

## Saksframlegg

Saksgang:

Styre	Møtedato
Styret i Sykehusapotekene HF	28. februar 2022

**SAK NR 006-22**

**TEMASAK: INFORMASJONSSIKKERHET SAHF, MED FOKUS PÅ INTERNREVISJON**

***Forslag til vedtak:***

1. Styret tar status på informasjonssikkerhetsområdet og innretning på internrevisjon til orientering.

Oslo, 21. februar 2022

Tore Prestegard  
Administrerende direktør

## 1. Hva saken gjelder

I saken blir det orientert om status på informasjonssikkerhetsområdet, med fokus på internrevisjon.

## 2. Hovedpunkter

### 2.1 Status

Ved forrige gjennomgang for styret, i juni 2021, ble det tegnet et bilde av informasjonssikkerhetsområdet i SAHF der tilstanden var vurdert som relativt god (ref modenhetsmålingen i styresak 034-21). Informasjonssikkerhetsleder har siden da sluttet, og det mest prioriterte på området har vært ivarettatt gjennom løpende arbeid hos IT-drift og ved innleid informasjonssikkerhetsressurs fra Sykehuspartner (40%). De pågående store prosjektene har hatt behov for noe støtte på området. Utover dette har innleid ressurs bistått ved behov på enkeltområder.

Ledelsessystemet for informasjonssikkerhet ble gjennomgått i 2021 før informasjonssikkerhetsansvarlig sluttet, og betydelig forenklet og oppdatert for å sikre samsvar med krav fra Helse Sør-Øst RHF og i tråd med tilbakemeldinger fra organisasjonsgjennomgangen (Org 2020).

Det har ikke vært særskilte hendelser i perioden, utover global problemstilling rundt en teknisk svakhet (Log4j) i desember. Sykehuspartner gikk i beredskap som følge av denne situasjonen, og kartleggingsarbeid og nødvendige tiltak ble iverksatt også hos SAHF. Situasjonen ble raskt avklart, og håndtert på en god måte.

I perioden har det vært jobbet aktivt med informasjonssikkerheten som en del av VOSS-prosjektet, der de berørte systemer som skal flyttes over til Sykehuspartner, skal igjennom en prosess med løsningsdesign og ROS. Dette som forutsetning for å kunne tas inn i Sykehuspartners systemportefølje.

Arbeidet har vært viktig i forhold til å løfte fokus og forsikre oss om at de gjeldende løsninger er der de skal være i forhold til regionens sikkerhetskrav. Dette er så langt gjennomført for teknisk infrastruktur for 4 av 17 applikasjoner, med tilfredsstillende resultat. ROS for de resterende er planlagt gjennomført innen utgangen av mars 2022

I forbindelse med Måling av digital sikkerhetskultur utført for resten av foretaksgruppen høst 2021, ble det også gjennomført samme modenhetsmåling blant et tilfeldig utvalg av ansatte hos sykehusapotekene (vedlegg 1). Overordnet viste undersøkelsen at nivået var tilsvarende som for øvrige foretak i foretaksgruppen. De ansatte har god sikkerhetsadferd, og det er liten variasjon mellom ansatte med og uten lederansvar. Rapporten oppsummerer med at det bør fokuseres på å få ledere til å anerkjenne viktigheten av digital sikkerhet, og ledelsen bør i større grad oppfordre til deltakelse på kurs og kompetansehevede tiltak på området. Undersøkelsen er tenkt gjennomført årlig, og årets undersøkelse vil derved stå som baseline for utviklingen på området. For å kunne heve oss på de sentrale områdene som vil påvirke resultatet fra undersøkelsen, vil det kreve at det settes av mer ressurser enn tidligere. Det fordrer også at informasjonssikkerhet i større grad får fokus og prioritet hos ledelsen i foretaket.

For å adressere kompetanse og kultur for informasjonssikkerhet generelt i foretaket vurderes ibruktage av verktøy (Hoxhunt) integrert i mail-løsning for dette formålet.

## **2.2 Rekruttering av Informasjonssikkerhetsansvarlig**

Rekruttering av ny informasjonssikkerhetsansvarlig ble igangsatt vår 2021 og har vært utfordrende. Det har vært to runder med støtte av rekrutteringsbyrå (vår sommer 2021, der byrået bidro med sitt nettverk, og ny prosess oktober 2021 til februar 2022, med byrå som gjennomførte hele prosessen). Status p.t. er at vi ikke har klart å komme i mål med gjennomførte tiltak og vurderer nå hvordan dette skal håndteres fremover.

