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

Bruk av veilederen

Bakgrunn

Fra regional beredskapsplan: «Helseforetakenes forpliktelse til å utarbeide og vedlikeholde egne beredskapsplaner fremgår av «Lov om helsemessig- og sosial beredskap». Dette er også videreført i helseforetakenes oppdrag og bestilling, senest for 2010, der det fremgår helseforetakenes beredskapsplaner til en hver tid skal være oppdaterte, øvede og koordinerte med rutiner for å oppdage og varsle hendelse og for effektiv ressursdisponering og samhandling ved kriser».

Spesialisthelsetjenesten benytter i økende grad IKT-systemer som støtteverktøy for virksomhetsprosesser. Det er derfor nødvendig å ha en god prosess for beredskap også innenfor IKT-området. Hensikten med denne veilederen er å gi innspill til hvordan dette arbeidet kan gjennomføres.

Målgruppe for veilederen

Ansvarlig for IKT-beredskapsplaner og beredskapssjef i foretaket er i hovedsak målgruppe for veilederen. De må involvere andre roller og funksjoner der det er nødvendig og hensiktsmessig.

Planlegging av IKT-beredskap og kontinuitet

Målet med arbeidet er å komme fram til et sett med planer som beskriver **roller, kommunikasjon og ansvar** for ulike aktiviteter. Disse skal være til hjelp ved beredskapshendelser som involverer IKT.

Grunnlaget for god IKT-beredskap og kontinuitet ligger i **god planlegging**. En viktig del av dette igjen er grundige og oppdaterte risikovurderinger, inkludert konsekvensanalyser. Ved hjelp av disse finner man ut hvilke virksomhetsprosesser som er kritiske. Det igjen avgjør hvilke tjenester som må støttes av beredskapsplanene, hvilke scenarioer som må utarbeides og hvor det er behov for nødrutiner. Risikovurderingene må gjøres av foretakene, og resultatene kan bli forskjellige for ulike foretak.

For det kliniske miljøet og virksomhetssiden ellers handler beredskap i stor grad om å iverksette nødrutiner og sørge for at pasientsikkerhet opprettholdes. Dette griper direkte inn i beredskapsplaner på andre områder. Denne veilederen har ikke til hensikt å legge føringer for hvordan arbeidet med nødrutiner og annet beredskapsarbeid gjøres i foretaket, men kommer med innspill til hvordan foretakene kan sikre at de også planlegger nødrutiner i forbindelse med kritiske IKT-hendelser og at nødrutinene støttes av IKT-løsninger der det er relevant.

Det er en kjensgjerning at det å hente fram planene ikke alltid er det første man gjør når det oppstår kritiske situasjoner. Det er derfor viktig at de som kommer til å håndtere situasjonen i størst mulig grad har vært involvert i å utvikle planene. Å bidra i planlegging, revisjoner, jevnlig gjennomlesing av planer inkludert rutiner og øvelser sørger for at reaksjoner sitter i ryggmargen i størst mulig grad.

Ettersom status på beredskapsarbeidet knyttet til IKT-hendelser i foretakene er ganske ulik, har vi valgt å ta utgangspunkt i at det ikke finnes planer for å håndtere IKT-kriser i foretaket. Vi håper dermed at veilederen kan være til stor hjelp for de som har større mangler innenfor beredskapsarbeidet, men også at det kan være nyttige ting å ta med seg for de som allerede har gjort en del innenfor området. Veilederen stiller ingen krav til

utseende og form på planene. Tvert i mot forventes det at de tilpasses foretakets øvrige kvalitetssystem. I Vedlegg C: Mal finnes imidlertid et forslag til hvordan en beredskapsplan for IKT-kriser kan se ut.

Flere av foretakene har i arbeidet med veilederen påpekt at de anser IKT-beredskap for å være Sykehuspartners ansvar, og at de selv har fokus på beredskap. Det er ingen tvil om at Sykehuspartner har ansvaret for den operative håndteringen, men foretakene har også en viktig rolle i disse situasjonene. Når vi snakker om IKT-beredskap i dette dokumentet handler det med andre ord om det foretaket må gjøre ved en IKT-krise.

Siste del av innledningen oppsummerer hvilke oppgaver som er beskrevet i veilederen. Foretaket står selvsagt fritt til å inkludere punkter som ikke er dekket i veilederen. Slike tillegg kan det gjerne meddeles ansvarlig for veilederen dersom det kan være av interesse for andre foretak.

Oppsummering av oppgaver beskrevet i veilederen

- Gjennomføre risikovurdering, inkludert konsekvensanalyse → identifisere kritiske virksomhetsprosesser.
- Utnevne ansvarlig for IKT-beredskapsplanlegging i foretaket, heretter kalt IKT-beredskapsansvarlig i foretaket
- Utarbeide og implementere planer for IKT-beredskap og kontinuitet av virksomhetsprosesser ved bortfall av IKT. Husk å inkludere flest mulig potensielle interessenter og aktører.
    - Utarbeide nødrutiner for kritiske virksomhetsprosesser.
    - Beskrive ansvarsforhold internt.
    - Beskrive varslings- og informasjonsrutiner internt i foretaket i en IKT-hendelse.
- Opprette rammeverk for forvaltning
    - Planlegge og gjennomføre opplæring og øvelser
    - Planlegge revisjoner

Lykke til med arbeidet!

