

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	3
1.1	Målsetning.....	3
1.2	Omfang og begrensninger	3
1.3	Ansvarlig for planen.....	4
2	Beredskapsnivå	5
2.1	Foretak i beredskap	5
2.2	Sykehuspartner i beredskap	6
3	Organisering, roller og ansvarsområder	7
3.1	I normalsituasjon	7
3.1.1	Foretak	7
3.1.2	Sykehuspartner	7
3.1.3	Helse Sør-Øst RHF	7
3.2	I responsituasjon.....	7
3.2.1	Foretak	8
3.2.2	Sykehuspartner	8
3.2.3	Helse Sør-Øst RHF	9
3.2.4	Prioriteringer	9
4	Varsling og informasjonsflyt.....	10
5	Krav til helseforetakenes IKT-beredskap.....	12
6	Krav til Sykehuspartners IKT-beredskap.....	13
7	Krav til Helse Sør-Øst RHFets IKT-beredskap	14
A.	Referanser	15

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: <ul style="list-style-type: none"> - Alternativ drift uten bruk av informasjonssystemene. - Alternativ drift med delvis støtte fra informasjonssystemene.
Styringssystem for informasjonssikkerhet, Helse Sør-Øst (Styringsdokument <foretaksnavn>)	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.
Styringssystem for informasjonssikkerhet, Helse Sør-Øst (Styringsdokument <foretaksnavn>)	3.1.1.1.7: IKT-leverandør skal utarbeide katastrofe- og beredskapsplan for IKT-området og dokumentere at disse møter kravene fra databehandlingsansvarlig

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 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-systemer, inkludert telefoni/ personsøkerløsninger. 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 er inkludert, på grunn av avtale med Sykehuspartner. Andre private institusjoner med avtale med HSØ er ikke inkludert, fordi de ikke har avtale med Sykehuspartner.

1.3 Ansvarlig for planen

Ansvarlig for planen er, som for resten av regional beredskapsplan, ledelsen i Helse Sør-Øst RHF. Avdeling for Teknologi og eHelse har et særlig ansvar for at denne delen av planen er oppdatert.

Regionalt beredskapsutvalgs(RBU) rolle er beskrevet i avsnitt 2.2 i regional beredskapsplan og dette er også gjeldende for denne delplanen.

2 Beredskapsnivå

2.1 Foretak i beredskap

Helse Sør-Øst opererer med tre beredskapsnivåer:

Beredskapsnivå	Betyr for foretakene
GRØNN	Betegner en beredskap der det etableres beredskapsledelse på foretaksnivå/sykehusnivå i situasjoner der det ikke eller i begrenset grad er behov for ekstra ressurser.
GUL	Betegner en beredskap som 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	Betegner en beredskap som 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 årsaket av IKT-systemer eller påvirker IKT-systemene direkte. Det er derfor nødvendig at Sykehuspartner eskalerer til minimum gul beredskap i en slik situasjon.

Gul beredskap i Sykehuspartner betyr:

- 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
- Driftssenteret sender ut en varslings SMS til alle lederne i SP IKT 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
- Helseforetaket bestiller fortløpende den assistansen de har behov for hos Sykehuspartner via Driftssenteret, som viderefremmer internt i Sykehuspartner og følger opp.
- 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 årsaket av IKT-systemer eller som påvirker IKT-systemene direkte**. Situasjonen som er beskrevet over er derfor *ikke* understøttet av denne delplanen. 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.

