Regional IKT-beredskapsplan

Dette dokumentet erstatter etter at det er godkjent nåværende vedlegg 4 i ***Regional beredskapsplan for Helse Sør-Øst,*** *og inngår således som en delplan til den regionale beredskapsplanen på linje med plan for smittevernberedskap og varslingsrutiner ved akutt oppstått mangel på legemidler.*

Innhold

1 Innledning/formål

Risikovurderinger har vist at IKT understøtter stadig flere av kjerneprosessene innen spesialisthelsetjenesten. Dette fører til at sårbarheten ved bortfall av IKT-tjenester øker, noe som igjen krever effektiv og god håndtering av kritiske IKT-hendelser. Målet med denne planen er således å tydeliggjøre ansvarsområder og grensesnitt mellom Helse Sør-Øst RHF, helseforetakene og tjenesteleverandøren Sykehuspartner.

Den IKT-relaterte delen av beredskapsrammeverket kan anses som en egen delplan, men er i så stor grad som mulig basert på samme organiseringsform som resten av beredskapsrammeverket.

Ulike nasjonale, regionale og lokale retningslinjer gir føringer for IKT-beredskapen, som vist i Tabell 1.

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 helseforetak)	3.11: Foretaket skal planlegge og etablere tilstrekkelig prosesskontinuitet på en slik måte at nødvendig 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 (styringsdokument for vedtak i alle helseforetak)	3.1.1.1.7: IKT-leverandør skal utarbeide katastrofe- og beredskapsplan for IKT-området og dokumentere at disse møter kravene fra databehandlingsansvarlig
Ledelsessystem for informasjonssikkerhet, Helse Sør-Øst (styringsdokument for vedtak i alle helseforetak)	NO-19: Regionale sikkerhetsprinsipper og -krav for IKT-infrastruktur og applikasjoner

Tabell 1 Relevante utdrag fra nasjonale, regionale og lokale retningslinjer

1.1 Målsetning

Denne delplanen gir føringer på strategisk og taktisk nivå og definerer roller, ansvarsområder og kommunikasjonsveier nødvendig i IKT-beredskap. 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.

1.2 Omfang og begrensninger

Delplanen skal bidra til å sikre tilgjengeligheten til virksomhetskritiske IKT-tjenester, inkludert telefoni og meldings-/varslingsløsninger. Håndtering av hendelser som påvirker tilgjengelighet til medisinsk-teknisk utstyr er ikke inkludert i planen, fordi dette er et område som i stor grad håndteres av hvert foretak, og i mindre grad påvirker hele regionen.

Delplanen gjelder for Helse Sør-Øst RHF og alle underliggende virksomheter. Martina Hansens Hospital, Stiftelsen Betanien Hospital, Sophies Minde Ortopedi og Revmatismesykehuset er inkludert, på grunn av avtale med Sykehuspartner HF. Andre private institusjoner med avtale med Helse Sør-Øst RHF er ikke inkludert, fordi de ikke har avtale med Sykehuspartner HF.

1.3 Ansvarlig for planen

Ansvarlig for utarbeidelse og ajourhold av planen er, som for resten av regional beredskapsplan, ledelsen i Helse Sør-Øst RHF, ivaretatt ved avdeling teknologi og e-helse i samarbeid med Sykehuspartner HF.

2 Beredskapsnivå

2.1 Foretak i beredskap

Helse Sør-Øst opererer med tre beredskapsnivåer for beredskapsnivå utover normalberedskap:

Beredskapsnivå	Betyr for foretakene
GRØNN	Beredskapsledelse etableres på foretaksnivå/sykehusnivå. Enkeltfunksjoner kan forsterkes ved behov.
GUL	Begrenset mobilisering av ekstra ressurser. Iverksettes når en uønsket hendelse er inntruffet (eller det er stor fare for at den kan inntreffe) og der det er sannsynlig at de ordinære ressursene ikke strekker til. På dette nivået iverksettes definerte tiltak og begrenset beredskapsøkning.
RØD	Mobilisering av betydelige ressurser og omlegging av drift. Iverksettes når en større uønsket hendelse er inntruffet og de ordinære ressursene ikke strekker til. På dette nivået iverksettes definerte tiltak og en mer omfattende beredskapsøkning.