Ordliste/definisjoner

IKT-beredskapssituasjon	Rød beredskap i Sykehuspartner som gir konsekvenser for foretak.
Gjenoppretting	Gjenopprette en tjeneste med midlertidige prosesseringsløsninger på alternativt/midlertidig driftssted, for dermed å kunne gjenoppta produksjon så raskt som mulig. Foregår etter fastsatt prioritering for hva som er mest kritisk.
IKT-beredskapsplan	Begrepet brukes i dette dokumentet for planer som skal avhjelpe håndtering av IKT-beredskapssituasjoner uavhengig av nivå (operativt, taktisk, strategisk) og organisasjon (foretak, Sykehuspartner, Helse Sør-Øst RHF).
IKT-beredskapsansvarlig	Den som er ansvarlig for å utarbeide IKT-beredskapsplan
IKT-beredskapskoordinator	IKT-rolle i foretaket i en beredskapssituasjon.

1. Innledning

1.1.Hensikt

Hensikten med IKT-beredskap er som all annen beredskap i Helse Sør-Øst; å sørge for at pasientene i størst mulig grad får den behandling de har krav på og behov for, også i ekstraordinære situasjoner.

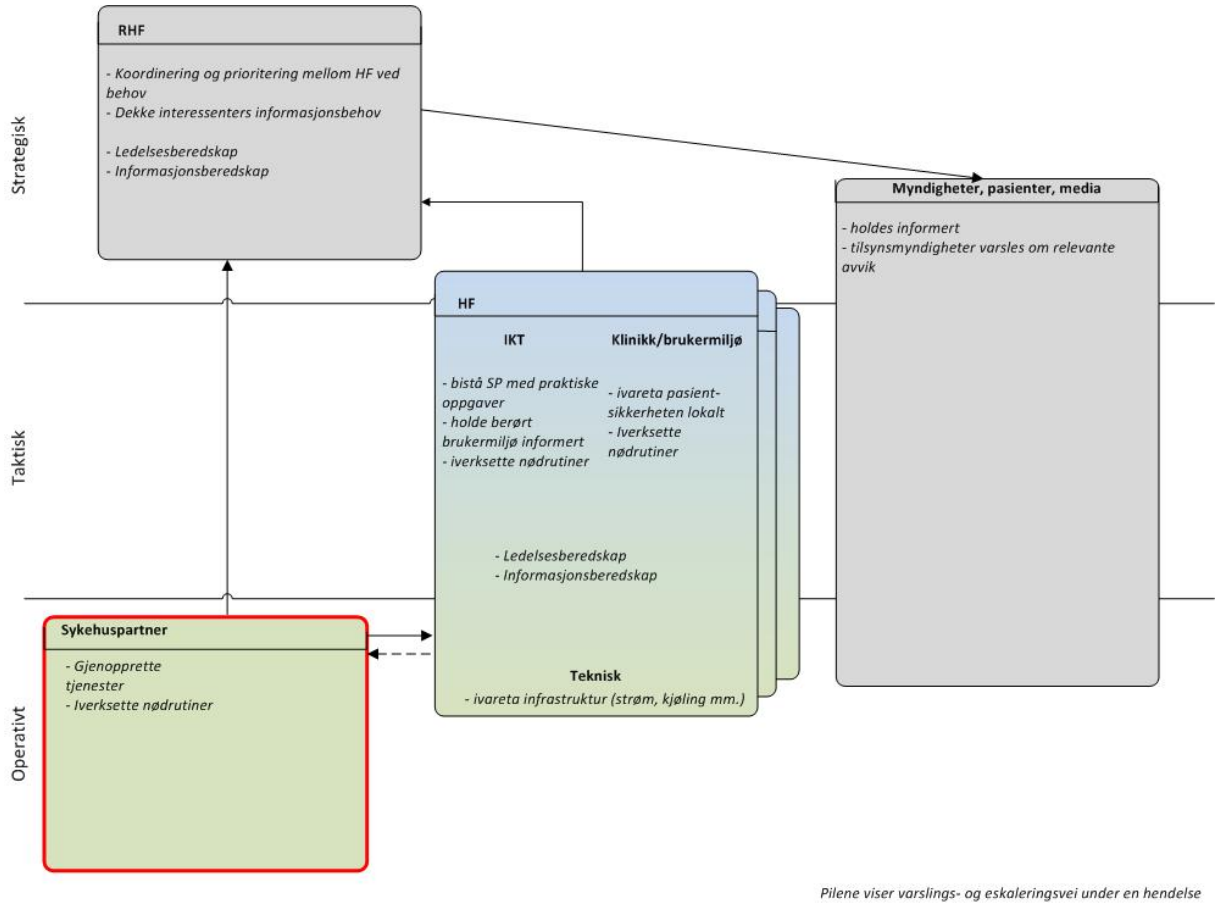
Foretakets IKT-beredskapsplaner skal understøtte to ulike situasjoner:

- Svikt i kritiske IKT-tjenester
- Beredskapssituasjoner i foretaket som krever bistand fra IKT

1.2.Ansvar og foretakets oppgaver

Figur 1 viser aktører involvert i en IKT-relatert beredskapssituasjon, samt hvilke ansvarsområder de ulike aktørene skal håndtere. Veilederen gir et forslag til hvordan ansvaret i foretaket kan implementeres. Dette må imidlertid tilpasses det enkelte foretak; både størrelse, organisering, ansvarsområder og andre faktorer vil påvirke implementasjonen. Uansett hvordan foretaket velger å implementere, skal følgende oppgaver ivaretas:

- Bistå Sykehuspartner i operativ håndtering ved behov for eksempel for lokalkunnskap
- Varsle nødvendige ressurser og interessenter i egen organisasjon
- Varsle nødvendige tilsynsmyndigheter, pasienter
- Iverksette lokale nødprosedyrer
- Ivareta infrastruktur (strøm, kjøling)



Figur 1: Aktører involvert i en IKT-relatert beredskapsituasjon

1.3.Omfang

Veilederen omhandler i hovedsak kritisk bortfall av IKT-tjenester levert av Sykehuspartner. Medisinsk-teknisk utstyr er i utgangspunktet ikke med i delplanen. Dersom foretaket ønsker det, er det selvsagt ingenting i veien for å inkludere det, for eksempel i scenarioer og varslingslister.

Sykehuspartner iverksetter sin beredskapsplan dersom det inntreffer en såkalt 1A-hendelse som forventes å vare i mer enn 1 time. Hvilke tjenester som kategoriseres med «kritikalitet 1» må komme ut av risikovurderinger. Disse tjenestene bør listes opp i IKT-beredskapsplanen.

En hendelse av type 1A har for øvrig 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**

Det er viktig å huske på at kritisk bortfall av IKT-tjenester ikke nødvendigvis fører til høyere beredskapsnivå enn grønt i foretakene, slik at retningslinjer og rutiner for eksempel for varslinger som gjelder for gul og rød beredskap ikke direkte aktiveres.

I tillegg skal beredskapsplanene innenfor IKT **legge til rette for IKT-støtte** i situasjoner der foretaket er i gul eller rød beredskap.

1.4.Produkter av etableringen i foretaket

Ved å følge veilederen vil foretaket ende opp med en del dokumenter. Disse er oppsummert i

Tabell 1, sammen med hvem som er sannsynlig bruker av dokumentet.

Dokumenter som bør utarbeides	**Bruker av dokumentet (også hensiktsmessig at disse er med i utarbeidelse av dokumentet)**
Kategorisering av tjenester	Brukermiljø i foretakene, Sykehuspartner, IKT-beredskapskoordinator
Rollebeskrivelse IKT-beredskapskoordinator	IKT-beredskapskoordinator
Andre rollebeskrivelser	Aktuelle roller
Nødrutiner ved bortfall av kritiske IKT-tjenester	Berørt brukermiljø, ansvarlig for iverksettelse av nødrutine
Varslingsrutiner	Ansvarlige for varsling i en kritisk IKT-hendelse
Varslingslister	Ansvarlige for varsling i en kritisk IKT-hendelse
Varslingsrutiner til IKT i beredskapssituasjoner	Funksjon ansvarlig for å varsle IKT i en beredskapssituasjon i foretaket.

Tabell 1: Produkter av etableringen

2. Håndtering av kritiske IKT-hendelser

Kapittel 2 handler om hvordan kritiske IKT-hendelser bør håndteres i foretaket. Det inneholder en beskrivelse av ulike aktiviteter som er nødvendig å planlegge, forslag til konsekvensscenarioer og en sjekkliste for utarbeidelse av nødrutiner. Husk at Sykehuspartner har hovedansvar for gjenoppretting av IKT-tjenester.

2.1 Roller og aktiviteter

Ulike roller vil være involvert i kritiske IKT-hendelser. Under følger en sannsynlig og anbefalt fordeling av aktiviteter for ulike funksjoner i foretaket:

- IKT bistår Sykehuspartner i å løse IKT-hendelsen og sørger for korrekt informasjon til foretaket for øvrig.
- Eiendomsavdeling/teknisk må bidra med bistand på sine ansvarsområder (strøm, kjøling osv.)
- Foretaket ellers bidrar til å opprettholde sykehusets funksjoner.

Under følger Tabell 2 med en oversikt over aktiviteter som bør utføres under en kritisk IKT-hendelse, og hvilke roller som kan ha ansvaret for aktiviteten. Det kan være at foretaket ser behov for å gjennomføre andre aktiviteter, og disse kan da selvsagt inkluderes. Det er også viktig å merke seg at flere av aktivitetene ikke er spesifikke for kritiske IKT-hendelser, slik at det i mange tilfeller kun vil være snakk om en oppdatering av eksisterende rutiner.