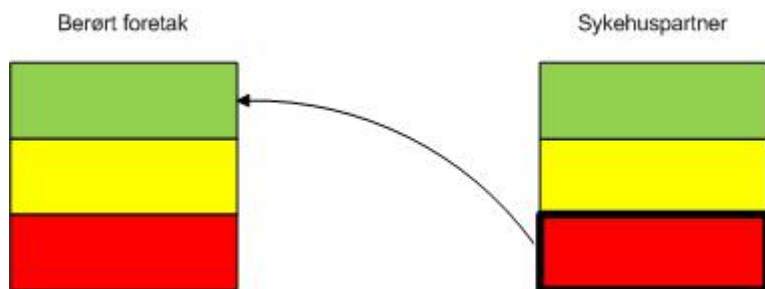
Tjenester vil være klassifisert etter hvor kritiske tjenestene er, det vil si etter hvilke konsekvenser nedetid vil medføre. Dette er dokumentert i foretakenes gjeldende SLA/tjenestekatalog. Dersom flere viktige klasse 1 systemer faller ned sammen skal de berørte helseforetakene gi beskjed om hvilke 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

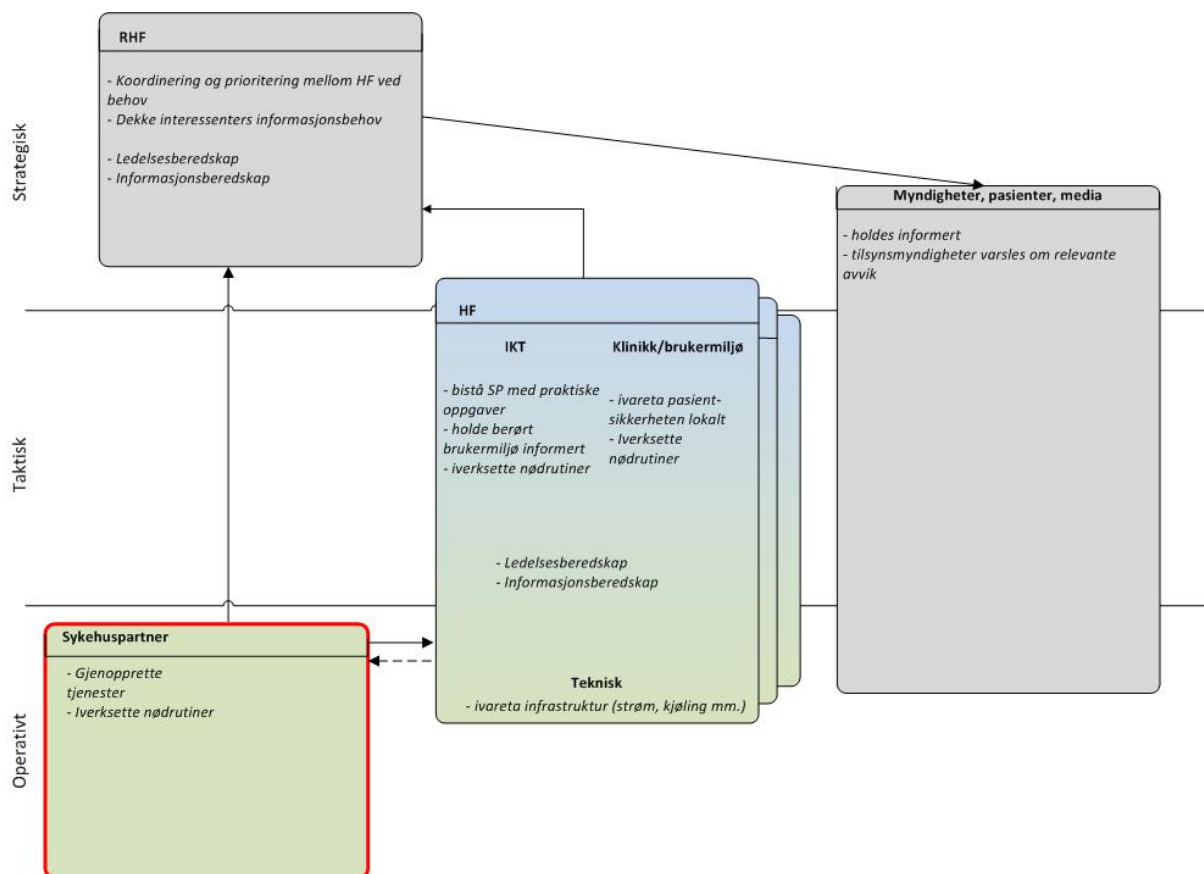
- Utarbeide operativ katastrofe- og beredskapsplan for IKT-området i henhold til krav fra databehandlingsansvarlig i foretakene. Dette inkluderer blant annet:
 - o Varslingslister over teknisk ekspertise og ledere i egen organisasjon og hos leverandører som kan kontaktes ved behov for bistand i forbindelse med kritiske IKT-hendelser.
- Forvalte den operative delen av planen
 - o Gjennomføre øvelser
 - o Gjennomføre jevnlig statusmøter med foretakene
 - o Oppdatere og vedlikeholde planen
- Jobbe for å oppdage og forhindre hendelser på en mest mulig effektiv måte
 - o Sikkerhetsovervåkning
 - o Driftsovervåkning
 - o Kunnskap om systemer
 - o Kunnskap om relevante sårbarheter
 - o 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)
 - o Utvikle og vedlikeholde den regionale delplanen for IKT-beredskap (dette dokumentet)
 - o Sørge for at IKT inkluderes i en helhetlig plan for gjennomføring av øvelser