Inntil videre bistår Sykehuspartner med kapasitet, slik de har gjort siden sommer 2021.

## **2.3 Internrevisjon**

Kvalitetsavdelingen har en prosedyre for internrevisjoner. Den omfatter interne og eksterne revisjoner som utføres av Kvalitetsavdelingen eller på vegne av den. Inntil mai 2021 hadde Systemet for informasjonssikkerhet (SIK) en egen prosedyre for utførelse av informasjonssikkerhetsrevisjoner, men i praksis ble aldri den prosedyren brukt. Den er nå faset ut.

Iht. kvalitetsavdelingens prosedyre for internrevisjoner skal informasjonssikkerhet revideres hvert år på utvalgte forretningsområder/ avdelinger/ sykehusapotek på samme måte som for ytre miljø og HMS. Produksjon i sykehusapotekene revideres i løpet av en treårsperiode. De andre forretningsområdene (Farmasøytiske tjenester, Publikum og Sykehusleveranser) revideres minimum hvert 5. år.

Ulike temaer innenfor informasjonssikkerhet velges etter innspill fra ledelsens gjennomgåelse, registrerte avvik, innspill fra informasjonssikkerhetsansvarlig, kvalitetsledere og fagsjefer.

I 2018, året etter at SIK ble innført i foretaket, ble det utført en systemrevisjon for informasjonssikkerhet hvor 6 av sykehusapotekene og IT på hovedkontoret ble revidert med hensyn til etterlevelse av SIK.

Etter dette har følgende områder inngått i de interne revisjonene som kvalitetsavdelingen utfører:

- Etterlevelse av sikkerhetsinstruks
- Etterlevelse av opplæringen i informasjonssikkerhet
- Etterlevelse av informasjonssikkerhetsrutinene fra Apotekforeningen i avdeling Publikum

I tillegg har enkelte informasjonssikkerhetstemaer også inngått i systemrevisjoner og leverandørrevisjoner som er utført, etter behov.

Som innspill til revisjon av informasjonssikkerhet i 2022, ble informasjonssikkerhetsavvik i 2021 gjennomgått i januar i år. Noen av avvikene er rene informasjonssikkerhetsavvik, andre er relatert til informasjonssikkerhet. Totalt er det registrert 56 avvik i 2021. De fleste av informasjonssikkerhetsavvikene er relatert til avdeling Publikum som i tidligere år.

I det planlagte revisjonsprogrammet for 2022 inngår revisjon av informasjonssikkerhet i avdelingene Publikum og Farmasøytiske tjenester som en integrert del av revisjonene.

Ved avviksgjennomgangen ble det kun observert ett informasjonssikkerhetsavvik relatert til etterlevelse av prosedyre 11290 (Sikkerhetsprinsipper og –krav for IKT-infrastruktur og applikasjoner). Denne prosedyren skal sikre tilfredsstillende informasjons-sikkerhet i

Sykehusapotekene HF's infrastruktur og informasjonssystemer, og sikre at det etableres like god sikring i Sykehusapotekene HF som i Helse Sør-Øst. Dette var uventet lavt. En internrevisjon ble derfor initiert i januar for å verifisere om prosedyre 11290 etterleves av systemeiere og systemansvarlige i foretaket. Revisjonen viste at etterleves av prosedyren for systemene i Sykehusapotekene HF ikke var tilfredsstillende. Prosedyren har vært gjeldende i 3 år. Problemstillingen er satt opp som diskusjonssak for ledermøtet i februar.

Ved avviksgjennomgangen ble det også observert flere informasjonssikkerhetsavvik i forhold til Pasientjournalloven og Helsepersonelloven som stammet fra en selvinspeksjon som var utført på et av sykehusapotekene. Sykehusapoteket hadde utarbeidet en egen sjekklister for selvinspeksjon i Farmasøytiske tjenester med følgende tema: «Oppslag i journal jfr tjenstlig behov, oppbevaring av personsensitiv informasjon samt ivaretagelse av taushetsplikt». Det anbefales at alle sykehusapotekene som har Farmasøytiske tjenester, gjør en selvinspeksjon i forhold til dette. Dette tas opp på kontaktmøtet med kvalitetsledere i mars.

Det vil bli gitt en presentasjon om temaet på styremøtet.

### **3. Administrerende direktørs anbefaling**

Administrerende direktør anbefaler at styret tar innretning av og status i arbeidet med informasjonssikkerhet og internrevisjoner på området til orientering.

1 vedlegg

Vedlegg 1: Måling av digital sikkerhetskultur SAHF desember 2021