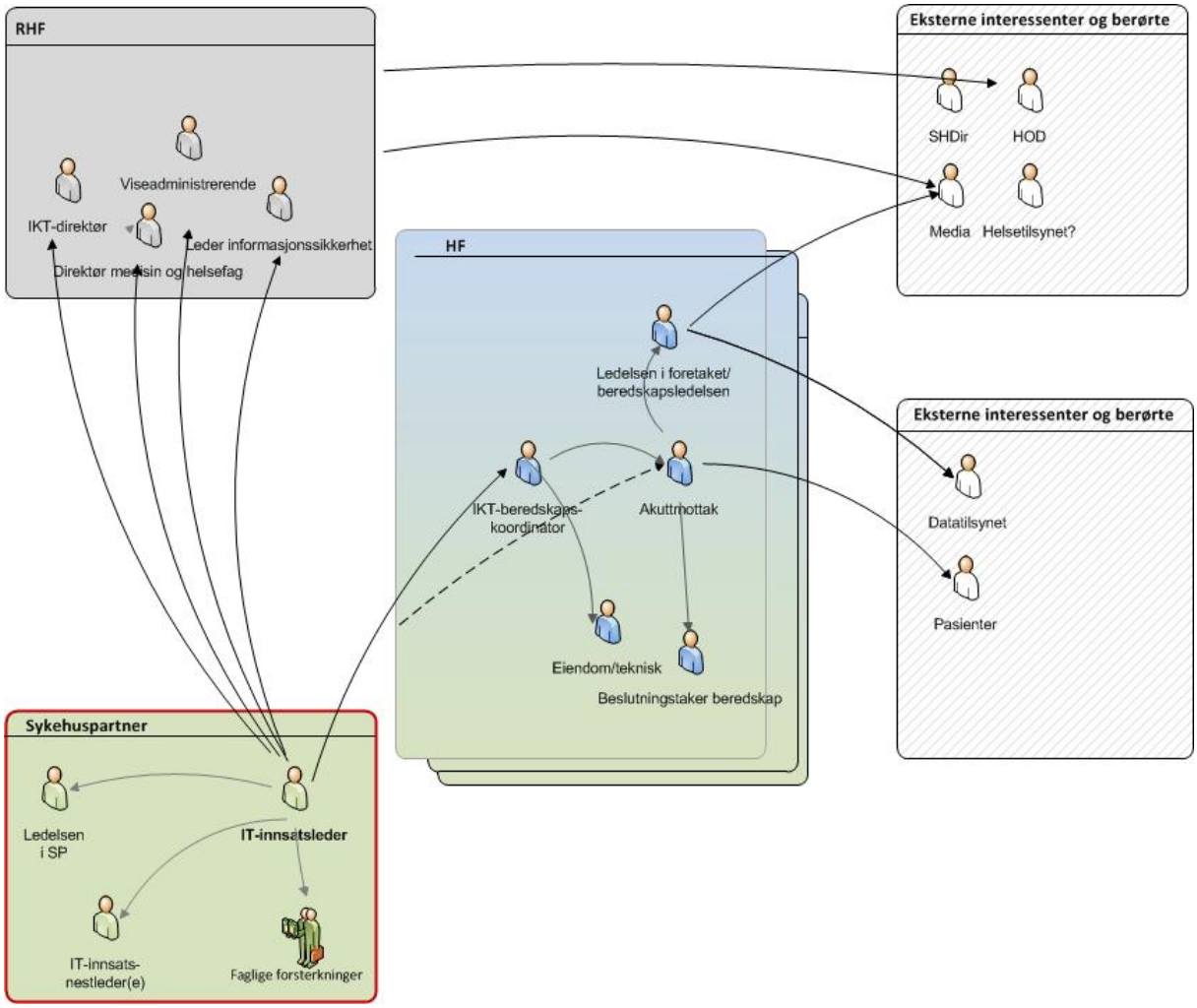
	Akuttmottak AMK	Berørt brukermiljø	Foretaksledelse / Beredskapsledelse	Medie-kontakt	Teknisk	IKT-beredskapskoordinator	Sykehus-partner
Varsling							
Varsle Sykehuspartner	Den som oppdager en kritisk IKT-hendelse.						
Varsle akuttmottak/AMK						X	X
Varsle berørte kliniske miljøer	X						
Varsle ledelse/beredskaps-ledelsen	X						
Varsle teknisk i foretaket						X	
Aktiviteter under hendelsen							

Sette beredskapsnivå[1]	X		X				
Utnevne operativ innsatsleder og iverksette nødrutiner	X	X					X
Prioritering av tjenester og beslutninger utenfor IKT-beredskapskoordinators myndighet			X				
Informere internt i foretaket om status i hendelsen						X	
Kommunikasjon med pasienter		X					
Informasjon fra foretak til media				X			
Bistå i problemløsning innenfor strøm, kjøling, medisinsk-teknisk utstyr osv.					X		
Eskalere til Helse Sør-Øst RHF			X				
Aktiviteter etter hendelsen							
Delta i debrief	Alle berørte					X	(X)

Tabell 2: Aktiviteter i en kritisk IKT-hendelse

Varslinger i tabellen er i henhold til

[1] Ansvarlig varierer fra foretak til foretak, derfor to kryss i tabellen.



Figur 2: Varsling i en kritisk IKT-hendelse

Ved utarbeidelse av foretakets IKT-beredskapsplan må foretaket også selv vurdere hvilke roller som skal bistå i håndteringen, og gjennom planen sørge for at disse blir varslet og holdt tilstrekkelig informert. Det bør også vurderes om det skal opprettes tiltakskort for rollene, se vedlegg A for forslag.

Det er i veilederen ikke laget egne rollebeskrivelser for andre enn IKT-beredskapskoordinator, ettersom andre roller i hovedsak skal ivareta samme oppgave som i andre beredskapssituasjoner. Det kan allikevel være at foretakene ønsker å lage rollebeskrivelser for flere roller, eller inkludere aktiviteter identifisert i arbeidet med IKT-beredskap i eksisterende rollebeskrivelser.

Alle aktiviteter som er felles for alle konsekvensscenarioer bør listes opp i en liste i foretakets IKT-beredskapsplan, og løses på samme måte uavhengig av hendelse.