3.2 I responsituasjon

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



Pilene viser varslings- og eskaleringsvei under en hendelse

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 direktør for 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
 - o Stille med operativ IT-innsatsleder samt andre nødvendige ressurser for å løse IKT-hendelsen
 - o IT-innsatsleder skal gis tilstrekkelige fullmakter i SP til å kunne iverksette de tiltak han/hun mener finner nødvendig.
 - o Gjøre prioriteringer for å hensiktsmessig gjenopprette kritiske tjenester i samarbeid med berørt foretak.
 - o Følge opp overfor eksterne leverandører.
- Varsle berørt foretak – IKT og berørt brukermiljø
- Varsle Helse Sør-Øst RHF
 - o Ved hendelser som kan få medieoppmerksomhet eller som på annen måte vurderes som viktig at Helse Sør-Øst RHF er kjent med

- Hendelser som oppstår lokalt og som utløser GUL eller RØD beredskap.
- Hendelser der det kan stilles spørsmål om "sørge for"-ansvaret oppfylles.
- Eskalere til Helse Sør-Øst RHF ved direktør for 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. RHFets oppgaver er således:

- Motta varslinger fra Sykehuspartner om røde eller gule situasjoner hos Sykehuspartner.
 - Beredskapsledelse i Helse Sør-Øst RHF, direktør for Teknologi og eHelse og leder Informasjonssikkerhet 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 plan.
- Motta eskaleringer og bistå med prioriteringer mellom foretak og tjenester, der SP eller foretakene anser det som nødvendig. Se for øvrig neste avsnitt.

