Regional beredskapsplan for teknologiområdet

*Dette dokumentet erstatter tidligere **Regional IKT-beredskapsplan for Helse Sør-Øst**, og inkluderer både IKT-, MTU- og BTU-tjenester. Dokumentet inngår som en delplan til den regionale beredskapsplanen, på linje med plan for smittevernberedskap og varslingsrutiner ved akutt oppstått mangel på legemidler.*

Innhold

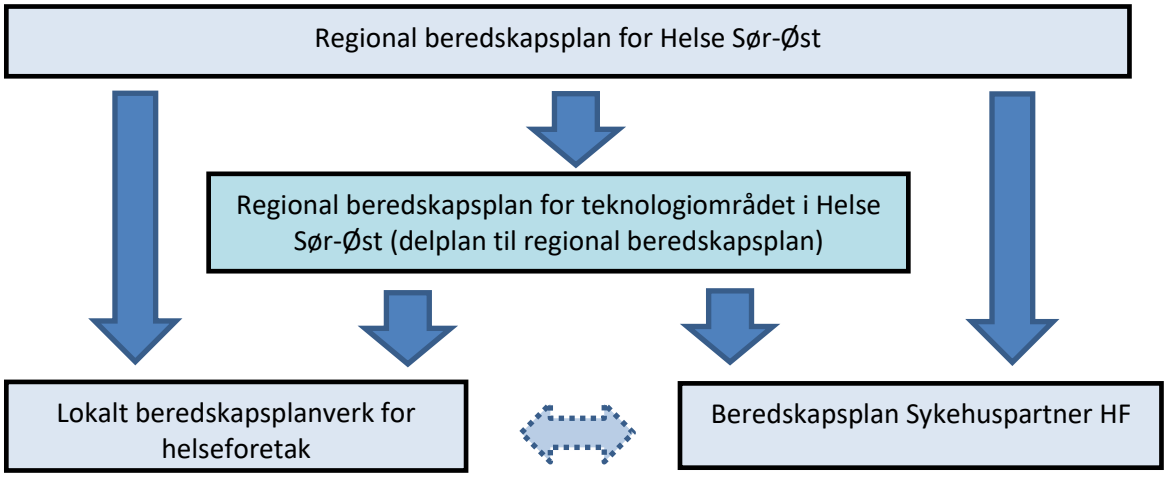
1 Mål, prinsipper og rammer for beredskapsarbeidet

1.1 Formål og retningslinjer

Hensikten med beredskapsplanverket er å sette virksomhetene i Helse Sør-Øst i stand til å håndtere uventede og uønskede hendelser som kan omfatte brudd på tilgjengelighet, konfidensialitet og/eller integritet for informasjon og IKT-tilknyttede systemer. Risikovurderinger har vist at helseteknologi understøtter stadig flere av kjerneprosessene innen spesialisthelsetjenesten. Dette fører til at sårbarheten ved bortfall av helseteknologi tjenester øker, noe som igjen krever effektiv og god håndtering av kritiske IKT-hendelser.

Målet med denne planen er å tydeliggjøre ansvarsområder og grensesnitt mellom berørte juridiske enheter innenfor helseregionen; Helse Sør-Øst RHF, helseforetakene og tjenesteleverandøren Sykehuspartner HF. Alle virksomhetene skal legge til rette for en god sikkerhets- og beredskapskultur der opplæring og øvelser er en del av grunnlaget. Helseforetakene skal gjennomføre egne risikovurderinger for å best kunne utarbeide egnede beredskapsplaner. Beredskapsplanen gir føringer på strategisk og taktisk nivå og definerer roller, ansvarsområder og kommunikasjonsveier nødvendig i beredskap for IKT-infrastruktur, IKT-tjenester og IKT-tilknyttede systemer. (Operativt nivå forutsettes dekket i lokalt beredskapsplanverk for det enkelte helseforetak og beredskapsplan for Sykehuspartner HF.) I dette inngår medisinskteknisk utstyr (MTU) og byggteknisk utstyr (BTU) som tilknyttes lokal eller regional IKT-infrastruktur. De føringer som er lagt i denne planen skal gjenspeiles i planverkene på helseforetaksnivå og hos Sykehuspartner HF slik at beredskapsarbeidet i Helse Sør-Øst fremstår som helhetlig og samordnet.

Regional beredskapsplan for teknologiområdet (denne planen) er en delplan under den regionale beredskapsplanen, som vist i figuren nedenfor. Helseforetakenes grensesnittene mot Sykehuspartner HF i en beredskapssituasjon innarbeides i andre deler av planverket.



1.2 Omfang og begrensninger

Regional beredskapsplan for teknologiområdet skal bidra til å sikre tilgjengeligheten til virksomhetskritiske IKT-tjenester, inkludert telefoni, meldings-/varslingsløsninger, medisinskteknisk utstyr (MTU) og byggteknisk utstyr (BTU). Delplanen har fokus på hendelser som er forårsaket av IKT-systemer eller som påvirker IKT-systemene direkte. Dette inkluderer blant annet IKT-systemer for diagnostikk og pasientbehandling, digitale beslutningsstøtteverktøy, medisinskteknisk utstyr, løsninger for hjemmearbeid, digital hjemmeoppfølging, samhandlingsløsninger, varslingssystemer, telefoni, med mere.

Håndtering av hendelser som påvirker tilgjengelighet av IKT-løsninger og medisinskteknisk utstyr skal inkluderes i lokale beredskapsplaner for hvert enkelt helseforetak.

Regional beredskapsplan for teknologiområdet gjelder for Helse Sør-Øst RHF og alle underliggende virksomheter, herunder også private institusjoner som har avtale med Helse Sør-Øst RHF. Plikt til overholdelse av beredskapsplanverket skal også inkluderes i IKT-tjenesteavtaler og databehandleravtaler med private institusjoner og virksomheter, og vil da gjelde for disse. Martina Hansens Hospital, Stiftelsen Betanien Hospital, Sophies Minde Ortopedi og Revmatismesykehuset er inkludert, på grunn av avtaler med Sykehuspartner HF. Private institusjoner uten IKT-tjenesteavtale eller databehandleravtale med helseforetak innenfor Helse Sør-Øst er ikke inkludert.