Vi har i dette avsnittet også laget en mer detaljert beskrivelse av aktivitetene i tabellen, samt skrevet noen tips for etableringen under de fleste av aktivitetene.

2.1.1 Beskrivelse av de ulike aktivitetene i tabell 2

Under følger en mer utfyllende beskrivelse av de ulike aktivitetene listet opp i tabell 2

Varsling

Varsle Sykehuspartner	
Beskrivelse	Den som oppdager en hendelse knyttet til IKT, skal varsle Sykehuspartner gjennom Kundesenteret/ Brukerstøtte på dagtid eller til lokal vakt utenfor avtalt arbeidstid. For mer informasjon om varsling av Sykehuspartner i forbindelse med IKT-hendelser,ta kontakt med kundeansvarlig.
Tips	- Rutiner for å varsle Sykehuspartner må innarbeides og gjøres kjent hos ulike roller. Dette kan for eksempel gjøres ved å opprette en «Meldeplakat» der varsling til Sykehuspartner inkluderes. (Meldeplakat er èn A4-side med viktige kontakter som kan henges opp rundt omkring der det er behov).

Varsle akuttmottak/AMK	
Beskrivelse	Noen hendelser vil oppdages av Sykehuspartner før det er synlig for foretaket. Dersom det er en så kritisk hendelse at det kan være umiddelbar fare for liv og helse ønsker Sykehuspartner å varsle nærmest mulig berørt brukermiljø. Det vil for de fleste foretak i praksis si til akuttmottak eller AMK. I tillegg varsles kontaktperson på IKT. Denne varsles også i tilfeller hvor Sykehuspartner ikke vurderer hendelsen som like kritisk. Kontaktperson på IKT må da gjøre videre vurdering av behov for varsling til klinisk miljø. Initiell varsling skal gjøres per telefon. Det er viktig at varslingen fra Sykehuspartner mottas på riktig måte. De som sitter som potensielle mottakere av disse varslingene, må derfor være klar over at de kan få dem. Sykehuspartner har i slike situasjoner ansvar for å overbringe mest mulig nøyaktig informasjon i slike situasjoner. Det er ønskelig at det i størst mulig grad er ett kontaktpunkt inn i det kliniske miljøet for Sykehuspartner. Det er flere årsaker til det: - Enklere rutiner for Sykehuspartner - Enklere opplæring av de som potensielt skal motta varslinger - Kontaktpunktet bør være tilgjengelig i hele tidsperioden kritisk IKT-svikt kan inntreffe. På grunn av organisering og geografi kan det å tilby ett kontaktpunkt for enkelte foretak være lite hensiktsmessig å innfri. Ett kontaktpunkt er derfor ikke et absolutt krav.

Tips	- Foretaket må i størst mulig grad tilby ett kontaktpunkt i det kliniske miljøet for Sykehuspartner. - Dette kontaktpunktet må få tilstrekkelig opplæring i å motta denne type varslinger.

Varsle berørte kliniske miljøer	
Beskrivelse	Etter å ha mottatt initiell varsling, enten fra Sykehuspartner eller IKT i foretaket, må kontaktpunktet i forrige aktivitet (akuttmottak/AMK for de fleste) varsle berørte brukermiljøer. Det må finnes en rutine for dette, samt oppdaterte varslingslister. Dette bør gjøres på samme måte som for andre typer hendelser. Det må også her sikres at mottaker av beskjeden forstår innholdet tilstrekkelig til å handle hensiktsmessig.
Tips	- Det må finnes varslingslister tilgjengelig i akuttmottak/AMK (eller hos tilsvarende funksjon) som også fungerer for IKT-hendelser.

Varsle ledelsen/beredskapsledelsen i foretaket	
Beskrivelse	Det må defineres hvem som har ansvar for å varsle ledelsen i foretaket i en kritisk IKT-hendelse. I følge regional beredskapsplan gjøres dette normalt av akuttmottak eller AMK, men foretaket bør ta en diskusjon på hvorvidt dette er hensiktsmessig også i kritiske IKT-situasjoner.
Tips	- Det må avklares hvilken rolle som varsler ledelsen/beredskapsledelsen - Det må finnes rutiner for å varsle ledelsen/beredskapsledelsen

Varsle eiendomsavdeling/teknisk i foretaket	
Beskrivelse	Ettersom foretakene selv har ansvar for teknisk infrastruktur, er det viktig at det etableres kommunikasjon mellom Sykehuspartner og teknisk, dersom hendelsen tilsier det. Varsling av teknisk kan for eksempel gjøres av IKT-beredskapskoordinator, fortrinnsvis per telefon.
Tips	- Det må avklares hvilken rolle som varsler teknisk - Det må finnes rutiner og varslingslister for å varsle teknisk

Varsle mediekontakt	
Beskrivelse	Mediekontakt må varsles om hendelsen, for å kunne vurdere kommunikasjonsstrategi for hendelsen.
Tips	- Det må avklares hvilken rolle som varsler mediekontakt - Det må finnes rutiner og varslingslister for å varsle mediekontakt

Aktiviteter under hendelsen

Sette beredskapsnivå	
Beskrivelse	Denne rollen må varsles og holdes informert om utviklingen i hendelsen. For de fleste foretak vil andre aktiviteter i **Tabell 2** være tilstrekkelig for å sørge for dette.
Tips	- Det må finnes rutiner som sørger for at ansvarlig for å sette beredskapsnivå er informert om utviklingen i hendelsen. - Det må avklares hvilken rolle som holder ansvarlig for beredskapsnivå oppdatert.