3.2.4 Prioriteringer

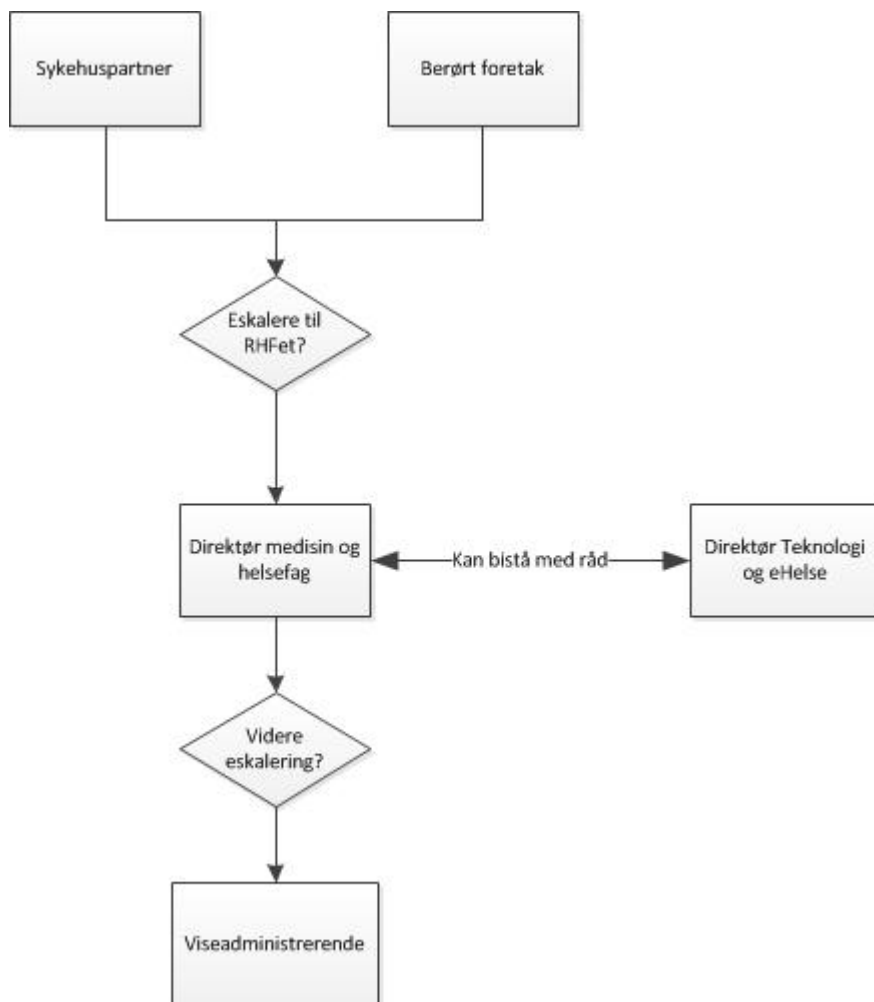
Sykehuspartner har et ansvar for å gjenopprette kritiske IKT-tjenester på en hensiktsmessig måte. Det kan i noen tilfeller bety at det må gjøres prioriteringer både mellom tjenester, og mellom foretak. Fokus skal være på å ta effektive (raske og gode) beslutninger for å redusere konsekvenser av hendelsen.

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 direktør for Medisin- og helsefag. Direktør for Teknologi og eHelse kan bistå med råd for å treffe beslutningen. Eventuell videre eskalering i det regionale helseforetaket følger vanlige eskaleringsrutiner til viseadministrerende og administrerende direktør. Disse eskaleringspunktene er i samsvar med det regionale helseforetakets oppdragsavtale med Sykehuspartner om eskalering i andre situasjoner.