I situasjoner der et foretak er i rød eller gul beredskap, innebærer det at en større uønsket hendelse er inntruffet. Disse hendelsene kan medføre behov for ekstraordinær bistand fra Sykehuspartner uten at de er forårsaket av IKT-systemer eller påvirker IKT-systemene direkte. Sykehuspartner må vurdere situasjonen og dersom det er nødvendig eskalere til minimum gul beredskap.

Gul beredskap i Sykehuspartner betyr:

a. Helseforetaket varsler Driftssenteret om at de har en beredskapssituasjon som krever økt beredskap hos Sykehuspartner. Helseforetaket vil så langt det er mulig spesifisere hva slags assistanse fra Sykehuspartner som kan bli aktuelt
b. Driftssenteret sender ut en varsling på SMS til alle lederne i Sykehuspartner om at vi nå befinner oss i gul beredskap med informasjon om hvilke helseforetak som har en beredskapssituasjon, type beredskapssituasjon og om mulig hva slags assistanse som kan bli aktuell
c. Helseforetaket bestiller fortløpende den assistanse de har behov for hos Sykehuspartner via Driftssenteret, som videreformidler internt i Sykehuspartner og følger opp.
d. Dersom enten helseforetaket krever at en representant stiller opp lokalt eller at Driftssenteret vurderer at situasjonen krever en egen it-innsatsleder, kan Driftssenteret kalle inn en it-innsatsleder og sette Sykehuspartner i rød beredskap.

Denne planen (Regional delplan IKT-beredskap) har **fokus på hendelser som er forårsaket av IKT-systemer eller som påvirker IKT-systemene direkte**. Grensesnittene mot Sykehuspartner i en beredskapssituasjon for foretak må innarbeides i andre deler av planverket.

2.2 Sykehuspartner i beredskap

Kriteriene Sykehuspartner bruker for å iverksette beredskap er:

Gul beredskap iverksettes for eksempel når et av helseforetakene har økt beredskapsnivå eller hvis Beredskapskoordinator i Sykehuspartner vurderer det slik at situasjonen krever skjerpet beredskap.
Rød beredskap benyttes når en har en hendelse med kritikalitet 1A og det er sannsynlig at det vil ta mer enn 1 time å rette feilen.

En hendelse av type 1A har følgende karakteristikker:

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

Ved kategorisering skal de berørte foretakene sin oppfatning av situasjonen være førende.

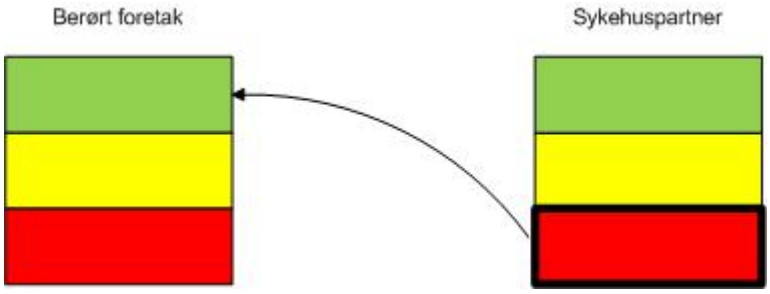
Tjenester vil være klassifisert etter hvor kritiske tjenestene er, det vil si etter hvilke konsekvenser nedetid vil medføre. Dette er dokumentert i foretakenes gjeldende SLA/tjenestekatalog. Dersom flere viktige klasse 1 systemer faller ned sammen skal de berørte helseforetakene gi beskjed om hvilke systemer som skal prioriteres først. Dersom en slik prioritering ikke foreligger kan følgende generelle prioriteringsliste benyttes:

- Telefon/Calling
- Bildediagnostikk
- Labsystemer
- EPJ/PAS

Det finnes en oversikt over hvilke systemer som er av kategori 1 for hvert enkelt helseforetak i den lokasjonsspesifikke delen av Sykehuspartners plan.

Sykehuspartner skal i rød beredskap snarest varsle foretakene og gi informasjon som gjør foretakene i stand til å vurdere sin egen beredskapssituasjon.

I Figur 1 er beredskapsnivå i berørt foretak satt til grønn.