Utnevne operativ innsatsleder og iverksette nødrutiner	
Beskrivelse	Nødrutiner iverksettes i berørte kliniske miljøer etter deres retningslinjer.
Tips	- Se avsnitt 4 for innspill til nødrutiner

Prioritering av tjenester og beslutninger utenfor IKT-beredskapskoordinators myndighet	
Beskrivelse	Selv om det gjennom ROS-analyser er gjort en vurdering av viktigheten av tjenestene, kan det være at omstendigheter rundt hendelsen gjør det nødvendig å gjøre omprioriteringer. Det kan også være andre beslutninger som ligger utenfor IKT-koordinators myndighet. Slike avgjørelser må tas av ledelsen i foretaket, etter innspill fra for eksempel Sykehuspartner og IKT-beredskapskoordinator. Om nødvendig kan Helse Sør-Øst RHF ved direktør for teknologi og eHelse involveres for endelig prioritering som beskrevet i regional delplan for håndtering av IKT-hendelser.
Tips	- Lage rutiner som sørger for å involvere beslutningstakere i større beslutninger utenfor IKT-beredskapens myndighet - Forbered disse på problemstillinger de kan bli presentert for

Informere internt i foretaket om status i hendelsen

Beskrivelse	For i størst mulig grad å hindre uønskede tiltak og støy, er det viktig å informere interessenter tilstrekkelig. IKT-beredskapskoordinator i foretaket vil sitte med kommunikasjon mot Sykehuspartner, og bør være ansvarlig for å bringe informasjonen videre til andre i foretaket. Det kan bety å informere akuttmottak/AMK, dersom ansvaret for å informere videre ligger der. Det må uansett lages en rutine som sikrer at berørte brukermiljø og andre interessenter får tilstrekkelig informasjon. Informasjon gis i størst mulig grad per normale kommunikasjonskanaler, men det er viktig å tenke på hva man gjør om for eksempel e-post er utilgjengelig. Det er også viktig å ta hensyn til situasjonen mottaker av informasjonen er i. Helsepersonell sjekker ikke nødvendigvis e-post og meldinger på Intranett like hyppig som kontormedarbeidere.
Tips	- Etablere rutine som sikrer foretaket tilstrekkelig informasjon i en kritisk IKT-hendelse

Kommunikasjon med pasienter	
Beskrivelse	All informasjon til pasienter skal komme fra det kliniske miljøet hvor pasienten behandles eller skulle vært behandlet.
Tips	

Informasjon fra foretak til media	
Beskrivelse	Mediekontakt i foretaket må holdes oppdatert om status, i tilfelle det er aktuelt å kommentere hendelsen i media.
Tips	- Lag rutiner for mediekontakt for orientering om IKT-hendelser, for eksempel: o Bør ikke uttale seg om tekniske detaljer o Pass på å ikke plassere skyld for situasjonen som har oppstått - Forbered mediekontakt på mulige situasjoner som kan oppstå for eksempel gjennom øvelser

Bistå i problemløsning innenfor strøm, kjøling, medisinsk-teknisk utstyr.	
Beskrivelse	Eiendomsavdeling/teknisk avdeling må bistå Sykehuspartner i problemløsing som involverer fysiske faktorer som de har ansvar for. Ansvarlige for medisinisk-teknisk utstyr må bistå i feilsituasjoner som inkluderer denne typen utstyr.
Tips	

Eskalere til Helse Sør-Øst RHF

Beskrivelse	I en kritisk IKT-hendelse varsler Sykehuspartner Helse Sør-Øst RHF. Dersom denne utløser noen av kriteriene for varsling av Helse Sør-Øst RHF, skal også foretaket varsle. Dersom det oppstår situasjoner hvor berørte foretak og Sykehuspartner ikke blir enige om for eksempel prioriteringer, kan situasjonen eksaleres til Helse Sør-Øst RHF.
Tips	

Aktiviteter etter hendelsen

Delta i debrief	
Beskrivelse	Vi foreslår at det gjennomføres en debrief i foretaket med deltakere fra berørte brukermiljø, ledelse, IKT-beredskapskoordinator og representant i Sykehuspartner, der IKT-beredskapskoordinator er ansvarlig for gjennomføringen. Fokus her bør være på det som skjedde internt i foretaket, og i grensesnittet mot Sykehuspartner (Sykehuspartner skal holde egne debriefinger, gjerne med deltakelse fra IKT-beredskapskoordinator i foretaket, knyttet til den operative håndteringen av selve IKT-hendelsen).
Tips	- Lag rutine for gjennomføring av debriefingsmøte. Sørg for at innspill til Sykehuspartner og andre relevante aktører kommer fram til mottaker på en konstruktiv måte.

2.1.2 IKT i foretaket

Oppgaver:

- Motta varslinger fra Sykehuspartner om IKT-beredskapssituasjon.
- Være Sykehuspartners kontaktperson ved foretaket.
- Varsle foretakets beredskapsledelse/ledelse.
- Styre egne IKT-ressurser for å sikre at Sykehuspartner får nødvendig lokalkunnskap i en beredskapssituasjon.
- Bistå Sykehuspartner med praktiske oppgaver, slik som å skaffe til veie arbeidsplasser og andre nødvendige ressurser som krever lokalkunnskap.
- Holde interessenter i foretaket informert.
- Bistå klinikken i å legge til rette for gjennomføring av nødrutiner, og å vurdere konsekvensen disse i forhold til videre problemløsning.