1.3 Retningslinjer

Ulike nasjonale, regionale og lokale retningslinjer gir føringer for IKT-beredskapen, som vist i **Feil! Fant ikke referansekilden.**.

Kilde	Føring
Lov om helsemessig og sosial beredskap	§2.2: Kommuner, fylkeskommuner, regionale helseforetak og staten plikter å utarbeide en beredskapsplan for de helse- og sosialtjenester de skal sørge for et tilbud av eller er ansvarlige for.
Norm for informasjonssikkerhet	5.5.3: Med utgangspunkt i klassifiseringen av informasjonssystemene skal virksomheten etablere nødprosedyrer: - Alternativ drift uten bruk av informasjonssystemene. - Alternativ drift med delvis støtte fra informasjonssystemene.
Ledelsessystem for informasjonssikkerhet, Helse Sør-Øst (styringsdokument for vedtak i alle	Foretaket skal planlegge og etablere tilstrekkelig prosesskontinuitet på en slik måte at nødvendig

helseforetak, publisert på Helse Sør-Øst nettsider: Ledelsessystem for informasjonssikkerhet - Helse Sør-Øst RHF (helse-sorost.no))	tjenestenivå blir opprettholdt selv ved bortfall av IKT-systemene. Foretakets kontinuitetsarbeid må ta hensyn til kravsetting til IKT-leverandører.
Ledelsessystem for informasjonssikkerhet, Helse Sør-Øst	IKT-leverandør skal utarbeide katastrofe- og beredskapsplan for IKT-området og dokumentere at disse møter kravene fra databehandlingsansvarlig
Ledelsessystem for informasjonssikkerhet, Helse Sør-Øst	NO-18: Kravspesifikasjon IKT-tjenester og informasjonssikkerhet for MTU
Ledelsessystem for informasjonssikkerhet, Helse Sør-Øst	NO-19: Regionale sikkerhetsprinsipper og -krav for IKT-infrastruktur og applikasjoner

Tabell 1 Relevante utdrag fra nasjonale, regionale og lokale retningslinjer

1.4 Helseforetak i beredskap

Et helseforetak går i beredskap når det oppstår hendelser som truer foretakets evne til å levere helsetjenester. Svikt eller bortfall av tjenester innenfor helseteknologiområdet kan være en slik hendelse. Ved svikt i eller bortfall av tjenester innenfor helseteknologiområdet vil foretaket gå i beredskap for å kunne håndtere konsekvensene av hendelsen (mens Sykehuspartner vil gå i beredskap for å håndtere årsakene til hendelsen og komme raskest mulig tilbake til normal drift).

Helse Sør-Øst opererer med tre beredskapsnivåer: Grønn, gul og rød. Den generelle definisjon av de ulike beredskapsnivåene står i den regionale beredskapsplanen, og de er detaljert beskrevet i de lokale beredskapsplanene.

Hvert helseforetak skal ha en oversikt over hvilke systemer som er av kategori 1 (kritisk for pasientbehandlingen) og kategori 2 i sine respektive beredskapsplaner.

Helseforetakenes IKT-driftsavtaler må benytte samhandlingsmodell, rollebeskrivelser og varslingsrutiner i samsvar med Regional beredskapsplanen for teknologiområdet.

1.5 Sykehuspartner HF i beredskap

Sykehuspartner HF skal i sitt beredskapsplanverk ivareta bistandsplikt til helseforetak i beredskap – som beskrevet i regional beredskapsplan.

Når et helseforetak går i beredskap grunnet svikt eller bortfall av tjenester innenfor helseteknologiområdet, skal Sykehuspartner vurdere å gå i beredskap for å håndtere årsakene til hendelsen og komme raskest mulig tilbake til normal drift. I situasjoner der et helseforetak er i rød eller gul beredskap, innebærer det at en større uønsket hendelse er inntruffet. Dette kan medføre behov for

ekstraordinær bistand fra Sykehuspartner HF uten at de er forårsaket av IKT-systemer eller påvirker IKT-systemene direkte. Sykehuspartner HF må vurdere situasjonen og gå i beredskap dersom det er nødvendig. Når et helseforetak går i beredskap kan det også utløse behov for beredskap hos Sykehuspartner, eller forsterkede IKT-tjenester på noen områder, selv om årsaken til at foretaket går i beredskap i utgangspunktet ikke er relatert til bortfall av eller svikt på helseteknologiområdet.

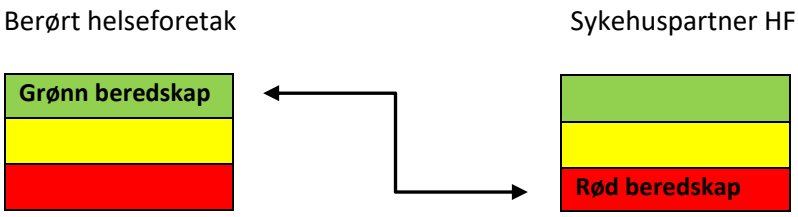
En hendelse av type 1A har følgende karakteristikker (se Sykehuspartners beredskapsplan for utfyllende oversikt over sammenhengen mellom kritikalitet, alvorlighet og beredskap/beredskapsnivå):

Kritikalitet	Alvorlighet
MEGET KRITISK: **Tjenester hvor stopp er eller kan være livstruende for pasienter inklusive feilmedisinering, eller kritisk for helsevirksomhetens drift.**	**MEGET ALVORLIG:** **Flere brukere får ikke gjort jobben sin.** **Fare for liv og helse.** **Betydelig merarbeid/tapt effektivitet.**

