

Regional handlingsplan for informasjonssikkerhet 3.0 2024 -2027

	Saksnummer Elements:	Versjon: 3.0
Behandlet dato:	Behandlet av: Adm. direktør	Utarbeidet av: Helse Nord RHF
Beslutning: <i>1. Styret i Helse Nord RHF tar foreslåtte endringer i regional plan for informasjonssikkerhet versjon 3.0, til orientering.</i> <i>2. Styret i Helse Nord RHF tar overordet årlig status for de ulike tiltakene i Handlingsplan for informasjonssikkerhet 2024-2027 til orientering.</i>		

Godkjent i styremøte 29.10.2025

Sak 109-2025

Innhold

1. Innledning.....	3
1.1. Formål	3
1.2. Oppfølging av regional handlingsplan	4
1.3. Lokale handlingsplaner	4
2. Innsatsområde organisasjon	4
2.1. Sikkerhetsstyring.....	4
2.2. Sikkerhetsorganisering	5
2.3. Gjennomføre verdivurdering	5
2.4. Risikostyringsprosesser og sammenstilling av risiko på virksomhetsnivå	6
2.5. Sikkerhet i anskaffelser	6
2.6. Modenhetsvurderinger.....	7
2.7. Sikkerhetsrevisjoner.....	8
2.8. Håndtere og gjenopprette.....	8
3. Innsatsområde teknologi (Infrastruktur og teknisk IKT sikkerhet).....	9
3.1. Forsvarlig sikkerhet etter sikkerhetsloven	10
3.2. Styrket robusthet i IKT infrastruktur.....	10
3.3. Oppfølging av målbilde for sikkerhet 2030	10
3.4. Understøtte digital strategi 2038	11
3.5. Oppfølging av gjennomførte forbedringsaktiviteter og revisjoner	11
3.6. Kontinuerlig forbedring	12
3.7. Statistisk logganalyse	14
4. Innsatsområde sikkerhetskultur og –kompetanse (mennesket).....	14
4.1. Utarbeide og benytte trusselvurdering.....	15
4.2. Opplæring/ kompetanse.....	15
4.3. Personellsikkerhet.....	16
4.4. Delta aktivt i nasjonale og regionale samarbeidsforum	17
4.5. Kartlegging av digital sikkerhetskultur.....	17

1. Innledning

1.1. Formål

Formål med regional handlingsplan for informasjonssikkerhet 3.0 er å gi en oversikt over innsatsområder, initiativer og tiltak som skal realisere regionale sikkerhetsmål og sikkerhetsstrategi i perioden frem mot 2027. Begrunnelsen for valg av tiltak forutsettes kjent og omtales ikke nærmere i denne versjonen av dokumentet.

I Regionalt styringssystem for informasjonssikkerhet (DS6121 og MS 0318) er regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet beskrevet:

1. Helse Nord skal ha målrettet sikkerhetsstyring gjennom god internkontroll (kvalitetsforbedring/ledelseskontroll) og robuste informasjonssystemer, som bidrar til effektiv og god pasientbehandling.
2. Helse Nord skal ha prosesser og tekniske løsninger som understøtter sikker og forsvarlig deling av relevant informasjon til forskning, utdanning og opplæring, nasjonalt og internasjonalt.
3. Helse Nord skal ha motstandsdyktighet mot, kunne avdekke og håndtere avanserte digitale angrep.
4. Helse Nord skal bruke trussel-, risiko- og verdibasert[4] sikring av IKT infrastruktur, systemer og tjenester, som ivaretar tilgjengelighet, integritet, konfidensialitet og robusthet.
5. Helse Nord skal inkludere informasjonssikkerhet i virksomhetskulturen[5]. I Helse Nord skal alle medarbeidere gjøre bevisste valg og bidra til åpenhet og kontinuerlig forbedring innenfor sikkerhetsområdet

Regional handlingsplan for informasjonssikkerhet skal bidra til målrettet og samordnet innsats for å sikre tilfredsstillende informasjonssikkerhet i alle tjenester og løsninger som tilbys, og etterlever de krav som følger av personopplysningsregelverket, nasjonal sikkerhetslov og digitalsikkerhetslov. Etter hvert som annet relevant regelverk, som eks «AI ACT», trer i kraft skal dette også etterleves i Helse Nord.

Informasjonssikkerhetsarbeidet skjer i samspillet av tiltak for å bedre organisasjon og arbeidsprosesser, applikasjoner, infrastruktur og teknisk sikkerhet, samt kunnskap, kompetanse, og bevissthet hos medarbeidere. Handlingsplanen har derfor tiltak innen innsatsområdene: organisasjon, teknisk sikkerhet og infrastruktur, samt mennesket.

Arbeidet med informasjonssikkerhet skal være risikobasert. Det vil derfor gjøres fortløpende vurderinger om behov for ytterligere tiltak for å oppnå akseptabelt risikonivå, sammenliknet med trusselbilde og øvrig risiko. Det skal derfor minimum årlig foretas justeringer i handlingsplanen i gyldighetsperioden.

1.2. Oppfølging av regional handlingsplan

Frem til nå har regional handlingsplan vært fulgt opp av en regional styringsgruppe. Det er foreslått at digitaliseringsstyret fremover overtar ansvaret for oppfølgingen.

