januar 2023 administrerende direktør sørge for at internrevisjonens anbefalinger følges opp, og at en handlingsplan for oppfølgingsarbeidet framlegges for styret i løpet av våren 2023.

2. Hovedpunkter og handlingsalternativer

Formålet med revisjonen i fase 1 har vært å bekrefte at Sykehusinnkjøp HF har etablert styrende dokumenter for internkontroll for informasjonssikkerhet og personvern, og at disse er tilpasset foretakets størrelse, risiko og egenart.

Sykehusinnkjøp har vedtatt et sett av overordnede, styrende dokumenter innen informasjonssikkerhet og personvern, og det gjennomføres generelle opplæringsaktiviteter innen temaet. Internrevisjonen konkluderer med at de styrende dokumentene i liten grad er tilpasset foretakets størrelse, risiko og egenart, ettersom de ikke knyttes til foretakets leveranser, prosesser og informasjonstyper. Beskrivelser av roller og ansvar har svakheter, og det mangler, eller er mangler ved, prosessbeskrivelser for sentrale aktiviteter i internkontrollen.

I rapporten kommer internrevisjonen med åtte anbefalinger til Sykehusinnkjøp HF:

1. *Tilpasse styrende dokumenter til foretakets størrelse, risiko og egenart.*
2. *Påse at alle sentrale rolle- og stillingsbeskrivelser innen informasjonssikkerhet og personvern er beskrevet.*
3. *Påse at revidert utgave av beredskaps- og kriseplan omhandler informasjonssikkerhet og personvern.*
4. *Prioritere fastsetting av nivå for akseptabel risiko for konfidensialitet, integritet, tilgjengelighet og robusthet, jf. styresak 56/2022.*
5. *Etablere prosessbeskrivelse for forvaltning av databehandleravtaler.*
6. *Etablere prosessbeskrivelse for forvaltning av protokoll over behandling av personopplysninger.*
7. *Inngå databehandleravtale der det mangler, og revidere/oppdatere databehandleravtaler inngått før personopplysningsloven ble endret i juli 2018.*
8. *Etablere og/eller revidere prosessbeskrivelse for sentrale aktiviteter i internkontrollen for informasjonssikkerhet og personvern, herunder: risiko- og sårbarhetsanalyser, personvernkonsekvensutredninger, risikohåndtering, gjennomføring av sikkerhetstiltak, og ledelsens gjennomgåelse.*

I styremøtet 26. januar 2023 ble det bemerket at anbefaling fire handler om fastsetting av nivå for akseptabel risiko. Styret ba administrasjonen om å vurdere innføring av kriterier for å akseptere risiko i stedet for nivå for akseptabel risiko, jamfør Digitaliseringsdirektoratets veiledning om at «virksomheten bør ha føringer for hvordan arbeidet med håndtering av risiko skal gjennomføres, inkludert kriterier for å akseptere risiko».

Internrevisjonsrapporten har vært gjennomgått og behandlet i IKT-sikkerhetsråd, som har vurdert anbefalingene. For å sikre et godt og systematisk fokus er det utarbeidet en handlingsplan med tilhørende tiltak for hver av de åtte anbefalingene fra internrevisjonen. Forslag til handlingsplan med tidsfrister følger nedenfor.

Nr.	Anbefaling	Tiltak		Tilknyttet dokument	Tidsfrist
1.	Tilpasse styrende dokumenter til foretakets størrelse, risiko og egenart.	a)	Tilpass dokumentet *System for informasjonssikkerhet og personvern* til foretakets størrelse, risiko og egenart	SIP*[1]	Q2-23
		b)	Tilpass dokumentet *Prinsipper for behandling av personopplysninger i Sykehusinnkjøp HF* til foretakets størrelse, risiko og egenart	Prinsipper for behandling av personopplysninger i Sykehusinnkjøp HF	Q2-23
		c)	Tilpass dokumentet *Behandling av personopplysninger i Sykehusinnkjøp HF* til foretakets størrelse, risiko og egenart	Behandling av personopplysninger i Sykehusinnkjøp HF	Q2-23
		d)	Oppdater *Vedlegg 1* slik at det beskriver hvordan de ulike regelverkene må tas hensyn til i etableringen av internkontroll	SIP-Vedlegg 1	Q3-23
		e)	Oppdater *Vedlegg 3* til «Sykehusinnkjøp sin egenart»	SIP-Vedlegg 3	Q3-23
		f)	Ferdigstill kapittel 2.4 i *vedlegg 5*	SIP-Vedlegg 5	Q3-23
2.	Påse at alle sentrale rolle- og stillingsbeskrivelser innen informasjonssikkerhet og personvern er beskrevet.	a)	Utarbeid rollebeskrivelse for informasjonssikkerhetsleder	SIP-Vedlegg 4	Q2-23
		b)	Utarbeide rollebeskrivelse for IT sjef		Q2-23
		c)	Oppdater rollebeskrivelsen for personvernombud i samsvar med personvernopplysningsloven artikkel 39 og datatilsynets beskrivelse av personvernombudets oppgave.	SIP – Behandling av personopplysninger i SHI	Q2-23
		d)	Utarbeide rollebeskrivelse for Juridisk rådgiver personvern		Q2-23
		e)	Vurder skille i rollebeskrivelse mellom intern forvaltning og ekstern forvaltning for systemeier og systemansvarlig	SIP - Vedlegg 4	Q2-23
		f)	Utarbeide rollebeskrivelse for virksomhetsarkitekt	SIP - Vedlegg 4	Q2-23
3.	Påse at revidert utgave av beredskaps- og kriseplan omhandler informasjonssikkerhet og personvern.	a)	Innarbeide håndtering av trusselbildet relatert til informasjonssikkerhet og personvern i revidert utgave av beredskaps- og kriseplan	Krise og beredskapsplan for Sykehusinnkjøp HF	Q4 -23