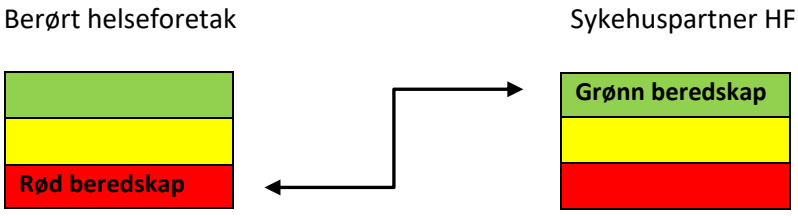
Den lokasjonsspesifikke delen av Sykehuspartners beredskapsplan skal ha en oversikt over kategori 1 systemer som er kritiske for pasientbehandlingen. Ved kategorisering skal de berørte helseforetakene sin oppfatning av situasjonen være førende.

IKT-tjenester og IKT-tilknyttede systemer vil være klassifisert etter hvor kritiske tjenestene/systemene er, det vil si etter hvilke konsekvenser nedetid vil medføre. Dette skal dokumenteres i helseforetakenes gjeldende SLA/tjenestekatalog med Sykehuspartner HF. Dersom flere viktige klasse 1 systemer faller ned sammen skal de berørte helseforetakene gi beskjed om hvilke systemer som skal prioriteres først.

Helseforetak kan ha ulik beredskapsnivå for samme hendelse. I figur 1 er beredskapsnivå i berørt helseforetak satt til grønn, selv om Sykehuspartner HF har gått til rød beredskap.. Ved bruk av bistandsplikten så kan forholdet være motsatt, hvilket er illustrert i figur 2.



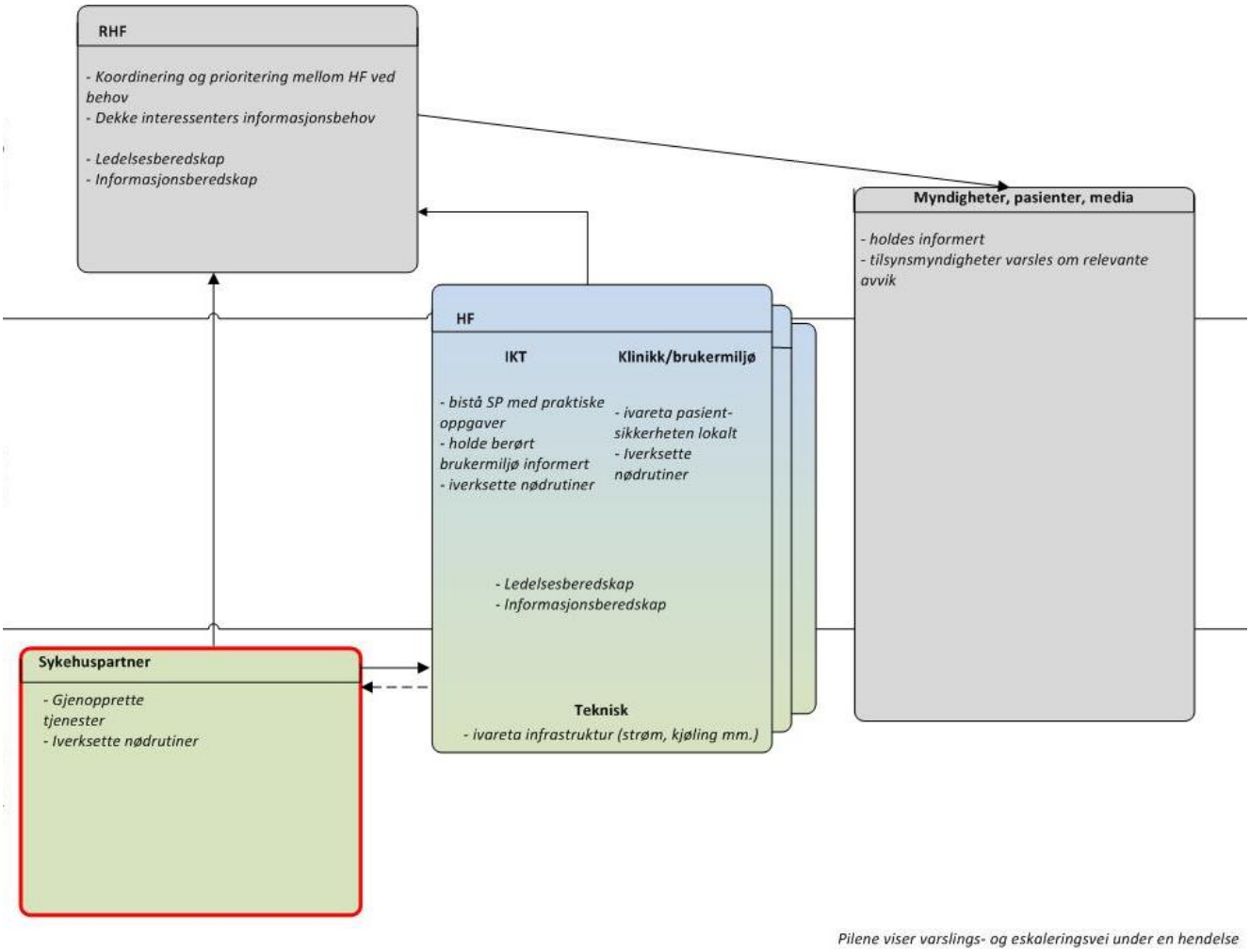
Figur 1: Sykehuspartner HF i rød beredskap (f.eks. cyberhendelse)



Figur 2: Helseforetak i rød beredskap (f.eks. krise med bistandsplikt)

2 Aktører, roller, ansvar og samhandling

Dette kapitlet skal overordnet beskrive involverte roller i normalsituasjon, hvilket ansvarsområde de har og hvordan planlegging av håndtering – og håndtering – av kritiske hendelser organiseres. Se for øvrig også regional beredskapsplan for overordnet ansvarsfordeling.



