Saksframlegg

Referanse

Saksgang:

Styre	Møtedato
Styret Helsetjenestens driftsorganisasjon for nødnett HF	1.juni 2017

SAK NR 30-2017 Tiltaksplan informasjonssikkerhet i HDO

Forslag til vedtak:

1. Styret tar saken til orientering

Gjøvik, 24.mai 2017

Lars Erik Tandsæther
Administrerende direktør

Sak 30-2017 Tiltaksplan informasjonssikkerhet i HDO

1 Administrerende direktørs anbefaling

Administrerende direktør anbefaler at Styret tar saken til orientering

2 Faktabeskrivelse

Styret behandlet i sitt møte 20.april 2017 Plan internrevisjon (sak 22-2017). Styret vedtok:

1. *Styret tar saken til orientering.*
2. *Styret ber samtidig om at tiltaksplan etter revisjon av anskaffelser legges frem for styret til orientering.*
3. *Styret ber videre om at det fremlegges en plan for revisjon av informasjonssikkerhet i HDO på styremøtet i juni.*

Denne saken omhandler pkt. 3 i vedtaket over, og gir Styret en orientering om HDO sitt arbeid med informasjonssikkerhet, med vekt på hva som må forbedres, samt at man presenterer en plan for det videre arbeidet.

Ved ferdigstillelse av nødnettutbyggingen i helsesektoren (trinn 2) vil Akuttmedisinforskriften for helseforetak og kommuner tre i kraft. Videre er HDO som helseforetak tilknyttet Norsk Helsenett SF, og som sådan omfattet av «norm for informasjonssikkerhet». Norm for informasjonssikkerhet helse og omsorgstjenesten (Normen) er et omforent sett av krav til informasjonssikkerhet basert på lovverket

I mai 2018 vil EU-forordningen erstatte Personopplysningsloven «General Data Protection Regulation (GDPR)» og vil stille strengere krav til personvern. Dette aktualiserer HDO sitt fokus på informasjonssikkerhet ytterligere, og er hensyntatt i den pågående prosess.

GDPR stiller nye krav til blant annet:
- innsyn i og sletting av personopplysninger
- behandling av personopplysninger
- informasjon til personer om behandling av personopplysninger
- overføring av informasjon til utlandet

I foretaksmøtet 12.desember 2016 fikk HDO i oppdrag å ivareta eierskapet til alt brukerutstyr og løsninger tilknyttet nødnett i kommune- og spesialisthelsetjenesten. Ivaretakelse av dette eierskapet, samt utviklingen av nødnettløsningene formaliserer HDOs ansvar og rolle ifht lover og forskrifter, og vil kreve at HDO utvikler sitt styringssystem innen informasjonssikkerhet.

3 Status

Styresak 22-2017 la fram en plan for prosessrevisjoner i HDO, og pekte på områder som HDO bør prioritere. Ett av områdene planen pekte på var informasjonssikkerhet. For å kunne ivareta sitt ansvar som eier og forvalter av alt nødnettutstyr og løsninger, ble det i februar 2017 iverksatt et arbeid for en re-etablering av informasjonssikkerhet i HDO. Arbeidet inngår i en aktivitet i prosessen med kontinuerlig forbedring av informasjonssikkerhet i HDO.

Arbeidet ble definert som et prosjekt, og tar utgangspunkt i behovet for å bevisstgjøre, dokumentere, forankre, skape nye og bedre prosedyrer i HDO. Grunnlaget for dette er behovet for informasjonssikkerhet og henvisninger til gjeldende vedtekter, lover og regler. Dette som en konsekvens av HDO sitt utvidede oppdrag etter 1.januar 2017 - som eier og forvalter av nødnett brukerutstyr i kommunehelsetjenesten og spesialisthelsetjenesten.

Det pågående arbeidet i HDO har gjennomført intervjuer, og gjennomført to GAP-analyser for å identifisere avstanden mellom nåsituasjonen i HDO og anbefalt nivå (ref. «norm for informasjonssikkerhet»). De utførte analysene har involvert og inkludert ledere og avdelinger i selskapet. GAP-analysene er splittet i 2 deler:

- «Del-1: Kontrollrom for nødnett»
- «Del-2: HDO, organisasjon, interne-systemer og samhandling».

Metodikken og rammeverktøyet som er lagt til grunn er hentet fra informasjonssikkerhet standardene ISO27001 og ISO 27002, og HDO har benyttet ekstern spisskompetanse i arbeidet. Det er vurdert som hensiktsmessig å benytte noe ekstern spisskompetanse for å løfte HDOs egen kompetanse innen området.