Gjennomgang av status for måleindikatorerne skal skje gjennom oppfølgingsmøtene mellom Helse Nord RHF og helseforetakene.

1.3. Lokale handlingsplaner

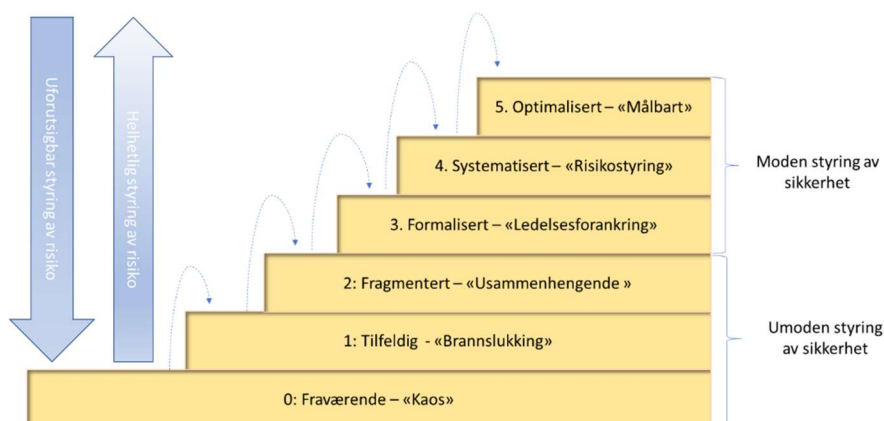
Alle helseforetakene har utarbeidet en handlingsplan for arbeidet med informasjonssikkerhet, som årlig oppdateres og presenteres for eget styre og for Helse Nord RHF.

De lokale handlingsplanene skal understøtte, og operasjonalisere (f.eks. gjennom en tiltaksliste) de ulike prinsippene/ tiltakene som er beskrevet i denne planen.

2. Innsatsområde organisasjon

Helse Nord skal ha et helhetlig arbeid med styring og kontroll. Uavhengig av ulike fagområder vil aktivitetene som gjennomføres for å ha styring og kontroll være ganske like. En helhetlig tilnærming til sikkerhetsstyring tar utgangspunkt i den samme strukturen som benyttes når man bygger styring og kontroll på ulike områder. Implementering av det regionale styringssystemet for informasjons-sikkerhet, herunder sikkerhetsstyringen, må skje i helseforetakene.

Graden av sikkerhet i en virksomhet kan ikke måles direkte. Derimot kan graden av sikkerhet måles indirekte ved å vurdere kvaliteten i prosessene som inngår i arbeidet med informasjonssikkerhet, f.eks. sikkerhetsstyring og risikostyring, ref. figur 1.



Figur 1- modenhet i styring av sikkerhet

Modellen illustrerer ulike grader av modenhet for styring av sikkerhet. Helse Nords ambisjon er å være på modenhetsnivå 4 og bør innenfor noen områder tilstrebe seg å komme opp til nivå 5.

2.1. Sikkerhetsstyring

Formål:

Handlingsplan for informasjonssikkerhet

Sikkerhetsstyringen er avgjørende for at riktige tiltak identifiseres og implementeres. Svakheter i sikkerhetsstyringen kan føre til at kjente sårbarheter og svakheter forblir åpne. Formålet med sikkerhetsstyringen er å medvirke til at bruken av IKT i Helse Nord på en best mulig måte realiserer virksomhetens samlede mål, er kostnadseffektiv og er i samsvar med lover og regler.

Beskrivelse av prinsipp/tiltak:	Helseforetakene må legge til rette for at både ansvar og oppgaver innen sikkerhet på strategisk, taktisk og operativt nivå ivaretas. Ledelsen, og spesielt mellomlederne, må ta eierskap, sette klare forventninger og disponere tilstrekkelig tid og ressurser til å ivareta sikkerhet i daglig drift/arbeidsoppgaver.
Ansvarlig:	Helseforetakene
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Sikkerhet er integrert i virksomhetsstyringen. 2. Ledelsens styring og oppfølging av eget ansvarsområde gjennomføres. 3. Helseforetakene har iverksatt tiltak slik at ledere, mellomledere og ansatte forstår sin rolle, og følger opp krav og retningslinjer/aktivitetene i det regionale styringssystemet 4. Helse Nord RHF følger opp helseforetakenes sikkerhetsstyring 5. Sikkerhetsprosesser i leveranser fra prosjekter til linjen skjer i henhold til fastsatt metodikk i styringslinjen (når det fremkommer hva prosjektleder er ansvarlig for, og hva og hvem i linjen som er ansvarlig).

2.2. Sikkerhetsorganisering

Formål:

Helseforetakene skal ha tilfredsstillende informasjonssikkerhet basert på vurdering av risiko og sårbarhet, og oppfølging gjennom styringssystemet for ledelse og kvalitetsforbedring (internkontroll).

Det enkelte helseforetak, har et selvstendig og overordnet ansvar for at informasjonssikkerheten blir ivaretatt i henhold til gjeldende krav som er beskrevet i regionalt styringssystem for informasjonssikkerhet; RL6911, med flere.