Figur 3: Illustrasjon av berørte aktørers roller, ansvar og samhandling

2.1 Helse Sør-Øst RHF

Beredskapsarbeid i normalsituasjon:

- Organisere sitt arbeid med beredskap, inkludert informasjons- og ledelsesberedskap, slik at denne også støtter IKT-hendelser.
- Vedlikeholde og oppdatere den regionale delplanen for teknologiberedskap (dette dokumentet).
- Sørge for at IKT/teknologi inkluderes i en helhetlig plan for gjennomføring av beredskapsøvelser.

- Avtalefeste beredskapskrav og –plikter, samt et kontrollregime, i alle drift- og tjenesteavtaler. Dette gjelder spesielt overfor Norsk helsenett SF, som har en tjenesteintegratorrolle for nasjonale IKT-tjenester.

Ved hendelser:

Helse Sør-Øst RHF skal ikke ha en operativ rolle i en IKT-beredskapssituasjon, men kan bistå med ledelses- og informasjonsberedskap og prioriteringer mellom helseforetak og tjenester ved behov. Dette vil i hovedsak styres av hendelsens omfang og konsekvenser. RHF-ets oppgaver er således:

- Motta varslinger fra Sykehuspartner HF om røde eller gule beredskapssituasjoner hos Sykehuspartner HF.
    - Mottas i Helse Sør-Øst RHF ved administrerende direktør, direktør teknologi og e-helse, med flere.
    - Ved behov etableres beredskapsledelse i Helse Sør-Øst RHF.
- Ved behov skal det etableres informasjonsberedskap i henhold til plan.
    - Informasjon til myndigheter
    - Presseinformasjon
- Ved behov skal det etableres ledelsesberedskap i henhold til beredskapsplan.
- Motta eskaleringer og bistå med prioriteringer mellom helseforetak og IKT-tjenester, der Sykehuspartner HF eller helseforetakene anser det som nødvendig. Se for øvrig neste avsnitt 2.2.

2.2 Helseforetak og andre instanser i Helse Sør-Øst

Følgende gjelder for alle helseforetak og andre virksomheter innenfor helseregionen. Sykehuspartner HF har et særskilt ansvar for sikker og stabil drift av teknologi-infrastruktur i Helse Sør-Øst, og er derfor omtalt særskilt under 2.3.

Beredskapsarbeid i normalsituasjon:

- Utvikle og vedlikeholde beredskapsplaner i helseforetaket som tar høyde for kritiske IKT-hendelser.
- Utarbeide og vedlikeholde kontinuitetsplaner ved bortfall av informasjonssystemer med tilhørende nødrutiner på «lavest» mulig nivå i organisasjonen.
- Delta i øvelser, og gjennomføre egne øvelser med fokus på håndtering ved bortfall av IKT-tjenester.
- Ha forberedt løsninger for fjernarbeid, hjemmekontorløsninger og mobilkommunikasjon ved ulike hendelser som påvirker tilgjengeligheten av ansatte, kontorfasiliteter med mer.

Ved hendelser:

- Stille med lokale IKT-ressurser som kan bistå Sykehuspartner HF og holde helseforetakets ledelse informert om status.
- Definere lokalt beredskapsnivå.
- Iverksette nødvendige nødrutiner.
- Varsle mediekontakt i eget helseforetak.
- Varsle relevante tilsynsmyndigheter.
- Bistå i å prioritere tjenester internt i helseforetaket og mellom helseforetak.
- Eskalere til Helse Sør-Øst RHF dersom det er situasjoner som ikke lar seg løse direkte med Sykehuspartner HF eller andre helseforetak. Sykehuspartner HF skal informeres om eskaleringen.
- Varsle Helse Sør-Øst RHF ledelse (se varslingsplan i Regional beredskapsplan)
    - Ved hendelser som kan få medieoppmerksomhet eller som på annen måte vurderes som viktig at Helse Sør-Øst RHF er kjent med.
    - Ved hendelser som oppstår lokalt og som utløser beredskapssituasjon.
    - Ved hendelser der det kan stilles spørsmål om «sørge for ansvaret» oppfylles.

2.2.1 Medisinskteknisk utstyr (MTU)

Alt medisinskteknisk utstyr i sykehusene og ute hos pasientene (behandlingshjelpemidler) skal inngå i helseforetakenes beredskapsplaner. Dette inkluderer vurdering av risiko og sårbarhet (informasjonssikkerhet og personvern), beredskapssituasjoner og nødvendige tiltak som innebærer opprettholdelse eller nedtak/stengning av IKT-tjenester.

Medisinskteknisk utstyr som kjører på maskinvare (server) driftet av Sykehuspartner HF og/eller er tilknyttet felles regional IKT-infrastruktur; skal i tillegg inkluderes i Sykehuspartners risiko- og sårbarhetsvurderinger, trusselvurderinger og beredskapsplaner (inkludert beredskapsrutine for hurtig nedkobling).

2.2.2 Byggteknisk utstyr (BTU)

Byggteknisk utstyr tilknyttet lokal IKT-infrastruktur skal inngå i helseforetakenes beredskapsplaner, når det byggtekniske utstyret også vurderes å være virksomhetskritisk. Det byggtekniske utstyret skal da inkluderes i vurderinger av risiko og sårbarhet (informasjonssikkerhet og personvern), beredskapssituasjoner og nødvendige tiltak som innebærer opprettholdelse eller nedtak/stengning av IKT-tjenester.

Byggteknisk utstyr som kjører på maskinvare (server) driftet av Sykehuspartner HF og/eller er tilknyttet felles regional IKT-infrastruktur; skal i tillegg inkluderes i Sykehuspartners risiko- og sårbarhetsvurderinger, trusselvurderinger og beredskapsplaner (inkludert beredskapsrutine for hurtig nedkobling).

