SYKEHUSET ØSTFOLD

## Tiltaksplan – konsernrevisjonens gjennomgang av leverandørenes tilgang til helse- og personopplysninger i MTU

# Handlingsplan for oppfølging av anbefalinger etter revisjon av leverandørenes tilgang til helse- og personopplysninger i medisinsk teknologisk utstyr

Ansvarlige ledere for tiltaksplanen:
Bengt Thompson (IKT) og Sverre Granmark (MTA)

| Anbefaling fra konsernrevisjonens rapport | Tiltak | Frist for gjennom-føring | Ansvarlig for gjennom-føring (utøver) | Mål-oppnåelse (%) | Status per 28.4.17 | Videre oppfølging |
|---|---|---|---|---|---|---|
| 1. *Arbeidet med å oppdatere styringssystemet for informasjonssikkerhet ferdigstilles og tilgjengeliggjøres, slik at det danner et grunnlag for informasjonssikkerhet i blant annet MTU.* | 1-1: Arbeidet med Styringssystem for informasjonssikkerhet ferdigstilles i den regionale arbeidsgruppen, tilpasses og innføres i SØ. | 1.10.16 | Lars Cato Skaar | 100 % | Gjennomført | |
| 2. *Etablere en oppdatert sikkerhetsnorm, -standard eller lignende som stiller krav til informasjonssikkerheten i MTU-miljøet* | 2-1: Innarbeide krav til informasjonssikkerhet i kravspesifikasjoner for alle anskaffelser av utstyr som tilkobles datanettverket. Kravene baseres på kravene i Norm for informasjonssikkerhet eller krav fra Sykehuspartner/ SØ dersom sistnevnte er strengere enn normens krav. | 1.7.16 | Lars Cato Skaar | 100 % | Gjennomført | |

| Anbefaling fra konsernrevisjonens rapport | Tiltak | Frist for gjennom-føring | Ansvarlig for gjennom-føring (utøver) | Mål-oppnåelse (%) | Status per 28.4.17 | Videre oppfølging |
|---|---|---|---|---|---|---|
| 3. *Etablere en prosess som sikrer at det ved anskaffelser av MTU stilles krav til informasjonssikkerhet overfor leverandøren og ved vurdering av leverandørens svar.* | 3-1: Informasjonssikkerhetsleder deltar i anskaffelsesprosessen og sørger for at kravene i ovennevnte punkt besvares og oppfylles av leverandør. | 1.9.16 | Lars Cato Skaar og Cecilie Vitting | 100 % | Gjennomført | |
| 4. *Ta i bruk ny mal for avtale om vedlikehold av MTU* | 4-1: Ny mal for avtale om vedlikehold av MTU inngås for fremtidige anskaffelser og alle fremtidige revideringer av leverandøravtaler. | 1.10.16 | Sverre Granmark | 100 % | Gjennomført | |
| 5. *Sykehuset Østfold HF gjennomgår utstyr anskaffet før PNØ og i samarbeid med Sykehuspartner HF utarbeider tjenestebeskrivelser på MTU der det mangler.* | 5-1: Det utarbeides tjenestebeskrivelse på alt MTU som mangler dette. For utstyr som skal erstattes innen 1. halvår 2017, utarbeides det tjenestebeskrivelse på det nye utstyret. | 31.12.16 | Sverre Granmark | 85 % | Ferdig | For utstyr som har integrasjon med annet utstyr eller servere er det utarbeidet tjenestebeskrivelse |
| 6. *Sykehuset Østfold HF følger opp igangsatte aktiviteter for utvikling og implementering av forbedret tekniske løsninger for styring og kontroll med MTU-leverandørenes fjernaksess på sykehusets nettverk.* | 6-1: Sykehuspartner har tilbudt en lokal analyseplattform som inneholder sensorer med mulighet for å overvåke trafikk i VPN. Pristilbudet er ikke akseptert av SØ. Det etterspørres om sensorene kan etableres uten at hele analyseplattformen må anskaffes. | 1.11.16 | Lars Cato Skaar | 75 % | Pågår | Avtale ikke akseptert. Det arbeides med andre løsninger. |
| 7. *Sykehuset Østfold HF gjennomfører alle former for oppfølgingsaktiviteter med* | 7-1: Det etableres rutine for jevnlig gjennomgang i egen prosedyre for: | 15.9.16 | Lars Cato Skaar | 100 % | Gjennomført | |

| Anbefaling fra konsernrevisjonens rapport | Tiltak | Frist for gjennom-føring | Ansvarlig for gjennom-føring (utøver) | Mål-oppnåelse (%) | Status per 28.4.17 | Videre oppfølging |
|---|---|---|---|---|---|---|
| *hensyn til informasjonssikkerhet innenfor MTU-området i henhold til Normen* | ▪ Sikkerhetsrevisjon (årlig)<br>▪ Revisjon av informasjonssikkerhet ved Sykehuspartner<br>▪ Gjennomgang av logger (kvartalsvis)<br>▪ Gjennomgang av autorisasjonsregister (årlig)<br>▪ Risikovurderinger (ved endringer og anskaffelser)<br>▪ Vurdering av risikobilde og oppfølging av tidligere gjennomførte risikovurderinger (årlig)<br>▪ Tilpasning av opplæringsmateriell (årlig) | | | | | |
| | 7-2:<br>Utarbeide organisasjonskart over roller med informasjonssikkerhet | 1.10.16 | Lars Cato Skaar | 100 % | Gjennomført | |
| | 7-3:<br>Det igangsatte arbeidet med å systematisere aggregert risikobilde fra PNØ fortsetter. Risikoelementene registreres i EK Risikomodul for intern oppfølging. | 1.12.16 | Lars Cato Skaar | 80 % | Gjennomført | Aggregert risikobilde ble gjennomgått og oppdatert i desember. Det gjenstår registrering i EK risikomodul. |
| | 7-4:<br>Etablere autorisasjonsregister for alle MTU med individuell pålogging. | 1.12.16 | Sverre Granmark | 100 % | Ferdig | Etablert oversikt over alle som har tilgang til utstyr som krever innlogging |
| | 7-5: | 1.12.16 | Lars Cato | 100 % | Gjennomført | |

| Anbefaling fra konsernrevisjonens rapport | Tiltak | Frist for gjennom-føring | Ansvarlig for gjennom-føring (utøver) | Mål-oppnåelse (%) | Status per 28.4.17 | Videre oppfølging |
|---|---|---|---|---|---|---|
| | Oppdatere opplæringsmateriell og informere opplæringsansvarlige til å eksplisitt informere om krav til informasjonssikkerhet. | | Skaar | | | |
| | 7-6:<br>Informere medarbeidere i MTA om funn i revisjoner og risikobilde. Informasjonen må gis til MTA straks etter at revisjoner er gjennomgått. Det arrangeres en fagdag i august hvor Direktoratet for e-Helse presenterer Veileder for medisinsk utstyr. Dette markerer starten på en kontinuerlig gjennomgang av informasjonssikkerhet for MTU. | 1.9.16 | Lars Cato Skaar | 100 % | Gjennomført | |

Deltagere ved utarbeidelsen:
Lars Cato Skaar
Bengt Thompson
Sverre Granmark