Beskrivelse av prinsipp/tiltak:	Helseforetakene skal beskrive sikkerhetsorganiseringen i eget dokument. Ansvar, roller og rapporteringsrutiner skal være tydeliggjort. Det overordnede ansvaret ligger hos administrerende direktør i helseforetaket.
Ansvarlig:	Helseforetakene
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Helseforetakene har implementert egnet sikkerhetsorganisering i egen virksomhet 2. Lokal og regional sikkerhetsorganisering er inkludert i øvrig virksomhetsstyring

2.3. Gjennomføre verdivurdering

Formål:

Handlingsplan for informasjonssikkerhet

Helse Nord skal ha oversikt over verdier som har betydning for pasientbehandlingen. Formålet er å identifisere de viktigste verdiene, kritikalitet og potensielle risikoområder som foretaksgruppen bør være spesielt oppmerksom på i risikovurderingen og risikohåndteringen. De viktigste verdiene skal sikres først.

Beskrivelse av prinsipp/tiltak:	Helse Nord IKT skal etablere regional forvaltning for verdivurdering av IKT-system. Vedlikehold og utvikling av verdivurderingen skal skje i samarbeid med helseforetakene som bruker systemene.
Ansvarlig:	Helse Nord IKT
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Helse Nord IKT har etablert regional forvaltning, 2. Regional rangering av verdier som har størst betydning for pasientbehandlingen er utarbeidet, og dette er tilsluttet fra sykehusforetakene/SANO. 3. Utarbeidet og tatt i bruk prosesser for å oppdatere med nye verdier 4. Helse Nord IKT operasjonaliserer vedtatt verdivurdering, og følger opp avhengigheter i IKT infrastrukturen.

2.4. Risikostyringsprosesser og sammenstilling av risiko på virksomhetsnivå

Formål:

Helhetlig risikostyring skal bidra til å forbedre organisasjonens evne til å oppnå fastsatte mål. Foretakene i Helse Nord skal ha kontroll på, og styring med, de risikoer foretakene står overfor på kort og lang sikt. Forhold eller hendelser som inntreffer og påvirker måloppnåelsen kan ha negative konsekvenser, positive konsekvenser eller begge deler.

Beskrivelse av prinsipp/tiltak:	Helseforetakene må legge til rette for at sikkerhet blir en del av den helhetlige risikostyringen.
Ansvarlig:	Helseforetakene
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Sikkerhet er en integrert del av regional risikostyringsprosess 1. Konsekvenskriterier for gjennomføring av risikovurdering er regionalisert. 2. Risikovurderinger utarbeidet i den enkelte foretak skal deles med foretaksgruppen. I Helse Nord har vi en felles infrastruktur, og risiko i et foretak kan påvirke hele foretaksgruppen.

2.5. Sikkerhet i anskaffelser

Formål:

Helse Nord må sørge for at alle som gjennomfører anskaffelser har tilstrekkelig sikkerhetskompetanse. Applikasjoner og medisinsk utstyr er i større grad enn tidligere koblet til nettverket. Dette krever at både utstyr har tilstrekkelig sikkerhet, og at utstyr støtter de sikkerhetsmekanismer som finnes i Helse Nord sitt nettverk. Utstyr og tjenester som anskaffes må også forvaltes gjennom hele livssyklusen. Anskaffelser på nasjonalt og regionalt nivå som erstatter lokale anskaffelser kan bidra til å øke sikkerhetsnivået.

Handlingsplan for informasjonssikkerhet

Ved anskaffelser som gjelder nasjonal sikkerhet gjelder kravene i nasjonal sikkerhetslov i tillegg til lov og forskrift om offentlige anskaffelser, og da skal prosedyre for anskaffelser omfattet av sikkerhetsloven følges (sjekkliste utviklet av Helse Nord IKT- juridisk).

Beskrivelse av prinsipp/tiltak:	Administrerende direktører i de regionale helseforetakene har besluttet at kravene til informasjonssikkerhet i anskaffelser skal dekkes ved å benytte regionens informasjonssikkerhetsmiljø. I Helse Nord skal dette skal ivaretas gjennom Helse Nord IKT. Antall lokale anskaffelser skal reduseres, og anskaffelsene skal primært være nasjonal eller regionale. For anskaffelser omfattet av sikkerhetsloven skal egen prosedyre/sjekkliste følges.
Ansvarlig:	Helseforetakene
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Sikkerhet er tilstrekkelig ivaretatt i regionale og nasjonale anskaffelser 2. Utarbeide kompetanseløp mht sikkerhet i anskaffelser 3. Leverandører følges opp gjennom hele produktets/tjenestens levetid. 4. HN RHF skal monitorere alle anskaffelsene. Anskaffelser gjennom Clockwork skal ha en avtalekode (SI-kode). 5. Prosedyre for anskaffelser omfattet av sikkerhetsloven skal brukes og følges. 6.

2.6. Modenhetsvurderinger

Formål: Modenhetsvurdering av implementering av NSM grunnprinsipper for IKT sikkerhet skal bidra til å øke bevisstheten om informasjonssikkerhet og gi tilgang til en standardisert regional modenhetsvurdering. Modenhetsvurderingen er en egenvurdering gjennomført av hvert helseforetak. Vurderingen er et godt utgangspunkt, sammen med andre verktøy, for å gi en samlet regional vurdering, og for å foreslå og iverksette risikoreduserende tiltak, og justeringer av lokal/ regional handlingsplan for informasjonssikkerhet.