Eksempler på byggteknisk utstyr som må vurderes:

- Adgangskontroll
- Pasientsignal
- Ventilasjon og vifter (kan ha konsekvenser blant annet på operasjonsstuer)
- Brannalarm
- Heisovervåkning

2.3 Sykehuspartner HF

Beredskapsarbeid i normalsituasjon:

- Utarbeide operativ katastrofe- og beredskapsplan for teknologi-området (IKT og MTU) i henhold til krav fra databehandlingsansvarlig i foretakene. Dette inkluderer blant annet:
    - Varslingslister over teknisk ekspertise og ledere i egen organisasjon og hos leverandører som kan kontaktes ved behov for bistand i forbindelse med kritiske IKT- og MTU-hendelser.
- Forvalte den operative delen av planen
    - Gjennomføre øvelser
    - Gjennomføre jevnlige statusmøter med foretakene
    - Oppdatere og vedlikeholde planen
- Jobbe for å oppdage og forhindre hendelser på en mest mulig effektiv måte
    - Sikkerhetsovervåkning
    - Driftsovervåking
    - Kunnskap om systemer
    - Kunnskap om relevante sårbarheter
    - Driftsrutiner
- Stille med representant i regionalt beredskapsutvalg (RBU)
- Overføre beredskapskompetanse og –krav til eksterne leverandører, inkludert Norsk Helsenett. Sørge for at beredskapsansvar blir ivaretatt av eksterne leverandører. Beskrive potensielle konsekvenser for helseforetakene.

Ved hendelser:

- Strategisk, operativt og taktisk ansvar for å håndtere IKT-hendelser.
    - Definere innsatsleder samt andre nødvendige ressurser for å løse hendelsen.
    - Teknologi-innsatsleder skal gis tilstrekkelige fullmakter i Sykehuspartner HF til å kunne iverksette de tiltak han/hun mener finner nødvendig.
    - Gjøre prioriteringer for å hensiktsmessig gjenopprette kritiske tjenester i samarbeid med berørt helseforetak.
    - Følge opp overfor eksterne leverandører.
    - Etablere nødvendig teknisk dialog med berørte helseforetak.

- Varsle og involvere berørt foretaks beredskapsledelse for teknologi og e-helse (eventuelt IKT- og medisinskteknisk avdeling) samt berørte brukermiljøer.
- Varsle Helse Sør-Øst RHF ledelse (se varslingsplan i Regional beredskapsplan)
    - Ved hendelser som kan få medieoppmerksomhet eller som på annen måte vurderes som viktig at Helse Sør-Øst RHF er kjent med.
    - Ved hendelser som utløser beredskapssituasjon i Sykehuspartner HF.
- Eskalere til Helse Sør-Øst RHF dersom det er situasjoner som ikke lar seg løse direkte med berørte helseforetak. Berørte helseforetak skal informeres om eskaleringen.
- Varsle Norsk helsenett SF.

Etter en hendelse:

- Gjennomføre erfaringsmøter i etterkant av hendelser, hvor berørte parter inviteres inn for å vurdere hva som fungerte bra, og hva som kunne vært gjort annerledes. Sykehuspartner HF må også skrive en rapport i etterkant med oppsummering av hendelsen.

2.3.1 Beredskapsrutine for hurtig nedkobling av virksomhetskritiske IKT-tilknyttede systemer

Vakthavende innsatsleder i Sykehuspartner HF har, i samråd med administrerende direktør i Sykehuspartner HF, anledning til å iverksette beredskap og nødvendige tiltak som innebærer nedtak/stengning av IKT-tilknyttede tjenester i berørte helseforetak dersom det er nødvendig. Innsatsleder må gjøre en selvstendig vurdering av mulig konsekvens av uønsket aktivitet samt tilgjengelig tidsvindu for å kunne stoppe trusselaktør. Ut fra denne vurderingen kan innsatsleder iverksette:

a. Ved behov for øyeblikkelig nedtak/stenging av tjenester vil innsatsleder i Sykehuspartner HF varsle egen ledelse, berørte helseforetak og Helse Sør-Øst RHF i henhold til etablert varslingsplan.
b. Ved tvil om aktivitetens konsekvens eller tilgjengelige tidsvindu skal administrerende direktør i Sykehuspartner HF eller dennes stedfortreder varsles for å vurdere om:
    i. - øyeblikkelig nedtak/stenging av tjenester skal gjennomføres.
    ii. - situasjonen skal avklares med administrerende direktør i Helse Sør-Øst RHF før evt. nedtak/stengning.
c. Ved behov for planlagt nedtak/stenging varsles helseforetakene i forkant av utførelse i henhold til etablert varslingsplan. Dersom det er uenighet mellom Sykehuspartner HF og helseforetak om tiltaket er nødvendig, skal dette avklares med administrerende direktør i Helse Sør-Øst RHF.

Det er Sykehuspartner HF som avgjør når IKT-tilknyttede tjenester kan tas opp igjen, både informasjonssikkerhetsmessig og som del av en helhetlig prioritering. Vurdering skal gjøres i samråd med helseforetakene som kjenner kritikaliteten til de ulike tjenestene. Dersom det er uenighet mellom

Sykehuspartner HF og helseforetak om når tjenestene kan tas opp igjen, skal dette avklares med administrerende direktør i Helse Sør-Øst RHF.