[1] System for informasjonssikkerhet og personvern

Nr.	Anbefaling	Tiltak		Tilknyttet dokument	Tidsfrist
4.	Prioritere fastsetting av nivå for akseptabel risiko for konfidensialitet, integritet, tilgjengelighet og robusthet, jf. styresak 56/2022. *Endret jf. styresak 03/2023: «Vurdere innføring av kriterier for å akseptere risiko i stedet for nivå for akseptabel risiko»*	a)	Implementere forslag til *risikoakseptkriterier* i styrende dokument «Prosessbeskrivelse risikostyring»	Utfør helhetlig risikostyring	8 før 4 Q4-23
		b)	Fastsette nivå for akseptabel risiko for konfidensialitet, integritet, tilgjengelighet og robusthet,	SIP-Vedlegg 2	Q4-23
5.	Etablere prosessbeskrivelse for forvaltning av databehandleravtaler.	a)	Etablere prosessbeskrivelse for forvaltning av databehandleravtaler	Behandling av personopplysninger og SIP-Vedlegg 4	Sammen med 7 Q4-23
6.	Etablere prosessbeskrivelse for forvaltning av protokoll over behandling av personopplysninger.	a)	Etablere prosessbeskrivelse for forvaltning av protokoll over behandling av personopplysninger	Behandling av personopplysninger	Q2-23
7.	Inngå databehandleravtale der det mangler, og revidere/oppdatere databehandleravtaler inngått før personopplysningsloven ble endret i juli 2018.	a)	Identifiser avtaler med behov for databehandleravtale	Oversikt over databehandleravtaler	Sammen med 5 Q4-23
		b)	Inngå databehandleravtale der det er identifisert behov og hvor dette mangler		Q4-23
		c)	Oppdatere databehandleravtaler inngått før juli 2018		Q4-23
8.	Etablere og/eller revidere prosessbeskrivelser for sentrale aktiviteter i internkontrollen for informasjonssikkerhet og personvern, herunder: risiko- og sårbarhetsanalyser, personvernkonsekvensutredninger, risikohåndtering, gjennomføring av sikkerhetstiltak, og ledelsens gjennomgåelse.	a)	Etablere prosessbeskrivelse for risiko- og sårbarhetsanalyse for informasjonssikkerhet		Q3-23
		b)	Etablere prosessbeskrivelse DPIA		Q3-23
		c)	Revidere prosessbeskrivelse for risikohåndtering	Utfør helhetlig risikostyring	Q4-23
		d)	Etabler prosessbeskrivelse for gjennomføring av sikkerhetstiltak	Behandling av personopplysninger	Q4-23
		e)	Revidere prosessbeskrivelse for ledelsens gjennomgåelse	Utfør ledelsens gjennomgåelse	Q4-23

3. Anbefaling

Administrerende direktør fremlegger forslag til handlingsplan som omfatter tiltak med estimert gjennomføringstid for å imøtekomme alle åtte forbedringsforslag fra revisjonsrapporten.

Styret inviteres med dette til å godkjenne handlingsplan for oppfølging av «*Internrevisjonsrapport 01/2022 - Informasjonssikkerhet og personvern – Fase 1»* slik det er redegjort for i denne saken.

Trykte vedlegg

- Internrevisjonsrapport 01/2022 - Informasjonssikkerhet og personvern – Fase 1