Vedlegg 1.
Regional handlingsplan for Informasjonssikkerhet i Helse Vest.

1. Roller, ansvar og oppgaver

1.1 Informasjonssikkerhet[1] som del av ordinær virksomhetsstyring
Ansvarlig: Hvert foretak i foretaksgruppen[2] Helse Vest, inkl. relevante private, ideelle
Relevant for: Hvert foretak i foretaksgruppen
Tidsperiode: 2021-2022
Beskrivelse: Informasjonssikkerhet skal ytterligere bli en mer integrert del av den ordinære virksomhetsstyringen, der beslutninger om risiko tas i de ordinære ledelseslinjene. Mål og strategi for informasjonssikkerhet stiller krav om at kriterier for å akseptere risiko utarbeides og tas i bruk i arbeidet med risikovurdering og beslutning om risiko. Dette er delvis håndtert i Helse Vest sitt styringssystem for informasjonssikkerhet og personvern, men det er utfordringer med å inkludere risikostyring som en del av ordinær virksomhetsstyring. Rolle og ansvar for Helse Vest RHF bør avklares, herunder også avklaring av rollen som informasjonssikkerhetsleder i Helse Vest RHF.

1.2 Revidere beskrivelser av ansvar og roller
Ansvarlig: Helse Vest RHF
Relevant for: Hvert foretak i foretaksgruppen
Tidsperiode: 2021-2022
Beskrivelse: I styringssystemet for informasjonssikkerhet og personvern skal beskrivelse av ansvar og roller revideres. Ansvars- og oppgavefordeling for medisinsk-teknisk utstyr (MU) og teknisk utstyr (TU) må avklares først, jfr. foregående tiltak og egen styresak om «Styringsstruktur for informasjonssikkerhet».

[1] *Informasjonssikkerhet* handler om å sikre at informasjon i alle former; (1) ikke blir kjent for uvedkommende (konfidensialitet), (2) ikke blir endret utilsiktet eller av uvedkommende (integritet), (3) er tilgjengelig ved behov (tilgjengelighet). *IKT-sikkerhet* er en delmengde av informasjonssikkerhet og fokuserer på teknisk sikring av IKT-infrastruktur og IKT-applikasjoner.

[2] Med foretaksgruppen Helse Vest RHF menes Helse Vest RHF, helseforetakene og Helse Vest IKT AS

1.3 Ansvarsforhold for IKT-sikkerhet for medisinsk utstyr og teknisk utstyr
Ansvarlig: Helse Vest RHF
Relevant for: Hvert foretak i foretaksgruppen, inkl. relevante private, ideelle foretak
Tidsperiode: 2021-2022
Beskrivelse: For medisinsk utstyr (MU) og teknisk utstyr (TU) skal ansvarsforholdet mellom leverandør, helseforetak og IKT-leverandør være avklart. Regional arbeidsgruppe gjennomfører utredning av ansvars- og oppgavefordeling for IKT-sikkerhet knyttet til medisinsk utstyr (MU) og tekniske anlegg (TU). Anbefalinger som drøftes er; - *Nye driftsmodeller med delt forvaltning mellom Helse Vest IKT og avdelingene for MU og TU.* - *Nye sikkerhetstjenester fra Helse Vest IKT til foretakene.* - *Helhetlig sikkerhetsarkitektur for Helse Vest som dekker MU, TU, lokal IKT.* - *Gode og tydelige sikkerhetskrav i anskaffelser av utstyr for MU og TU.*

2. Oversikt, rapportering og oppfølging

2.1 Rapportering av risiko, tilstand og avvik innen informasjonssikkerhet
Ansvarlig: Helse Vest RHF
Relevant for: Hvert foretak i foretaksgruppen, inkl. relevante private, ideelle foretak
Tidsperiode: 2021
Beskrivelse: Rapportering innen informasjonssikkerhet fra helseforetakene og Helse Vest IKT som en del av ordinær rapportering skal styrkes, slik at Helse Vest RHF får bedre styringsinformasjon innen informasjonssikkerhet og bedre innsikt i risikobildet. Avklare rollen til Helse Vest RHF for å styrke styring og kontroll, herunder også avklaring av rollen som informasjonssikkerhetsleder i Helse Vest RHF. Regelmessig rapportering av risiko på området bør etableres fra virksomhetene i regionen til det regionale helseforetaket. Forbedring av ROS-prosesser og ROS-verktøy for å styrke risikostyringen, inkludert bedre eierskap og oppfølging av risiko og tiltak og sammenstilling av risiko på virksomhetsnivå.