2.4 Norsk helsenett SF

Norsk helsenetts tjenesteavtaler med helseforetakene og Helse Sør-Øst RHF må inkludere en plikt til å bistå helseforetak i beredskap, innenfor avtalte tjenesteområder. Dette gjelder spesielt:

- Helsenettet
- Digitale innbyggertjenester på Helsenorge.no
- Meldingsutveksling
- Videotjenester inkludert nasjonal videobro
- Nasjonal løsning for AMK
- Nasjonal Medusa (MTU + behandlingshjelpemidler)
- Nasjonal Kjernejournal
- E-resept, inkludert Reseptformidler, Forskrivningsmodul og Sentral forskrivningsmodul
- Pasientens legemiddelliste (PLL) og SAFEST (strukturert legemiddelinformasjon for spesialisthelsetjenesten)
- Grunndata og HelseID
- Persontjenesten / Modernisert folkeregister
- Felles nettløsning for spesialisthelsetjenesten (FNSP)
- Helselogistikk
- Statistisk logganalyse

2.5 Helsetjenestenes driftsorganisasjon for nødnett (HDO)

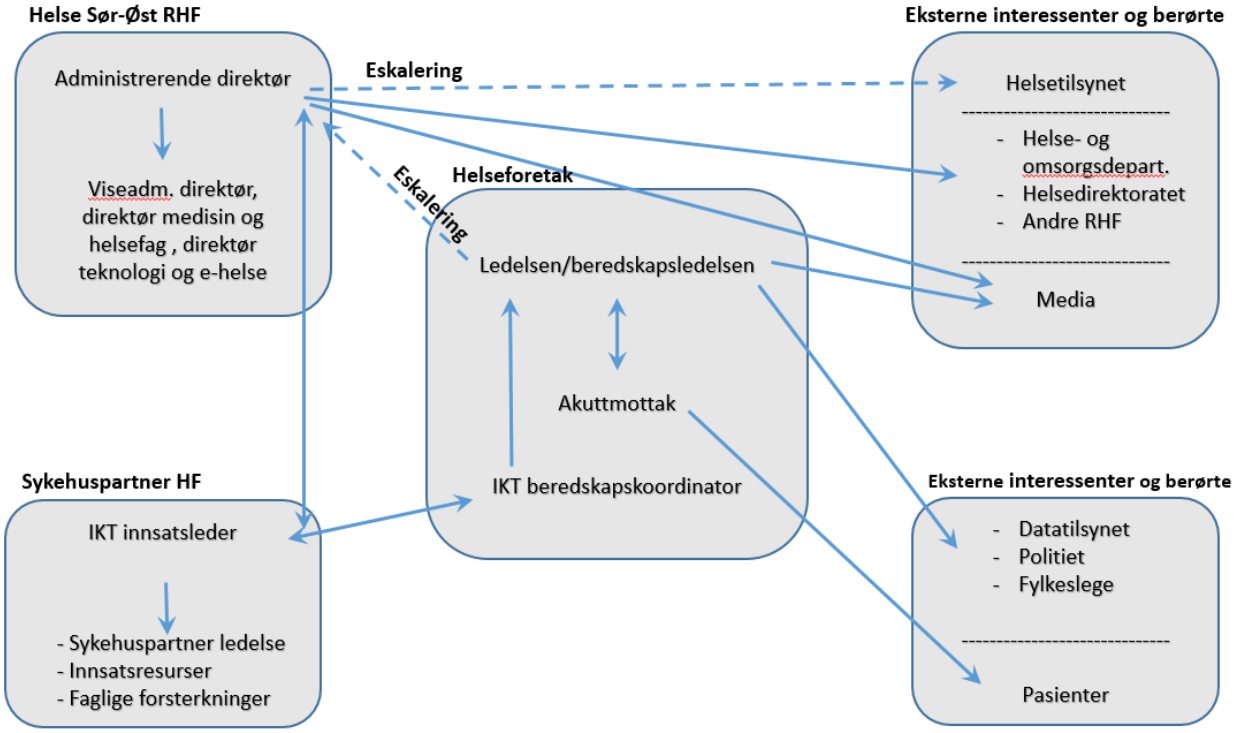
Helse Sør-Øst RHF skal stille krav til HDOs beredskapsarbeid gjennom årlig oppdragsdokument.

HDO må:

- Jobbe for å oppdage og forhindre hendelser på en mest mulig effektiv måte.
- Lage beredskapsplaner for sine tjenester.
- Ha plikt til å bistå helseforetak i beredskap, innenfor avtalte tjenesteområder.
- Varsle alle berørte helseforetak og Helse Sør-Øst RHF ved kritiske beredskapshendelser av betydning for sykehusene.
- Stille med representant i regionalt beredskapsutvalg (RBU).

3 Varsling ved hendelser og kriser

For en smidig håndtering av hendelser og minst mulige konsekvenser er det viktig at riktige personer blir varslet tidligst mulig i hendelsen. Det er viktig å skille tydelig mellom varsling av IKT driftshendelser og tilsiktede cyberhendelser fra kjent/ukjent trussel-aktør. Cyberhendelser kan ofte ikke varsles bredt pga. hendelsens natur eller behov for begrenset varsling. Andre etater (Politiet, Datatilsynet) kan overta ansvar for ekstern varsling ved cyberhendelser. Figur 4 (nedenfor) viser hvordan varslinger skal gjøres i en kritisk IKT driftshendelse. Rollene media, myndigheter og eiendom/teknisk i helseforetaket varsles dersom situasjonen tilsier det, og vurderes fortløpende av de ansvarlig for varslingen.



Figur 4: Varslinger i en kritisk IKT driftshendelse

Ved gul eller rød beredskap i Sykehuspartner HF, så skal innsatsleder i Sykehuspartner HF snarest varsle Helse Sør-Øst RHF og varsle aktuelle helseforetak. Sykehuspartner skal gi tilstrekkelig informasjon som gjør foretakene i stand til å vurdere egen beredskapssituasjon.