Beskrivelse av prinsipp/tiltak:	Helseforetakene skal gjennomføre, og videreutvikle prosess for å vurdere egen modenhet av implementering av NSMs grunnprinsipper for IKT sikkerhet (prioritet 1 & 2)
Ansvarlig:	Helseforetakene
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Helseforetakene har dokumentert egenvurdering av modenhet for tiltakene. 2. Helse Nord RHF har sammenstilt en samlet regional vurdering. 3. Modenhetsvurderingen gjennomføres av eksterne (hvert 2. eller 3. år.) 4. Når det er foreslått tiltak/justeringer av lokal og regional handlingsplan

2.7. Sikkerhetsrevisjoner

Formål:

Regionale sikkerhetsrevisjoner er et ledd i kvalitetsarbeidet i foretaksgruppen, og et kjerneelement i det regionale styringssystemet. Formålet med en sikkerhetsrevisjon er å verifisere at Helse Nord etterlever egne krav til informasjonssikkerhet og personvern. Det skal gjennomføres både lokale, regionale og inter-regionale sikkerhetsrevisjoner. Siste nevnet er et samarbeid mellom helseregionene for å gjennomføring av sikkerhetsrevisjoner av felles leverandører.

Beskrivelse av tiltak:	Videreutvikle og gjennomføre regionale sikkerhetsrevisjoner
Ansvarlig:	Avdeling sikkerhet og beredskap
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Når revisjoner i regional revisjonsplan er gjennomført 2. Når revisjoner i inter – regional revisjonsplan er gjennomført 3. Når revisjoner følges opp

2.8. Håndtere og gjenopprette

2.8.1. Håndtering av IKT beredskapshendelser

Formål:

Helse Nord skal styrke regional beredskap og evne til hendelseshåndtering, slik at digitale hendelser oppdages hurtig, kontrolleres, skaden minimeres og hendelsesårsaken fjernes effektivt. Dette omfatter også evnen til gjenoppretning og sykehusenes evne til å yte helsetjenester.

Beskrivelse av tiltak:	Delplan regional beredskapsplan IKT er et rammeverk for IKT beredskapsarbeidet i foretaksgruppen. Helse Nord IKT er ansvarlig for å utarbeide planer for tekniske håndtering og gjenoppretting ved reduksjon og bortfall av IKT for inntil 7 døgn. Sykehusforetakene skal ha planer for håndteringen av pasientbehandlingen ved reduksjon og bortfall av IKT for inntil 7 døgn. Kravet er også gitt i styringskrav og rammer 2024. Det skal suksessivt arbeides med å definere og etablere reserveløsninger for de mest kritiske tjenestene som har betydning for pasientbehandlingen, jf punkt2.3.
Ansvarlig:	Helseforetakene / Helse Nord IKT/ Helse Nord RHF
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Når reserveløsninger for de mest kritiske tjenester som har betydning for pasientbehandlingen er definert. 2. Styringskrav og rammer er innarbeidet i lokalt beredskapsplanverk. 3. IKT beredskapshendelser er håndtert i henhold til regional beredskapsplan IKT.

2.8.2. Øvelser

Formål:

Den digitale sikkerheten utsettes stadig for nye trusler og sårbarheter. For å øke bevisstheten og for å være bedre rustet til å håndtere digitale sårbarheter skal Helse Nord ha øvingsplan som sikrer at hele foretaksgruppen har gjort nødvendige øvelser for reduksjon og totalt bortfall av IKT.

Handlingsplan for informasjonssikkerhet

Beskrivelse av tiltak:	Helse Nord RHF skal sammenstille en overordnet øvingsplan for reduksjon og totalt bortfall av IKT. Helseforetakene skal ha egne lokale øvingsplaner.
Ansvarlig:	Helseforetakene
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Planlegge iverksetting av nødvendige øvelser 2. Helseforetakene har utarbeidet lokale øvingsplaner, og oversendt disse til Helse Nord RHF. 3. Helse Nord RHF har sammenstilt dette til en regional øvingsplan, og denne er publisert. 4. Øvelser i øvingsplan er gjennomført

2.8.3. Evaluering av hendelser og øvelser

Formål:

Hva kan vi som virksomhet lære av denne hendelsen/øvelsen? Hvordan kan vi bruke lærdommen fra denne hendelsen/øvelsen til å forebygge, og til å bedre håndteringen av kommende hendelser?

Beskrivelse av tiltak:	Helseforetakene skal evaluere alle IKT beredskapshendelser, og øvelser. Læringspunkter skal ledelsesforankres og innarbeides i egen tiltaksplan for oppfølging. Evalueringer skal sendes til Helse Nord RHF.
Ansvarlig:	Helseforetakene
Måleindikator (Når kan tiltaket anses å være fullført?)	1. IKT beredskapshendelser/øvelser er evaluert. 2. Helseforetakene skal oversende egen evaluering til Helse Nord RHF. 3. Når resultater fra øvelser og fulgt opp, og det er gjort nødvendige tilpasninger i relevante beredskapsplaner.