2.2 Revisjon/etterlevelse av Regionalt styringssystem for informasjonssikkerhet
Ansvarlig: Helse Vest RHF
Relevant for: Foretaksgruppen, inkl. relevante private, ideelle foretak
Tidsperiode: 2021-2022
Beskrivelse: Regionalt IKT-sikkerhetsutvalg bør utarbeide en plan for revisjon av det regionale styringssystemet for informasjonssikkerhet, samt gjennomføre kontrolltiltak vedrørende etterlevelse av styringssystemet. Det regionale IKT-sikkerhetsutvalget må avklare behov for kompetanse og kapasitet for kontinuerlig forbedring av styringssystemet og for gjennomføring av kontrolltiltak.
2.3 Utarbeide og benytte trusselvurderinger
Ansvarlig: Helse Vest IKT

Relevant for: Hvert foretak i foretaksgruppen, inkl. relevante private, ideelle foretak
Tidsperiode: 2022
Beskrivelse: Helse Vest IKT skal bidra inn i årlige trusselvurderinger i samarbeid med relevante aktører fra både privat og offentlig sektor. Helseforetakene skal benytte denne og andre kilder i sitt arbeid med informasjonssikkerhet. Helse Vest IKT skal bidra i det samarbeidet som Sykehuspartner HF og Helse Nord IKT har etablert på dette området, i den hensikt at alle regionene blir representert. Rapporten bør legges fram for alle foretakene i foretaksgruppen Helse Vest, herunder Helse Vest RHF, Helse Vest IKT, helseforetakene og relevante private, ideelle. Dette må være en årlig rapport. Foretakene skal legge trusselvurderingen til grunn i sitt arbeidet med informasjonssikkerhet.

3. Informasjonssikkerhetskultur og –kompetanse

3.1 Måling av informasjonssikkerhetskultur og gjennomføring av tiltak
Ansvarlig: Helse Vest RHF i samarbeid med helseforetakene
Relevant for: Hvert foretak i foretaksgruppen, inkl. relevante private, ideelle foretak
Tidsperiode: 2021-2022
Beskrivelse: Informasjonssikkerhetskulturen i foretaksgruppen skal måles, og eventuelle tiltak iverksettes med bakgrunn i målingen. Gjennomføre kartlegging av sikkerhetskultur i Helse Vest basert på mal fra Direktoratet for digitalisering (DigDir). Basert på resultatene fra kartleggingen, må det utarbeides relevante tiltak for å styrke sikkerhetskulturen. Det må også gjøres vurdering av behov for å øke kompetansen for ulike grupper av ansatte (medarbeidere, ledere, personell med utvidede rettigheter, mm.) når det gjelder informasjonssikkerhet.

4. Informasjonssikkerhet i anskaffelser

4.1 Informasjonssikkerhetskompetanse i anskaffelser
Ansvarlig: De regionale helseforetakene og Sykehusinnkjøp HF
Relevant for: Hvert foretak i foretaksgruppen
Tidsperiode: 2021-2022
Beskrivelse: For bedre kravstilling og vurdering av informasjonssikkerhet i anskaffelser, skal Sykehusinnkjøp HF benytte kapasitet og kompetanse innen informasjonssikkerhet fra helseregionenes IKT-leverandører. Dette er forankret til det inter-regionale AD-møtet og følges opp av det inter-regionale IKT-direktørmøtet. Resultatene av dette arbeidet må innarbeides i rutiner for anskaffelser i Helse Vest. Tema om anskaffelser må revideres i styringssystemet for informasjonssikkerhet og personvern. Helse Vest IKT AS sine retningslinjer for IKT-sikkerhet skal ligge til grunn for kravene i anskaffelser av IKT i Helse Vest.
4.2 Forvaltning og oppfølging av leverandører til nasjonale og inter-regionale løsninger
Ansvarlig: De regionale helseforetakene
Relevant for: Hvert foretak i foretaksgruppen

Tidsperiode: 2021-2022
Beskrivelse: For inter-regionale anskaffelser bør det pekes på en region for å forvalte området som en anskaffelse omfatter, slik at arbeidet med risikoanalyser og oppfølging av leverandører blir mer effektivt, etter at anskaffelsen er gjennomført.

5. Applikasjoner, IKT-infrastruktur og teknisk sikkerhet

5.1 Grunnprinsipper for IKT-sikkerhet
Ansvarlig: Helseforetak og Helse Vest IKT
Relevant for: Hvert foretak i foretaksgruppen, inkl. relevante private, ideelle foretak
Tidsperiode: 2021-2022
Beskrivelse: Helseforetakene og Helse Vest IKT skal arbeide med systematisk innføring av Nasjonal sikkerhetsmyndighet (NSM) sine grunnprinsipper for IKT-sikkerhet versjon 2.0. Helse Vest IKT og helseforetakene har i oppdrags- og bestillingsdokument for 2021 fått i oppdrag å videreføre arbeidet med Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet. Arbeid med innføring av grunnprinsippene pågår. Innføring av NSMs grunnprinsipper pågår med kartlegging av mulig gap og etablering av relevante tiltak i Helse Vest IKT og i enkelte foretak. Det er særlig behov for tiltak knyttet til; - *Oversikter over IKT tjenester, systemer og informasjon – inkludert lokal IKT i foretakene* - *Overvåking, deteksjon og håndtering av hendelser gjennom etablering av et «Security Operations Center (SOC)» i samarbeid med Norsk Helsenett SF.* - *Sikkerhetstiltak mellom de ulike virksomhetene i regionen* - *Sikkerhetstiltak mellom ulike kategorier av informasjon og tjenester* - *Kvalitetssikring av sikkerhetskopiering («backup» og «restore/recovery»)* - *Revidere og øve på bruk av Beredskapsplaner*