Videre i hendelsen kan det være nødvendig å opprette informasjonsflyt på ulike nivåer. Det er imidlertid vesentlig at det holdes ryddig, og at informasjon om gjenoppretting kommer til alle interessenter fra IKT-innsatsleder hos Sykehuspartner HF. Informasjon om tilstanden i helseforetaket skal komme fra lokal leder med delegert ansvar (for eksempel beredskapsledelsen i helseforetaket) på tilsvarende måte som for andre hendelser. Fagressurser innen informasjonssikkerhet og personvern trekkes tidlig inn i hendelser som vedrører informasjonssikkerhet-/cyberhendelser der det er fare for konfidensialitetsbrudd, integritetsbrudd og/eller tilgjengelighetsbrudd (K-I-T).

Helsedirektoratet skal varsles ved større teknologi-hendelser som potensielt kan få konsekvenser utover egen helseregion. Helsedirektoratet vil da koordinere arbeidet med hendelsen på nasjonalt nivå.

4 Etablere beredskapsledelse, rapportere og håndtere

4.1 IKT-beredskapsledelse i helseforetak

Det skal gjennomføres risikovurderinger for å avdekke hendelser relatert til IKT som krever spesiell håndtering fra foretakenes side. Basert på disse risikovurderingene skal det beskrives eller vises til rutiner for håndtering av ulike scenarioer, inkludert nødrutiner. Problemstillinger som vil være nødvendig å se nærmere på inkluderer, men er ikke nødvendigvis begrenset til:

- Kritisk svikt i kliniske IKT-løsninger
- Kritisk svikt i administrative IKT-tjenester
- Svikt i telefonisystem
- Svikt i meldings-/varslingssystem
- Svikt i samhandlingsløsninger, tavleløsninger og mobilapplikasjoner
- Svikt i medisinskteknisk utstyr (MTU)
- Svikt i byggteknisk utstyr (BTU) tilknyttet IKT-infrastruktur

Helseforetakene bør inkludere representant for teknologiområdet i sin beredskapsledelse ved hendelser som involverer helseteknologi. Videre skal det finnes en beskrivelse av de rollene som helseforetaket ifølge denne planen skal stille med i en IKT-beredskapshendelse. Disse skal inkludere en IKT-ressurs (IKT-beredskapskoordinator), som skal være Sykehuspartners kontaktpunkt gjennom hendelsen.

Dette er videre beskrevet i veilederen som er utarbeidet som hjelp for foretakene.

4.2 IKT-beredskapsledelse i Sykehuspartner HF

Sykehuspartner HF er ansvarlig for å utarbeide planer for teknisk håndtering og gjenoppretting ved kritisk bortfall av IKT-tjenester. Det skal være en beredskapsorganisasjon i Sykehuspartner HF som holder planverket oppdatert, samt at tilstrekkelige ressurser skal være kjent med og kunne bruke planen ved hendelser.

Basert på risikovurderinger bør det lages relevante hendelsesscenarioer som beskriver riktige aksjoner, hvem som må varsles og hva det bør informeres om i ulike situasjoner. Detaljgraden i disse scenarioene påvirker hensikten, og det anbefales at disse er relativt detaljerte, selv om det betyr at det er mindre sjanse for at en virkelig hendelse følger nøyaktig samme mønster. De vil allikevel kunne gi nyttige innspill til håndteringen. I tillegg vil disse scenarioene være nyttige som utgangspunkt for øvelser. Aktuelle scenarioer kan for eksempel være:

- Utbrudd av ondsinnet kode hos Sykehuspartner HF
- Utbrudd av ondsinnet kode hos helseforetak

- Mistanke om at uautoriserte har fått tilgang til sensitive personopplysninger
- Fysisk bortfall av datarom
- Ressursmangel hos Sykehuspartner HF på grunn av evakueringer, pandemi eller lignende.

I tillegg må det finnes dokumentasjon av de spesifikke tjenestene og «backup» av relevante data, slik at gjenoppretting kan gjøres effektivt.

Sykehuspartner HF skal også varsle i henhold til rutiner beskrevet i denne delplanen. I situasjoner der et helseforetak varsler om en kritisk IKT-hendelse, må Sykehuspartner HF allikevel varsle teknologileder i helseforetaket i henhold til vanlige beredskapsrutiner (se for øvrig varslingsplan i Regional beredskapsplan).

Sykehuspartner HF skal etablere en egen øvingsplan og vedlikeholde planer for bistand til helseforetak i rød beredskap. Øving av varslingsrutiner og beredskapsplanene skal for øvrig skje regelmessig i Sykehuspartner HF og i henhold til de lover, regler og krav som er stilt til helseforetakene samt Sykehuspartners IKT-leveranseorganisasjon.

4.3 Rapportering

Strategisk beredskapsledelse i det enkelte helseforetak er ansvarlig for loggføring og rapportering etter fastsatte retningslinjer og rutiner i lokalt beredskapsplanverk. Sykehuspartner skal vedlikeholde distribusjonslister og varslingslister for alle helseforetak, for varsling av IKT-hendelser. Ved cyber-hendelser skal behov for gradering vurderes. Egne planer for skjermet varsling og rapportering benyttes når gradering krever det.

All hendelsesrapportering mellom Sykehuspartner HF og helseforetakene skal gjøres i nettløsningen HelseCIM. Situasjonsrapporter og referat fra møter i strategisk beredskapsledelse skal også føres inn i HelseCIM. Eventuell gradert informasjon må behandles i egnede systemer, utenom HelseCIM. Dersom HelseCIM faller bort eller tas ned, så følges kapittel 3.3 «Kommunikasjonsmidler og krisestøttesystem» i den overordnede regionale beredskapsplanen.

Helse Sør-Øst RHF skal ivareta rapportering fra foretaksgruppen til nasjonale myndigheter, som del av eieransvaret.

4.4 Håndtering og prioritering

Sykehuspartner HF har et ansvar for å gjenopprette kritiske IKT- og MTU-tjenester på en hensiktsmessig måte. Det kan i noen tilfeller bety at det må gjøres prioriteringer både mellom tjenester, og mellom helseforetak. Fokus skal være på å ta effektive (raske og gode) beslutninger for å redusere konsekvenser av hendelsen.