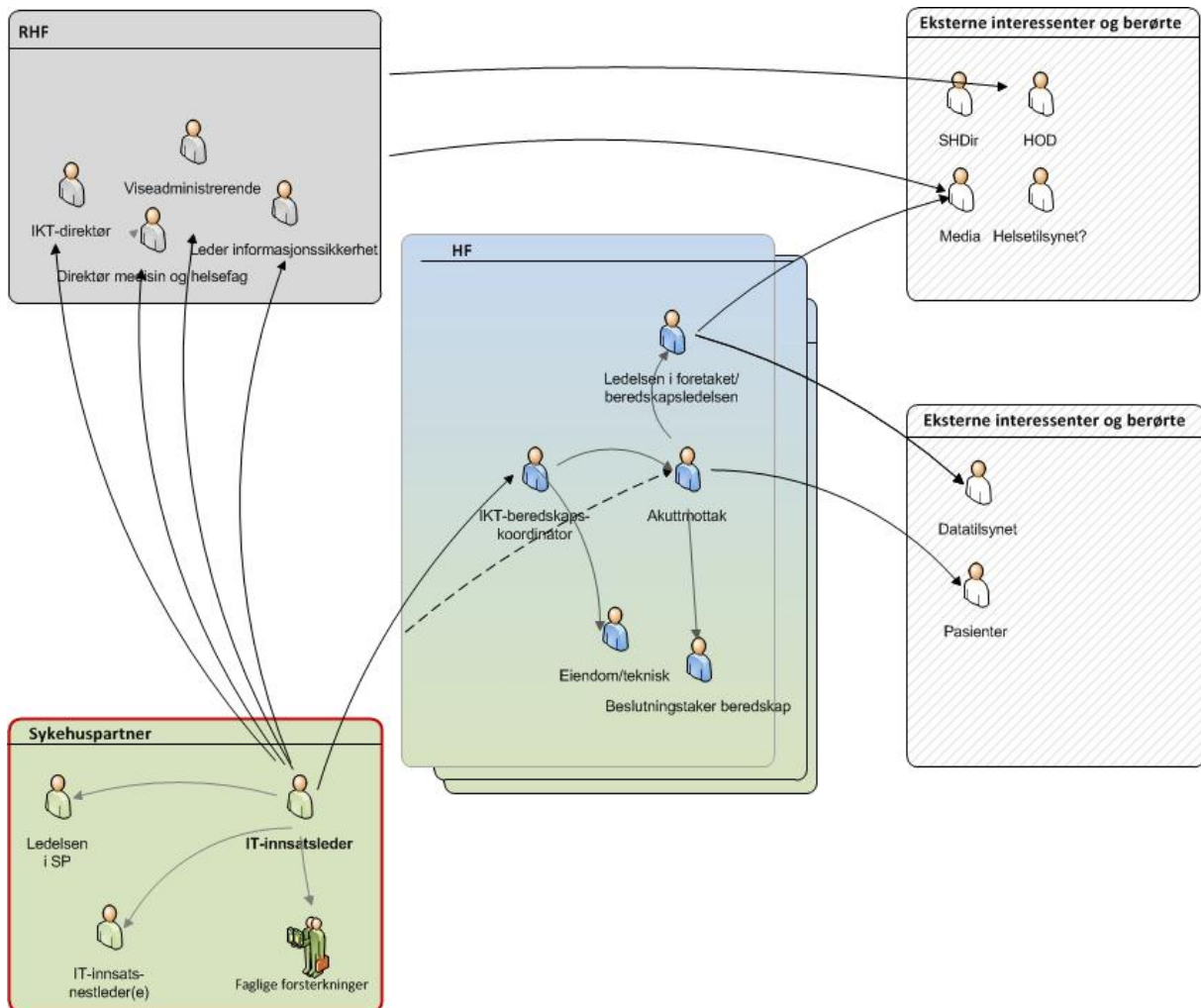


Figur 2: Eskalering

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.

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 IKT-systemer levert av SP
- Kritisk svikt i eventuelle andre IKT-systemer
- Svikt i telefonisystem
- Svikt i personsøkersystem

Videre skal det finnes en beskrivelse av de rollene som foretaket i følge 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 beredkapsorganisasjon 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 SP
- 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, 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 beredkapsrutiner.

Øving av varslingsrutiner og beredkapsplanene skal skje regelmessig i SP og i henhold til de lover, regler og krav som er stilt til helseforetakene samt SPs IKT-leveranseorganisasjon per 1. september 2009. Det må etableres en egen øvingsplan.

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

7 Krav til Helse Sør-Øst RHFets IKT-beredskap

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

- Direktør for Medisin og helsefag
- Direktør for Teknologi og eHelse
- Leder informasjonssikkerhet

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.

A. Referanser

Styringssystem for informasjonssikkerhet for <foretak>

Norm for informasjonssikkerhet i helsesektoren

Regional beredskapsplan

SP_Felles_Beredskapsplan_v.1.1

Veilder 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 ledergruppa i Teknologi og eHelse i RHFet.
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 eHelse
Versjon 1.2	TP: Oppdatering ved revisjon mars/april 2014