IKT-beredskapskoordinator

I veilederen legger vi oppgavene til rollen IKT-beredskapskoordinator. Selv om disse oppgavene i veilederen er tillagt én rolle, må det vurderes i de enkelte foretak om dette er hensiktsmessig. For store foretak, særlig der det er stor geografisk spredning på lokasjonene, kan det være nødvendig å dele opp denne rollen eller ha flere personer til å fylle rollen.

IKT-beredskapskoordinators myndighet i en kritisk IKT-hendelse må avklares i planleggingen. En mulighet er å gi IKT-beredskapskoordinator samme myndighet som leder for IKT i foretaket i en normalsituasjon. Myndighet bør stå i IKT-beredskapskoordinators rollebeskrivelse, og det må gjøres opplæring av de som potensielt innehar denne rollen i en kritisk IKT-hendelse. Det må også kommuniseres til andre deler av organisasjonen, slik at IKT-beredskapskoordinator ikke får problemer med å utøve sin myndighet i en større hendelse. Opplæring og bevisstgjøring av rollen kan gjerne gjennomføres ved øvelser.

Husk også at det er naturlig at IKT-beredskapskoordinator har en rolle i situasjoner med gul eller rød beredskap i foretaket. Det er noe mer beskrevet i kapittel 0.

Se vedlegg A for forslag til tiltakskort for IKT-beredskapskoordinator.

Vi anbefaler for øvrig at IKT, og da gjerne gjennom rollen IKT-beredskapsansvarlig, inkluderes i foretakets beredskapsutvalg.

3. Konsekvensscenarioer

Basert på risikovurderinger og konsekvensanalyse i foretaket skal det identifiseres ulike scenarioer som beskriver hendelser som kan gi uønskede konsekvenser (konsekvensscenarioer). Fokuset for disse scenarioene er IKT-relatert. Noe av hensikten med scenarioene er selvsagt for å ha dokumentert hva som gjøres i ulike situasjoner. Men vel så viktig er selve jobben med å utarbeide scenariene, ettersom dette er en god måte å sørge for at tilstrekkelige nødrutiner og rollebeskrivelser blir dokumentert ute i foretakene.

Under følger noen eksempler på scenarioer:

1. Svikt i personsøkersystem -> personell kan ikke tilkalles over personsøkersystem
2. Svikt i telefonisystem -> personell kan ikke tilkalles over ordinært telefonisystem
3. Alvorlig svikt i IKT-systemer -> Brukermiljø i foretaket har ikke tilgang til pasientjournaler
4. Alvorlig svikt i IKT-systemer -> Brukermiljø i foretaket har ikke tilgang til laboratorieresultater
5. Alvorlig svikt i IKT-systemer -> Røntgen kan ikke utføres
6. Alvorlig svikt i IKT-systemer -> Bilder eller prøvesvar er ikke tilgjengelig på operasjonsstua

«Aktiviteter» bør inneholde hva foretaket som helhet må gjøre for det spesifikke scenarioet. Aktivitetene i avsnitt 2.1 som er like for alle scenarioer kan enten repeteres i de ulike scenarioene, eller de kan beholdes i et eget avsnitt i planen.

Kolonnen «ansvarlig» skal inneholde rollenavnet som er ansvarlig for at aktiviteten blir utført. Det kan være ulike roller eller enheter, som akuttmottak, AMK, klinikk, avdeling, IKT-beredskapskoordinator, Sykehuspartner, beredskapssjef osv., avhengig av aktivitet som skal uføres. Det kan være flere ansvarlige for en aktivitet, men det bør da vurderes om aktiviteten skal deles opp, slik at det ikke oppstår uklarheter rundt ansvar. Utførende for de ulike aktivitetene vil i hovedsak stå i selve nødrutinen, og er derfor ikke inkludert i disse tabellene.

Tabellene under viser eksempler på hvordan det kan se ut for det som i lista over er scenario 1 og scenario 4.

1. Svikt i personsøkersystem -> personell kan ikke tilkalles over personsøkersystem

<Dersom det er spesielle rutiner som gjelder for akkurat det scenarioet, kan det beskrives her. Det bør imidlertid tilstrebes at alt er mest mulig likt for ulike typer scenarioer.

Nødrutiner vil være ulike, og det beskrives her. >		
Aktivitet	**Ansvarlig**	**Kommentar/beskrivelse**
Iverksettelse av nødrutiner	<Enhet/rolle> *Eksempel: Akuttmottak*	<Link til nødrutine> *Eksempel: Kontakte nødvendig personell på mobiltelefoner*

……

3. Alvorlig svikt i IKT-systemer -> Brukermiljø i foretaket har ikke tilgang til pasientjournaler <Dersom det er spesielle rutiner som gjelder for akkurat det scenarioet, kan det beskrives her. Det bør imidlertid tilstrebes at alt er mest mulig likt for ulike typer scenarioer. Nødrutiner vil være ulike, og det beskrives her. >		
Aktivitet	**Ansvarlig**	**Kommentar/beskrivelse**
Iverksettelse av nødrutiner	<Enhet/rolle> *Eksempel: Berørt brukermiljø*	<Link til nødrutine> *Eksempel: Skrive ut alle journaler på papir*

4. Nødrutiner

For hendelser som medfører uønskede konsekvenser for virksomhetsprosesser, kan det være nødvendig å iverksette nødrutiner. I IKT-planen bør det være en kort beskrivelse av aktuelle nødrutiner, med hovedfokus på hvem som er ansvarlige for å utvikle og iverksette rutinene. Selve nødrutinene bør dokumenteres andre steder enn i denne planen, men det kan gjerne legges inn en link til relevante nødrutiner.