Figur 1: Sykehuspartner i rød beredskap

3 Organisering, roller og ansvarsområder

3.1 I normalsituasjon

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

3.1.1 Foretak

- Utrope ansvarlig for å bistå i utvikling og vedlikehold av beredskapsplaner i foretaket som tar høyde for kritiske IKT-situasjoner.
- Utarbeide og vedlikeholde kontinuitetsplaner ved bortfall av informasjonssystemer (nødrutiner) på «lavest» mulig nivå i organisasjonen.
- Delta i større øvelser, og gjennomføre egne øvelser med fokus på håndtering ved bortfall av IKT-tjenester

3.1.2 Sykehuspartner

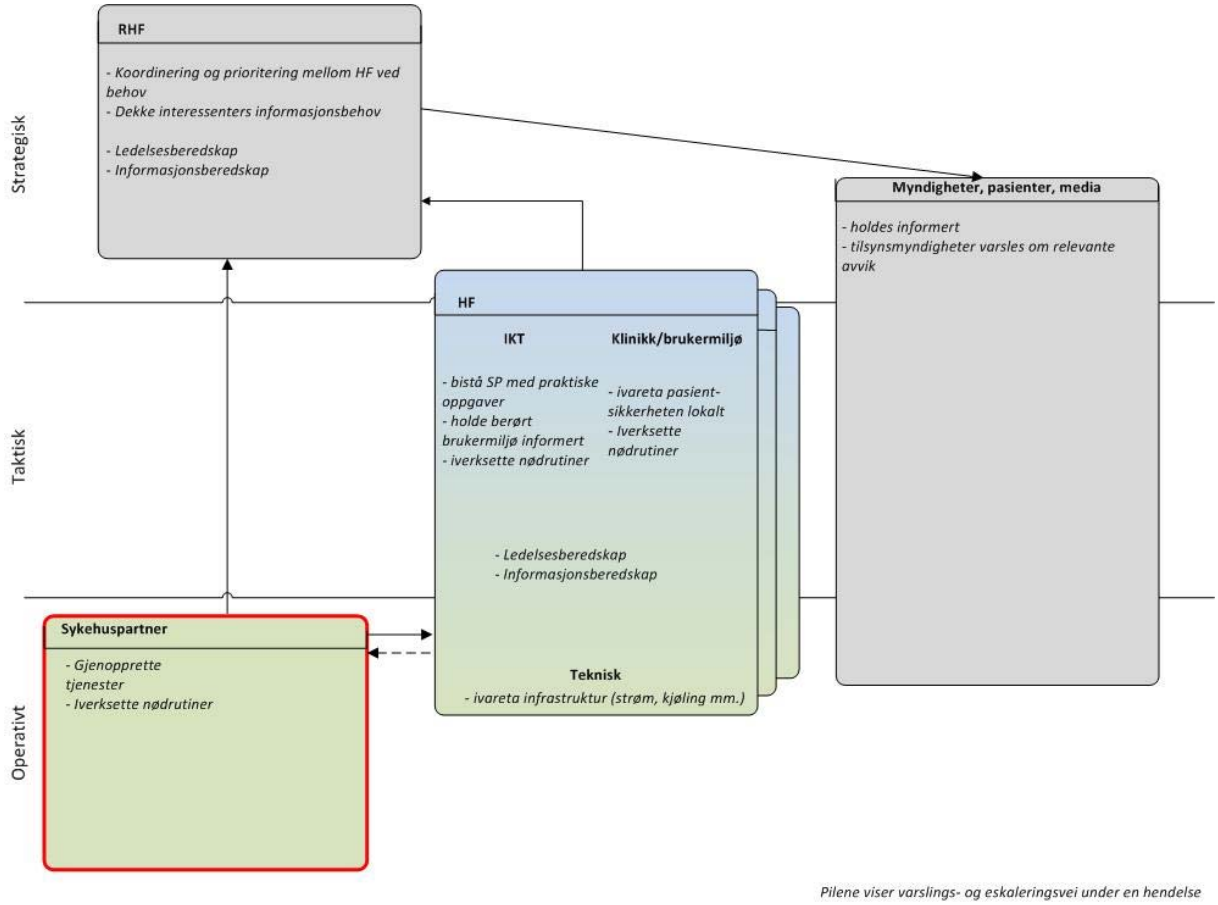
- Utarbeide operativ katastrofe- og beredskapsplan for IKT-området i henhold til krav fra databehandlingsansvarlig i foretakene. Dette inkluderer blant annet:
    - Varslingslister over teknisk ekspertise og ledere i egen organisasjon og hos leverandører som kan kontaktes ved behov for bistand i forbindelse med kritiske IKT-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)