I en kritisk IKT-hendelse kan det være ulike tjenester som er utilgjengelige. Det kan også være nødvendig med tiltak som potensielt reduserer tilgjengeligheten til fungerende tjenester. Prioriteringer og avgjørelser av en slik art gjøres av Sykehuspartner HF i tett dialog med berørt helseforetak.

Der Sykehuspartner HF er i en beredskapssituasjon for flere eller alle helseforetak, kan det oppstå situasjoner hvor det må gjøres prioriteringer mellom helseforetak og tjenester på ulike helseforetak. Disse prioriteringene skal baseres på konsekvensvurderinger, med utgangspunkt i følgende retningslinjer:

- Hvor mange og på hvilke måte pasienter påvirkes
- Hvordan akuttsituasjonen er i helseforetaket
- Type tjeneste som er utilgjengelig
- Hvor IKT-intensivt helseforetaket er
- Status på foretakets nødrutiner
- Antatt tid for gjenoppretting
- I hvor stor grad sykehus og helseforetak i nærheten har kapasitet til å ta over oppgaver innenfor IKT-drift og forvaltning, når helseforetak ber om bistand til å håndtere sin beredskapssituasjon.
    - Kapasitet for å gi utvidete tilganger i DIPS for ansatte, i situasjoner der restriksjoner/sperringer kan settes til side.
    - Økt kapasitet for bruk av videomøte i pasientbehandlingen.
    - Kapasitet for å gi utvidete tilganger i kliniske applikasjoner for ansatte.

Prioriteringer gjøres av Sykehuspartner HF, i tett dialog med berørte helseforetak. Dersom det oppstår en situasjon hvor de involverte ikke blir enige om prioriteringene, kan det eskaleres til det regionale helseforetakets ledelse. Direktør teknologi og e-helse kan bistå med råd for å treffe beslutninger. Hvorvidt det skal eskaleres må avgjøres av Sykehuspartner HF eller berørte helseforetak i den konkrete hendelsen, men det er viktig at disse beslutningene ikke tar for lang tid, og det bør derfor ikke brukes for lang tid på vurderinger hos de ulike eskaleringspunktene. Det må etterstrebes å ta avgjørelsene nærmest mulig de som håndterer hendelsen.

Sykehuspartner HF beredskapsplanverk har dedikerte delplaner for håndtering av spesielle hendelser innenfor foretaksgruppen:

- Delplan 1 – Virksomhetsområdene IKT-tjenester og Kliniske IKT-tjenester
- Delplan 2 – Virksomhetsområde Kunder- og servicetjenester
- Delplan 3 – Virksomhetsområde HR, økonomi og regnskap
- Delplan 4 – Beredskapsplan HSØ Forsyningssenter
- Delplan 5 – Virksomhetsområde Prosjekttjenester og leverandørstyring
- Delplan 6 – Informasjonsberedskapsplan (informasjonshåndtering)
- Delplan 7 – Bortfall av personale
- Delplan 8 – Spesielle rutiner for Cyber hendelser
- Delplan 9 – Sambandsberedskap

A. Referanser

- Regionalt ledelsessystem for informasjonssikkerhet, vedtatt ved alle helseforetak
- Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, versjon 6.0
- Regional beredskapsplan
- Sykehuspartner HF beredskapsplan
- Veileder for IKT-beredskap og kontinuitet i foretakene i Helse Sør-Øst
- Lov om helsemessig og sosial beredskap
- Foretakenes gjeldende tjenestenivåavtaler/SLA med Sykehuspartner HF

B. Versjonskontroll

Versjonsnr.:	**Årsak til endring:**	**Dato:**
Versjon 0.1	MEØ: Dokument opprettet	
Versjon 0.2	MEØ: Dokument endret etter innspill fra Anne Marie Dalen Øverhaug og prosjektgruppa	
Versjon 0.3	MEØ: Dokument oppdatert etter spesifisering av beredskapsnivåer hos Sykehuspartner.	
Versjon 0.4	MEØ: Dokument oppdatert etter innspill i IKT-lederforum, fra IKT i Sykehuspartner og enhetsledermøte teknologi og e-helse i RHF-et.	
Versjon 0.5	MEØ: Dokument oppdatert etter innspill fra Gry Sundberg og Anne Marie Dalen Øverhaug.	
Versjon 0.9	MEØ: Dokumentet ferdigstilles for godkjenning.	
Versjon 0.91	MEØ: Oppdatering etter innspill fra prosjektgruppa	
Versjon 0.92	MEØ: Oppdatering etter innspill fra foretak og RHF	
Versjon 1.0	MEØ: Dokument ferdigstilt	
Versjon 1.1	MEØ: Oppdatert etter innspill fra teknologi og e-helse	
Versjon 1.2	Tim Papas: Oppdatering ved revisjon	mars/april 2014
Versjon 1.3	Frank Ivar Aarnes: Oppdatering ved revisjon	februar 2016
Versjon 1.4	Frank Ivar Aarnes: Oppdatering til LG-sak med oppfølging av tiltak etter datainnbrudd, «trinn 1»	januar 2020
Versjon 1.5	Frank Ivar Aarnes: Oppdatering «trinn 2»	februar 2020
Versjon 1.51	FIA: Oppdatert varslingsrekkefølge. Vedtatt i ledermøte teknologi og e-helse.	februar 2020
Versjon 1.6	FIA: Oppdatert dokumentstruktur, harmonisering mot Sykehuspartners beredskapsplanverk, fjernet innhold som hører hjemme andre steder, inkludering av MTU-området. Behandlet i LG.	desember 2021
Versjon 1.61	FIA: Begrensede justeringer etter innspillsrunde med IKT-ledere og sikkerhetsledere i helseforetakene. Utvidet og tydeligere omtale av byggteknisk utstyr (BTU).	januar-april 2022