3. Innsatsområde teknologi (Infrastruktur og teknisk IKT sikkerhet)

Helse Nord skal arbeide med teknologiske sikkerhetstiltak etter en risikobasert metodikk, der prinsippet om sikkerhet i dybden står sentralt. Dette følger i stor grad tråden til oppbygningen av de ulike kategoriene til NSM grunnprinsipper, og definisjonen slik den er definert for fysiske tiltak gjennom barrierer, deteksjon, verifikasjon og reaksjon. For Helse Nord handler sikkerhet i dybden om å ha et helhetlig fokus på sikkerhet, og at teknologiske tiltak dimensjoneres sammen med menneskelige og organisatoriske tiltak sett opp mot den vurderte risikoen.

Helse Nord IKT har etablert en sikkerhetsportelje som skal legge til grunn en strukturert tilnærming for, og anbefaling av fremtidige sikkerhetsinitiativ. Dette med bakgrunn i behov avdekket gjennom modenheitsvurderinger, målinger, handlingsplaner sett opp imot etablert målbilde for sikkerhet og målarkitekturer. Nye initiativ vil besluttes gjennom områdestrukturen som rapporterer til Digitaliseringsstyret.

3.1. Forsvarlig sikkerhet etter sikkerhetsloven

Formål:

Det er utpekt fysiske og logiske skjermingsverdige objekter etter sikkerhetsloven i Helse Nord. Det skal etableres forsvarlig sikkerhetsnivå for de utpekte verdiene.

Beskrivelse av tiltak:	Gjennomføre systematisk arbeid for å opprettholde forsvarlig sikkerhetsnivå på utpekte ugraderte skjermingsverdige objekter i helseforetakene.
Ansvarlig:	Helse Nord RHF og Helseforetakene
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Sikringsrisikovurdering på utpekte objekter et gjennomført eller oppdatert inneværende år, nødvendige tiltaksforslag er utarbeidet. 2. Tiltak er besluttet i aktuell styringslinje hos objekteier. 3. Status på gjennomføring av besluttede tiltak rapporteres til ledelse hos objekteier. RHF informeres på status minst årlig.

3.2. Styrket robusthet i IKT infrastruktur

Formål:

I styringsrammer og krav 2024 er det gitt økte krav til robusthet ift helseberedskap.. Det må etableres robusthet i design og konfigurasjon av infrastrukturen for å styrke evnen til kontinuitet ved hendelser.

Beskrivelse av tiltak:	Etablere robust IKT infrastruktur som sikrer en forsvarlig drift selv ved utfall av kommunikasjonslinjer.
Ansvarlig:	Helse Nord IKT
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Det er etablert aktivitet for å designe ny arkitektur for å ivareta robusthet for IKT infrastruktur. 2. Det er etablert mulighet for tilfredsstillende «break-out»/internett-tilgang fra lokal infrastruktur.

3.3. Oppfølging av målbilde for sikkerhet 2030

Formål:

Et oppdatert målbilde for sikkerhet skal gi føringer for å etablere kontroll og sikkerhet i regional infrastruktur.

Beskrivelse av tiltak:	Utarbeide målbilde for informasjonssikkerhet mot 2030, som skal gi føringer for oppgradering av sikkerhet i IKT infrastruktur og løsninger/tjenester, for å sikre en enhetlig retning på sikkerhetsarbeidet relatert til IKT i regionen.
Ansvarlig:	Helse Nord IKT
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Målbildet er presentert for relevante styringsorganer i Helse Nord. 2. Målbildet er behandlet i arkitekturråd i HN IKT. 3. Plan for realisering av prioriterte initiativ i tråd med målbilde 2030 er behandlet i områdestyre infrastruktur og sikkerhet

3.4. Understøtte digital strategi 2038

Formål:

Beskrivelse av tiltak:	Digi 2038 skal realisere fremtidens pasientbehandling. Det er viktig med en bevisst og sikker tilnærming til denne digitaliseringen.
Ansvarlig:	Helse Nord IKT
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Rammer og krav for trygg og sikker bruk av skytjenester er etablert 2. Rammer og krav for trygg etablering av KI er etablert 3.

3.5. Oppfølging av gjennomførte forbedringsaktiviteter og revisjoner

3.5.1. Oppfølging av tekniske tester

Formål:

Det gjennomføres årlig ulike tekniske tester på intern infrastruktur. Funn fra disse aktivitetene må ha en målrettet oppfølging.

Beskrivelse av tiltak:	Identifiserte tekniske forbedringsområder og avvik identifisert av bl.a. Riksrevisjonen, HelseCERT og interne sikkerhetsrevisjoner må følges opp helhetlig. Det skal etableres en prosess der HN IKT holder en overordnet oversikt over tekniske oppfølgingstiltak som følge av disse testene.
Ansvarlig:	Helse Nord IKT
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Alle foretak rapporterer fortløpende status på tekniske avvik/tiltak i sitt foretak til HN IKT, iht etablerte rutiner. 2. HN IKT rapporterer minimum kvartalsvis status på oppfølging til foretakene gjennom sikkerhetskoordinatormøter, og halvårlig til FRIS. 3. Behov for nye tiltak/aktiviteter som følge av gjennomførte tester legges frem for områdestyre infrastruktur og sikkerhet og ved behov Digitaliseringsstyret i Helse Nord

3.5.2. Oppfølging av gjennomførte forbedringsaktiviteter og revisjoner

Formål:

Iht regional revisjonsplan og punkt 2.6 og 2.7 i denne handlingsplanen, vil det årlig bli gjennomført modenhetskartlegginger og revisjonsaktiviteter som skal følges opp i tråd med dette tiltaket. Andre testaktiviteter som gjennomføres som del av den kontinuerlige sikkerhetstesting skal også systematisk følges opp.