3.1.3 Helse Sør-Øst RHF

- Forvalte sin beredskapsplan, inkludert informasjons- og ledelsesberedskap, slik at denne støtter også IKT-situasjoner.
- Utrope ansvarlig for den regionale delplanen for IKT-beredskap (dette dokumentet)
    - Utvikle og vedlikeholde den regionale delplanen for IKT-beredskap (dette dokumentet)
    - Sørge for at IKT inkluderes i en helhetlig plan for gjennomføring av øvelser

3.2 I responssituasjon

Dette kapitlet skal overordnet beskrive involverte roller, hvilket ansvarsområde de har og hvordan beredskapen knyttet til **håndtering** av kritiske hendelser organiseres.



3.2.1 Foretak

- Stille med IKT-ressurs som kan bistå Sykehuspartner og holde foretaket informert om status
- Sette beredskapsnivå for foretaket (gjøres av ulike roller i de ulike foretakene)
- Iverksette nødvendige nødrutiner
- Varsle mediekontakt i eget foretak
- Varsle relevante tilsynsmyndigheter
- Bistå i å prioritere tjenester internt i foretaket og mellom foretak
- Eskalere til Helse Sør-Øst RHF ved viseadministrerende direktør, medisin- og helsefag, dersom det er situasjoner som ikke lar seg løse direkte med Sykehuspartner eller andre foretak. Sykehuspartner skal informeres om eskaleringen.

3.2.2 Sykehuspartner

- Operativt ansvar
    - Stille med operativ IT-innsatsleder samt andre nødvendige ressurser for å løse IKT-hendelsen
    - IT-innsatsleder skal gis tilstrekkelige fullmakter i Sykehuspartner til å kunne iverksette de tiltak han/hun mener finner nødvendig.
    - Gjøre prioriteringer for å hensiktsmessig gjenopprette kritiske tjenester i samarbeid med berørt foretak.
    - Følge opp overfor eksterne leverandører.
- Varsle berørt foretak – IKT og berørt brukermiljø
- Varsle Helse Sør-Øst RHF

  - I følgende rekkefølge eller samlet: Administrerende direktør, viseadministrerende direktør, direktør teknologi og e-helse, konserndirektør, kommunikasjonsdirektør, direktør personal- og kompetanseutvikling, økonomidirektør, eierdirektør.
  - 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 GUL eller RØD beredskap.
  - Ved hendelser der det kan stilles spørsmål om "sørge for"-ansvaret oppfylles.
- Eskalere til Helse Sør-Øst RHF viseadministrerende direktør, Medisin- og helsefag, dersom det er situasjoner som ikke lar seg løse direkte med berørte foretak. Berørte foretak skal informeres om eskaleringen.
- Varsle Norsk Helsenett
- 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 må også skrive en rapport i etterkant med oppsummering av hendelsen.

3.2.3 Helse Sør-Øst RHF

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

- Motta varslinger fra Sykehuspartner om røde eller gule situasjoner hos Sykehuspartner.
  - Beredskapsledelse i Helse Sør-Øst RHF, direktør teknologi og e-helse.
- Ved behov skal det etableres informasjonsberedskap i henhold til plan.
  - Informasjon til myndigheter
  - Presseinformasjon
- Ved behov skal det etableres ledelsesberedskap i henhold til plan.
- Motta eskaleringer og bistå med prioriteringer mellom foretak og tjenester, der Sykehuspartner eller foretakene anser det som nødvendig. Se for øvrig neste avsnitt.