5.2 Tekniske sikkerhetstiltak i IKT-infrastruktur
Ansvarlig: Helse Vest IKT
Relevant for: Hvert foretak i foretaksgruppen, inkl. relevante private, ideelle foretak
Tidsperiode: 2021 og fremover
Beskrivelse: Infrastrukturmodernisering er et pågående og kontinuerlig arbeid. En viktig del av moderniseringen handler om å redusere kompleksitet i IKT-porteføljen og få mindre teknisk gjeld. Styrket kontroll med nettverk og styrket autentisering er to sentrale områder. Felles IKT infrastruktur i Helse Vest bør utvikles til å ha en sikkerhetsarkitektur som dekker større deler av virksomhetenes behov og er iht god praksis, særlig for beskyttelse mellom de ulike kundegruppene i regionen og mellom ulike kategorier av informasjon og tjenester. Målarkitektur for autentisering og autorisering må være førende for oppgradering av infrastruktur innenfor identitet og tilgangsstyring. Tiltaket bør blant annet sees i sammenheng med - *Status for innføring av NSMs grunnprinsipper for IKT-sikkerhet.* - *Modenhetsmåling i Helse Bergen.* - *Vedvarende arbeid med vurdering av risiko og sårbarheter og risikostyring av tiltak knyttet til IKT-infrastruktur i Helse Vest IKT.* - *Risikovurdering av totalt bortfall av IKT som pågår i Helse Bergen - Hvor lenge kan vi ivareta liv og helse uten IKT? Effektivisering/sentralisering opp mot forsvarlighet.*

5.3 Nye modeller for drift og forvaltning
Ansvarlig: Helse Vest IKT
Relevant for: Foretaksgruppen Helse Vest RHF
Tidsperiode: 2021-2023
Beskrivelse: Felles IKT infrastruktur i Helse Vest bør utvikles til å ha en sikkerhetsarkitektur som dekker større deler av virksomhetenes behov og er iht god praksis, særlig for beskyttelse mellom de ulike kundegruppene i regionen og mellom ulike kategorier av informasjon og tjenester. Nye modeller for drift og forvaltning må etableres for å muliggjøre felles forvaltning, der Helse Vest IKT og virksomhetene samarbeider om forvaltning av ulike komponenter, særlig for medisinsk utstyr (MU) og teknisk utstyr (TU).

5.4 Tiltak for å sikre samsvar med styringsstruktur for IKT-sikkerhet
Ansvarlig: Helse Vest RHF, Helse Vest IKT og helseforetakene
Relevant for: Foretaksgruppen Helse Vest RHF
Tidsperiode: 2021-2023
Beskrivelse: Ansvar og styringsmyndighet for IKT-sikkerhet er drøftet i en egen styresak. Saken er lagt frem for styret i Helse Vest RHF, og deretter lagt frem for behandling i styrene for helseforetakene. Gitt vedtak som foreslått, vil det være nødvendig å gjennomføre tiltak for å bringe omfanget av lokal IKT i tråd med styringsstrukturen, samt gjennomføre relevante tiltak knyttet til medisinsk utstyr (MU) og teknisk utstyr (TU). Tiltaket må gjennomføres i tett samarbeid mellom Helse Vest IKT og helseforetakene.

5.5 Sikkerhetsrevisjon av Helse Vest IKT
Ansvarlig: Helse Vest IKT
Relevant for: Foretaksgruppen, inkl. relevante private, ideelle foretak
Tidsperiode: 2022-2023
Beskrivelse: En sikkerhetsrevisjon omfatter kontroll og verifikasjon av nødvendige sikkerhetstiltak (både prosesser og tekniske løsninger) i virksomheten, og skal gjennomføres jevnlig. Helse Vest IKT, som regionens felles tjenesteleverandør av IKT-infrastruktur og IKT-tjenester, bør etablere kompetanse og kapasitet for å kunne gjennomføre sikkerhetsrevisjon. Det bør også vurderes om slike sikkerhetsrevisjoner skal etterspørres fra eller gjennomføres for utvalgte underleverandører til Helse Vest IKT. Helse Vest IKT må vurdere behov for intern kapasitet på sikkerhetsrevisjon.