Beskrivelse av tiltak:	Identifisere og sette i gang nødvendige tekniske tiltak etter utførte internrevisjoner, egen sikkerhetstesting eller andre kontrollaktiviteter.
Ansvarlig:	Helse Nord IKT (Infrastruktur og plattform og Applikasjonstjenester), Helse Nord RHF (felles administrative), Helseforetak (MTU/BTU)

Måleindikator (Når kan tiltaket anses å være fullført?)	1. Tiltaksplan etter endt revisjon leses tilbake til eier 2. Aktivitet for håndtering av tiltak er iverksatt 3. Besluttete tiltak er avsluttet
--	--

3.6. Kontinuerlig forbedring

3.6.1. Asset management som regionalt enhetsregister

Formål:

For å ivareta god livssyklusforvaltning må Helse Nord ha et regionalt register med oversikt over egne IKT eiendeler.

Beskrivelse av tiltak:	Videreutvikle asset management system til teknisk og prosessuelt å inneha oppdatert oversikt over klienter, servere og MTU enheter. Asset skal fungere som primært enhetsregister.
Ansvarlig:	Helse Nord IKT (forvalte Asset), Alle (bidra med datakvalitet)
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Løpende oversikt over enheter i bruk er tilgjengeliggjort for systemeiere. 2. Løpende oversikt på konfigurasjons- og sårbarhetsstatus er tilgjengelig for systemeiere. 3. Sikkerhetsorganisasjonen presenteres måledata med oversikt over omfang enheter i infrastrukturen som ikke er registrert i Asset.

3.6.2. Løpende oversikt over medisinteknisk utstyr

Formål:

Understøtte kap 3.5.1 med nødvendig informasjon som er registrert i egne registre.

Beskrivelse av tiltak:	Helseforetakene skal ha oversikt over alt medisinsk utstyr som er koblet til digitalt nettverk.
Ansvarlig:	Sykehusforetakene
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Nødvendige opplysninger er registrert og oppdatert i «Asset management». 2. Rapportering på status med arbeid er innarbeidet i tertialrapporter.

3.6.3. Oversikt over brukergrupper og brukere

Formål:

Iht NSM grunnprinsipp 1.3 må Helse Nord ha god livsløpsforvaltning over brukere og deres tilganger i infrastrukturen.

Beskrivelse av tiltak:	Innføre IAM for alle foretak, og ha oversikt over alle privilegerte, og ikke-menneskelige brukere.
Ansvarlig:	Punkt 1 og 2: Alle, punkt 3-5: Helse Nord IKT

Handlingsplan for informasjonssikkerhet

Måleindikator (Når kan tiltaket anses å være fullført?)	1. IAM er tatt i bruk i samtlige foretak for tilganger til arbeidsflater. 2. Implementere regionale retningslinjer for ikke-menneskelige brukere (RPA, systemkontoer, KI, mm). 3. Gjennomført verifikasjon av etablerte system- og servicebrukere og tilganger. 4. Gjennomført verifikasjon* på tildelte brukertilganger på utpekte systemer fra regional verdivurdering. 5. Gjennomført verifikasjon* på at tildelte privilegerte brukertilganger er korrekt i PAM. <i>*Hyppighet kravstilles i styringssystem for informasjonssikkerhet</i>
--	--

3.6.4. Etablere livsløpsforvaltning av applikasjonsporteføljen

Formål:

HN IKT er gitt ansvar for teknisk og merkantil forvaltning av applikasjoner. Oppdraget må operasjonaliseres gjennom livsløpsforvaltning av applikasjonsporteføljen.

Beskrivelse av tiltak:	Ferdigstilling av overføring av teknisk og merkantil forvaltning av applikasjoner til HN IKT.
Ansvarlig:	Helse Nord IKT
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Etablert evne til å gi livsløpstilstand over applikasjonsporteføljen til systemeiere. 2. Det er etablert årlige KPI for omfang av applikasjoner med etablerte prosesser for å motta sikkerhetsoppdateringer. 3. Applikasjoner tilknyttet regional verdivurdering er integrert med sentral loggløsning.

3.6.5. Operasjonalisere portvaktfunksjonen

Formål:

Sikre at nye løsninger som innføres i infrastrukturen er i tråd med kravstillinger og gjeldene risikoappetitt.

Beskrivelse av tiltak:	Videreutvikle prosess og teknisk understøttelse av portvaktfunksjon for å sikre at nye enheter og løsninger tilfredsstiller sikkerhetsmessige krav. (Iht NSM 2.1.1, 2.1.2)
Ansvarlig:	Helse Nord IKT
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Etablert prosess for å ivareta sikkerhetskrav i anskaffelser. 2. Etablert prosess og kapabilitet for godkjenning av sikkerhetstilstanden til nye enheter inn i infrastrukturen. 3. Etablert kapabilitet for sikkerhetsskann av nye enheter. 4. Etablert kapabilitet for å avdekke uautoriserte enheter i infrastrukturen.