3.2.4 Prioriteringer

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

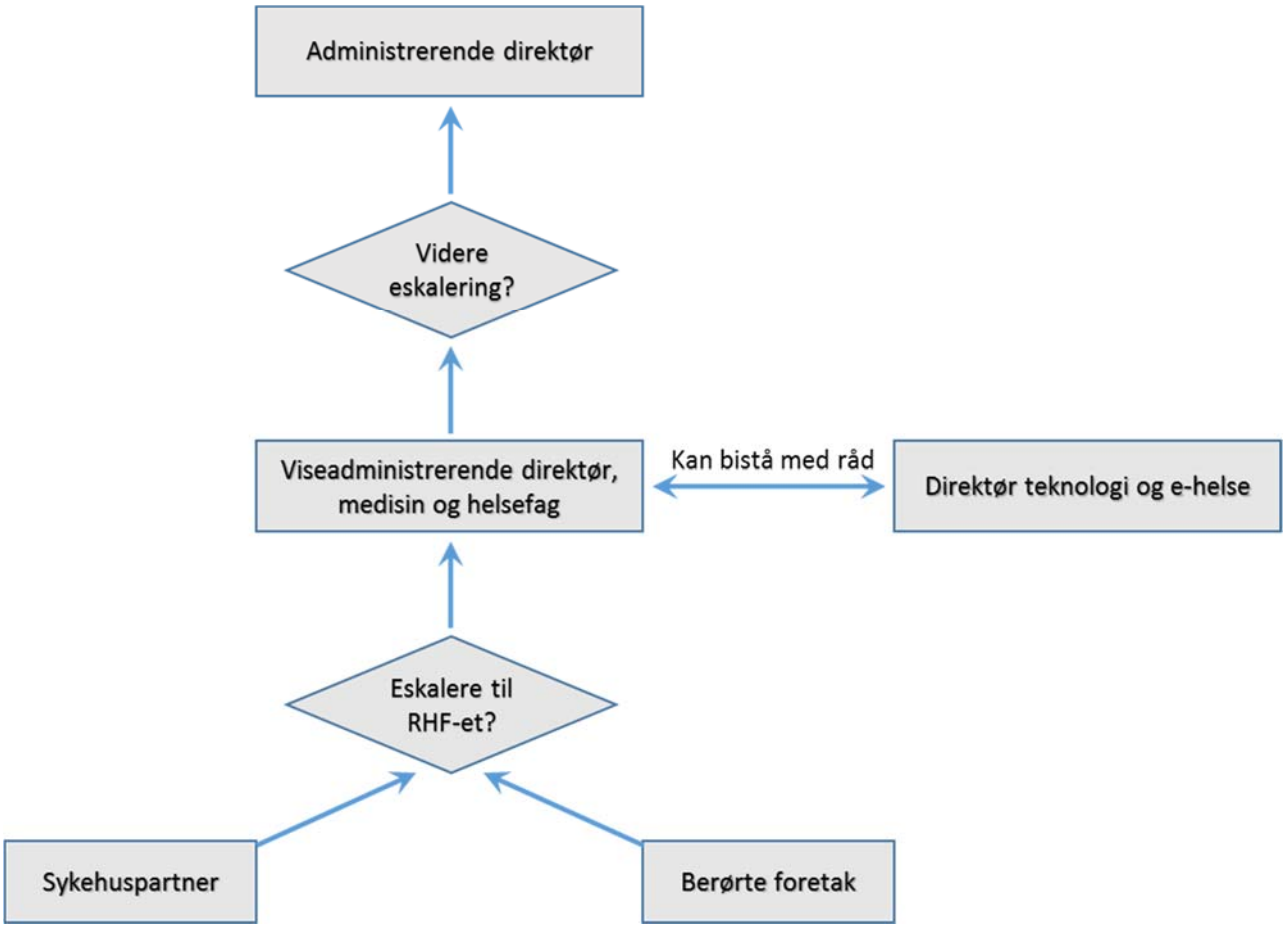
I en kritisk IKT-hendelse kan det være ulike tjenester som er utilgjengelige. Det kan også være nødvendig med tiltak som potensielt reduserer tilgjengeligheten til fungerende tjenester. Prioriteringer og avgjørelser av en slik art gjøres av Sykehuspartner i tett dialog med berørt foretak.