Basert på GAP analysene er det indentifisert et antall anbefalte tiltak. Tiltakene peker i sum på oppbygging av et system for informasjonssikkerhet i HDO («Information Security Management System – ISMS»)

3.1 Plan - målbilde

Resultatene av GAP analysene er grunnlaget for planen som er etablert, og de tiltak som er iverksatt, har som formål å sikre dokumenterte resultater og oppnåelse av anbefalt mål innenfor:

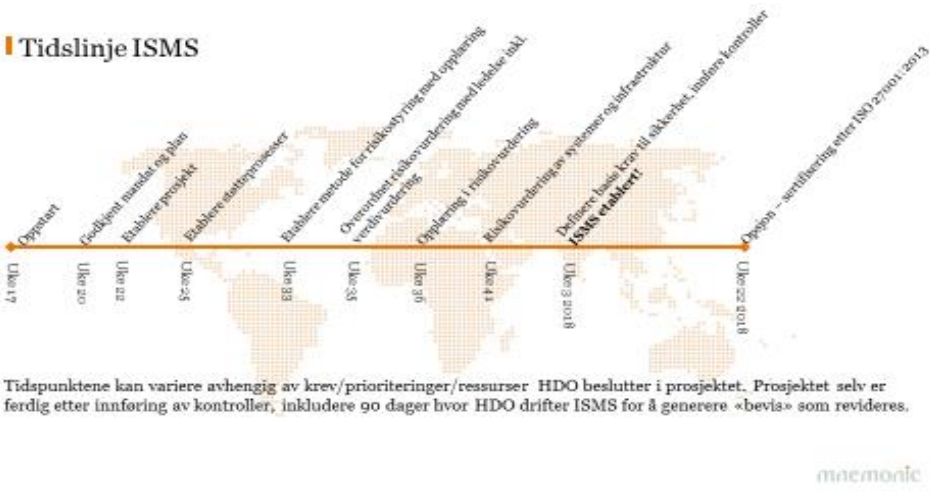
- Informasjonssikkerhetspolicy
- Organisasjon, herunder beredskap.
- Risikovurdering
- Aktiva
- Aksesskontroll
- Kryptografi
- Fysisk sikkerhet
- Drift
- Kommunikasjon
- Informasjonssystemer
- Leverandørforhold
- Hendelseshåndtering
- Ansvaret for samsvar med lover og forskrifter
- Kontinuitet

GAP analysene har pekt på områder som kan forbedres, og en plan for videre aktivitet er utarbeidet.

3.2 Plan for det videre arbeidet inkl. tidslinje.

Arbeidet som nå er iverksatt vil pågå gjennom hele 2017, og med planlagt ferdigstillelse innen uke 22-2018.

Prosjektet jobber med å tydeliggjøre ressursbehov videre, samt legge til rette for god styring og gjennomføring i henhold til planen. Blant annet skal knytningen til de styringsprosesser HDO allerede jobber med videreutvikles, for eksempel virksomhetsplan, rapportering og risikohåndtering.



Etter at dette arbeidet er gjennomført anbefales det at det iverksettes en revisjon av området informasjonssikkerhet i HDO.

4 Administrerende direktørs vurdering

Administrerende direktør mener at det er nødvendig å styrke arbeidet med informasjonssikkerhet i HDO. Ivaretagelse av eierskap og forvaltning av nødnett utstyr krever at HDO formaliserer og styrker seg innen blant annet informasjonssikkerhet. De gjennomførte GAP-analyser peker på områder som HDO må videreutvikle, samtidig som det er viktig å ta vare på den kapasiteten HDO allerede har innenfor området.

Administrerende direktør mener at det iverksatte arbeidet fører til en bevisstgjøring og forsterker fokuset på Informasjonssikkerhet i HDO. Det har blitt jobbet systematisk med analyser, og det er identifisert områder hvor HDO vil iverksette tiltak.

Administrerende direktør er fornøyd med at det ikke er rapportert om sikkerhetsbrudd, men ser også at den videre utviklingen og leveranser av tjenester til kommuner og helseforetak vil stille krav om utvikling av området. Blant annet vil HDO måtte være tydelig på sin håndtering av eventuell journalverdig informasjon, og overholdelse av lover og forskrifter. Eierskapsansvaret for nødnett brukerutstyr og løsninger i helsesektøren tillagt HDO vil medføre at HDO må ha etablert nødvendige kontroll og kompetanse også på informasjonssikkerhet.