3.6.6. Forbedring av gjestenett-løsning i regionen, inkl gjestenett-wifi

Formål:

Handlingsplan for informasjonssikkerhet

Det er ved flere anledninger identifisert behov for å forbedre løsning for gjestenett ved foretakene.

Beskrivelse av tiltak:	Forbedre dagens gjestenettløsning, både kablet og wifi, med tanke på å styrke etterlevelse av sikkerhetskrav
Ansvarlig:	RHF (2)/ HN IKT (1)/ Alle foretak (3)
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Det er implementert avhjelpende (mitigerende) tiltak for permanent utstyr på dagens løsning. 2. Igangsatt aktivitet for å etablere ny løsning. 3. Ny løsning implementert.

3.6.7. Målrettet arbeid med reduksjon av teknisk gjeld

Formål:

I tråd med oppfølging av Riksrevisjonens tekniske test 2019, må det arbeides systematisk med reduksjon av teknisk gjeld, for å forbedre sikkerhetstilstanden.

Beskrivelse av tiltak:	Det skal arbeides målrettet med å redusere andel teknisk gjeld i eget foretak
Ansvarlig:	HNIKT (1,3). Alle foretak (2)
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Det er etablert målinger med definerte årlige måleindikatorer for omfang av teknisk gjeld. 2. Teknisk gjeld i eget foretak inngår i ledelsesrapportering. 3. Antall enheter i kritisk infrastruktur som er EOL = 0. 4. Det er besluttet tiltak i områdestyrer som adresserer teknisk gjeld

3.7. Statistisk logganalyse

Formål:

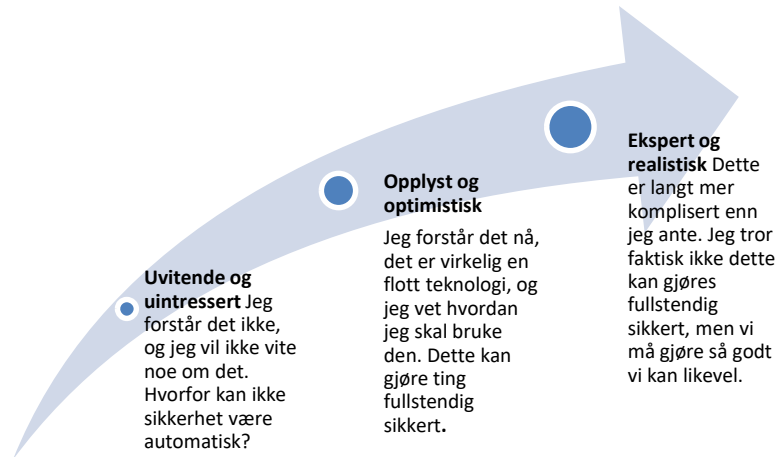
Helse Nord skal ha en tilgangsstyring, logging og etterfølgende kontroll for å hindre urettmessig tilgang til journaler. Antall oppslag i journal er så stort at manuell oppfølging for etterfølgende kontroll i helseforetakene er krevende.

Beskrivelse av tiltak:	Innføre og ta i bruk verktøy for statistisk logganalyse, og prosess for oppfølging av uvanlige oppslag.
Ansvarlig:	Helse Nord RHF
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Når verktøy for statistisk logganalyse er tatt i bruk i Helse Nord

4. Innsatsområde sikkerhetskultur og -kompetanse (mennesket)

Å skape god sikkerhetskultur krever langsiktige og målrettede tiltak slik at alle enkeltindivider utvikler en god sikkerhetsatferd. Dette må kombineres med organisatoriske og tekniske sikkerhetstiltak slik at muligheten for å gjøre feil, og konsekvenser av menneskelige feil, reduseres. Medarbeideres modenhetsutvikling er illustrert i figur 2:

Handlingsplan for informasjonssikkerhet



Figur 2 Stadier av sikkerhetslæring som medarbeidere gjennomgår. Ved å følge tiltakene i handlingsplanen skal medarbeider i Helse Nord få en realistisk oppfatning av hva som er mulig å oppnå med informasjonssikkerhet. Kilde: Gjøsang, og Esponosa: *The smartest person in the Room: The Root Cause and new solution for cybersecurity*

4.1. Utarbeide og benytte trusselvurdering

Formål:

Trusselvurderinger er en viktig del av beslutningsunderlaget innen styring av informasjonssikkerhetsarbeidet.