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

- Hvor mange og på hvilke måte pasienter påvirkes
- Hvordan akuttsituasjonen er i foretaket
- Type tjeneste som er utilgjengelig
- Hvor IKT-intensivt foretaket er

- Status på foretakets nødrutiner
- Antatt tid for gjenoppretting
- I hvor stor grad sykehus og foretak i nærheten har kapasitet til å ta over oppgaver

Prioriteringer gjøres av Sykehuspartner, i tett dialog med berørte foretak. Dersom det oppstår en situasjon hvor de involverte ikke blir enige om prioriteringene, kan det eskaleres til det regionale helseforetakets ledelse ved viseadministrerende direktør, medisin- og helsefag. Direktør teknologi og e-helse kan bistå med råd for å treffe beslutninger. Eventuell videre eskalering i det regionale helseforetaket følger vanlige eskaleringsrutiner til administrerende direktør. Disse eskaleringspunktene er i samsvar med det regionale helseforetakets oppdragsavtale med Sykehuspartner om eskalering i andre situasjoner.



Figur 2: Eskalering

Hvorvidt det skal eskaleres må avgjøres av Sykehuspartner eller berørte foretak 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.

3.2.5 Beredskapsrutine for hurtig nedkobling av virksomhetskritiske IKT-systemer

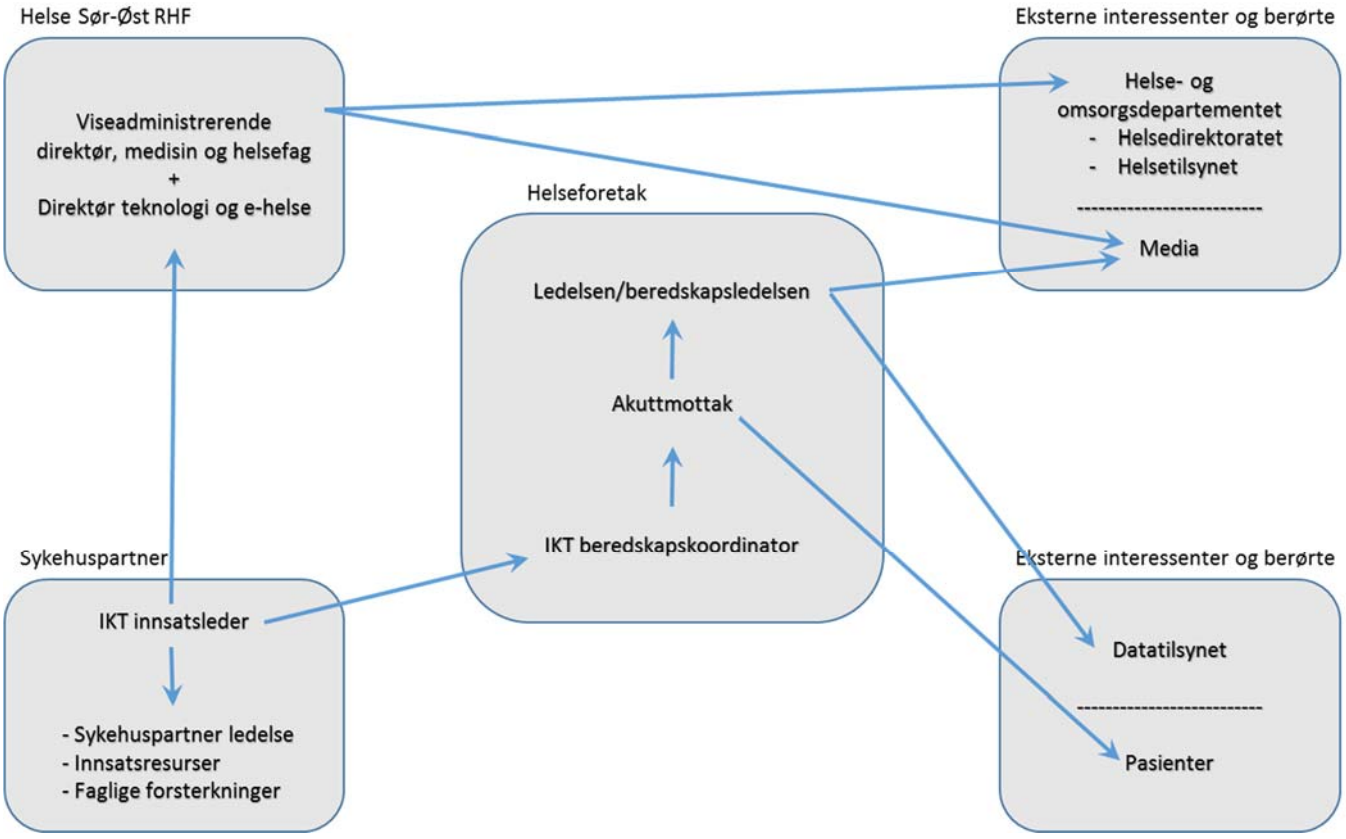
Vakthavende innsatsleder i Sykehuspartner har anledning til å iverksette beredskap og nødvendige tiltak som innebærer nedtak/stengning av tjenester i berørte helseforetak dersom det er nødvendig. Innsatsleder må gjøre en selvstendig vurdering av mulig konsekvens av uønsket aktivitet samt tilgjengelig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

a. Ved behov for øyeblikkelig nedtak/stenging av tjenester vil Sykehuspartner varsle egen ledelse, 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 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 og helseforetak om tiltaket er nødvendig, skal dette avklares med administrerende direktør i Helse Sør-Øst RHF.

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

4 Varsling og informasjonsflyt

For en smidig håndtering av hendelser og minst mulige konsekvenser er det viktig at riktige personer blir varslet tidligst mulig i hendelsen. Figur 3 viser hvordan varslinger skal gjøres i en kritisk IKT-hendelse. Rollene media, myndigheter og eiendom/teknisk i foretaket varsles dersom situasjonen tilsier det, og vurderes fortløpende av de ansvarlig for varslingen. De andre skal varsles uavhengig av situasjon.



Figur 3: Varslinger i en kritisk IKT-hendelse

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 fra IT-innsatsleder hos Sykehuspartner til alle interessenter. Informasjon om tilstanden i foretaket skal på tilsvarende måte komme fra et sentralt punkt (for eksempel beredskapsledelsen i foretaket) som for andre hendelser.

5 Krav til helseforetakenes IKT-beredskap

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 andre IKT-tjenester
- Svikt i telefonisystem
- Svikt i meldings-/varslingssystem

Videre skal det finnes en beskrivelse av de rollene som foretaket 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.

6 Krav til Sykehuspartners IKT-beredskap

Sykehuspartner er ansvarlig for å utarbeide planer for teknisk håndtering og gjenoppretting ved kritisk bortfall av IKT-tjenester. Det skal være en beredskapsorganisasjon i Sykehuspartner 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
- Utbrudd av ondsinnet kode hos foretak
- Mistanke om at uautoriserte har fått tilgang til sensitive personopplysninger
- Fysisk bortfall av datarom
- Ressursmangel hos Sykehuspartner 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 skal også varsle i henhold til rutiner beskrevet i denne delplanen. I situasjoner der foretaket varsler om en kritisk IKT-hendelse, må Sykehuspartner allikevel varsle IKT i foretaket i henhold til vanlige beredskapsrutiner.

Øving av varslingsrutiner og beredskapsplanene skal skje regelmessig i Sykehuspartner og i henhold til de lover, regler og krav som er stilt til helseforetakene samt Sykehuspartners IKT-leveranseorganisasjon per 1. januar 2016. Det må etableres en egen øvingsplan.

Sykehuspartner skal også vedlikeholde planer for bistand til foretak i rød beredskap.

7 Krav til Helse Sør-Øst RHFs IKT-beredskap

Når varslinger i henhold til planverket kommer til mediekontakt, er det viktig at det finnes gode varslingsrutiner til:

- Viseadministrerende direktør, medisin- og helsefag
- Direktør for teknologi og e-helse

Varslingene skal følge normale kommunikasjonsveier, og bidra til at ledelsen er godt informert om situasjonen. Dette igjen for å kunne gi god informasjon ut til tilsynsmyndigheter, media og andre interessenter.

Ved varsling til ledelsen i Helse Sør-Øst RHF skal disse varsles samlet eller i følgende rekkefølge:

- Administrerende direktør
- Viseadministrerende direktør
- Direktør teknologi og e-helse
- Konserndirektør
- Kommunikasjonsdirektør
- Direktør personal- og kompetanseutvikling
- Økonomidirektør
- Eierdirektør

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 felles beredskapsplan

Veileder for IKT-beredskap og kontinuitet i foretakene i Helse Sør-Øst

Lov om helsemessig og sosial beredskap

Foretakenes gjeldende tjenestenivåavtaler/SLA

Versjonskontroll

Versjonsnummer:	**Årsak til endring:**	
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: Dokument 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.	3. februar 2020