Beskrivelse av tiltak:	Helse Nord IKT skal utarbeide årlig trusselvurdering sammen med Sykehuspartner HF/ regionene, i samarbeid med Helse- og kommune-CERT. Trusselvurderingen gir et grundig bilde av hvilke digitale trusler spesialisthelsetjenesten står overfor. Trusselvurderingen skal bidra til situasjonsforståelse og lederstøtte, og skal brukes aktivt av alle helseforetak i arbeidet med sikkerhet.
Ansvarlig:	Helse Nord IKT er ansvarlig for å utarbeide trusselvurdering. Alle helseforetak er ansvarlig for å benytte trusselvurdering i eget arbeid.
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Når trusselvurdering er utarbeidet. 2. Når trusselvurdering er tatt i bruk. 3. Når arbeidet med trusselvurdering blir inkludert i risikoarbeidet for sikkerhetsarbeidet i Helse Nord (risikovurderingsarbeidet)

4.2. Opplæring/ kompetanse

Formål:

Kompetanse innen sikkerhet på alle nivåer er et forbyggingselement. Svak sikkerhetsadferd kan utgjøre en vei inn i systemene for en trusselaktør. Arbeidet med sikkerhetskultur og opplæring i Helse Nord skal være en systematisk og kontinuerlig forbedringsprosess. Trusselvurdering i spesialisthelsetjenestens skal ligge til grunn for arbeidet med opplæring og kompetanseutvikling.

Handlingsplan for informasjonssikkerhet

Beskrivelse av tiltak:	Helse Nord RHF må gi en overordnet beskrivelse av kompetansenivå på regionalt nivå. Helseforetakene må ha en tilsvarende beskrivelse på lokalt nivå og iverksette nødvendige tiltak slik at egne medarbeidere forstår sitt ansvarsområde og har tilstrekkelig opplæringen innen sikkerhet.
Ansvarlig:	Punkt 1 og 3: Helseforetakene, punkt 2: Helse Nord RHF, punkt 3: Helse Nord RHF/ Helse Nord IKT
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Når alle ansatte har gjennomført generelle kompetansehevingstiltak innen sikkerhet. 2. Når det er utarbeidet en regional opplæringsplan for sikkerhet. 3. Når det er utarbeidet lokale opplæringsplaner innen sikkerhet for relevante roller 4. Når systemeier/tjenesteeier/bestiller tilbys relevant opplæring 5. Når Helse Nord IKT har tatt i bruk strukturert og automatisert prosess for phishing e-post. Aktiviteten skal ses i sammenheng med e-post sikkerhet.

4.3. Personellsikkerhet

Formål:

Statlige og ikke-statlige trusselaktører bruker metoder for å kartlegge og dra nytte av personer på innsiden av virksomheter. Medarbeidere på innsiden har direkte eller indirekte tilgang til verdier, og i større eller mindre grad tilgang til informasjon som en trusselaktør kan forsøke å utnytte.

Helse Nord skal gjennom risikobasert tilnærming sikre at medarbeidere som innehar høyrisikoroller er identifisert. Tiltak for å forebygge innsidervirksomhet deles inn i tre hovedkategorier: Sikkerhetsklarering, autorisasjon og sikkerhetsmessig ledelse og kontroll. Medarbeidere som innehar stillinger som kan defineres som høyrisikoroller skal gjennomføre kompetansehevende tiltak for å kunne håndtere risiko knyttet til stillingen på en god og forsvarlig måte.

Beskrivelse av tiltak:	Kartlegge høyrisikoroller som har tilgang til virksomhetens viktigste verdier. Risikovurdere stillinger ift hvilken tilgang til sensitiv informasjon som er knyttet til stillingen.
Ansvarlig:	Helse Nord RHF avdeling sikkerhet og beredskap. Helseforetakene.
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Når høyrisiko-roller er identifisert. 2. Når internopplæring om innsidere med fokus på å være en barriere mot sikkerhetstruende virksomhet, er utarbeidet og tatt i bruk. 3. Når HR-avdelingene er involvert i arbeidet slik at det er forankret hos dem som har mest kunnskap om når det rekrutteres, tilsettes og avsluttes.

4.4. Delta aktivt i nasjonale og regionale samarbeidsforum

Formål:

Bidra til og sørge for erfaringsdeling innen digital sikkerhet mellom regionene.

Beskrivelse av tiltak:	Delta i samarbeidsforum for å dele erfaringer mellom HOD, helseregionene, Helsedirektoratet og Norsk helsenett SF. Delta i utvalg for digital sikkerhet.
Ansvarlig:	Helse Nord RHF og Helse Nord IKT
Måleindikator (Når kan tiltaket anses å være fullført?)	Helse Nord deltar på aktuelle lokale, regionale og nasjonale møtefora knyttet til digital sikkerhet. Deltakere i de aktuelle møtefora sørger for erfaringsdeling.

4.5. Kartlegging av digital sikkerhetskultur

Formål:

Det skal fremskaffes informasjon som gir økt innsikt i hvordan den menneskelige faktoren påvirker den digitale sikkerheten, og bedre forståelse av effekten av tiltak som Helse Nord gjennomfører. Formålet er å øke de ansattes bevissthet, holdninger, kunnskaper og adferd innen digital sikkerhet.

Beskrivelse av tiltak:	Kartlegge digital sikkerhetskultur, og følge opp resultatene fra kartleggingen.
Ansvarlig:	Foretaksgruppen
Måleindikator (Når kan tiltaket anses å være fullført?)	1. Når kartlegging av digital sikkerhetskultur er gjennomført 2. Når resultatene er gjennomgått i egen virksomhet og avdeling 3. Når regionale og lokale tiltak er implementert