Ansvar for nødrutiner vil være delt mellom ulike roller avhengig av hensikten med den spesifikke nødrutinen.

Følgende sjekkliste i forbindelse med nødrutiner kan være til hjelp for å sikre at de er tilstrekkelige:

- Det finnes dokumenterte nødrutiner for alle kritiske virksomhetsprosesser ved kritisk svikt i IKT-tjenester identifisert i risikovurderinger.
- Brukerne av virksomhetsprosessen er kjent med nødrutinene.
- Nødrutinen har en eier som er ansvarlig for oppdatering, testing og opplæring.
- Nødrutinene er utarbeidet av en tverr-faglig gruppe (brukere av virksomhetsprosess, IKT, teknisk, Sykehuspartner osv.). Hensikten med dette er selvsagt å hjelpe hverandre med å komme fram til rutiner som fungerer best mulig.
- Nødrutiner oppbevares med et fornuftig sikkerhetsnivå (konfidensialitet og integritet), samt er tilgjengelige dersom det skulle være nødvendig i en kritisk IKT-hendelse (husk at det kan være nettverksbrudd som er årsak til hendelsen, da hjelper det lite å ha dokumenterte nødrutiner på ekstern server).

- Nødrutinene inkluderer opprydning etter at selve hendelsen er løst. Et eksempel på det kan være innføring av notater i pasientjournal.

Merk: Det kan også være hensiktsmessig å inkludere Sykehuspartner under utarbeidelse av nødrutiner for andre områder enn bortfall av IKT-tjenester, for å sikre at nødrutinen er teknisk gjennomførbar dersom den bygger på tjenester levert av Sykehuspartner, og om det eventuelt krever spesiell støtte fra Sykehuspartner.

5. Foretak i rød beredskap

Et foretak i rød beredskap må varsle Sykehuspartner som beskrevet i vedlegg 4 i generell beredskapsplan og Sykehuspartners beredskapsplan. Det betyr at foretaket må lage rutiner for å varsle Sykehuspartner som beskrevet nedenfor:

Aktivitet	**Ansvarlig**	**Kommentar/beskrivelse**
Vurdering av behov for bistand fra Sykehuspartner	<Enhet/rolle>	
Varsling av Sykehuspartner	<Enhet/rolle>	Driftssenteret hos Sykehuspartner skal varsles: **22 73 42 60** Nødvendig informasjon: - Hva slags assistanse har foretaket behov for? - Trenger foretaket IT-innsatsleder fra SP?

Det kan også være nyttig å inkludere IKT i foretaket i situasjoner hvor foretaket er i gul eller rød beredskap. Blant annet vil det for de fleste foretak være hensiktsmessig at IKT varsler Sykehuspartner, og at kommunikasjonen her i størst mulig grad foregår på samme måte som for kritiske IKT-hendelser.

6. Etablering av forvaltningsrammeverk

For å holde selve beredskapsplanen enklest mulig, anbefaler vi at forvaltning beskrives i et eget forvaltningsrammeverk. Dette bør inneholde:

- Ansvarlig for forvaltning av IKT-beredskap
- Beskrivelse av andre relevante roller
- Plan for oppdatering
    - Rutiner for jevnlige oppdateringer
    - Husk informasjon til øvrig beredskapsorganisasjon, Sykehuspartner og RHFet ved relevante endringer
    - Husk særlig oppdatering av varslingslister og kontaktinformasjon
- Plan for opplæring
    - Hvem
    - Tidsplan
- Plan for øvelser (helst i samarbeid med øvrig beredskapsorganisasjon i foretaket og Sykehuspartner)
    - Hvem
    - Når
    - Hva

Forvaltningen av IKT-beredskapsplan bør være mest mulig samkjørt med øvrig beredskap i foretaket.

Vedlegg A: Tiltakskort IKT-beredskapskoordinator

For enkelte roller vil det være nyttig med tiltakskort. Dette gjelder i IKT-sammenheng særlig for IKT i foretaket, men kan også vurderes for andre roller.

Tiltakskortene bør være så korte og presise som mulig, aller helst på én A4-side, slik at den kan skrives ut og være lett tilgjengelig i sekken eller kontoret. Under følger et forslag til tiltakskort for IKT-beredskapskoordinator.

TILTAKSKORT FOR IKT-BEREDSKAPSKOORDINATOR	
IKT-beredskapskoordinator har oppgaver både i kritiske IKT-hendelser og i beredskapssituasjoner i foretaket. Forslag til oppgaver er beskrevet nedenfor. Der det ikke står spesifikt, gjelder oppgaven både i kritiske IKT-hendelser og i situasjoner som utløser gul/rød beredskap for foretakene.	
Husk!	**OPPGAVER**
Still spørsmål ved prioriteringer. Tenk konsekvenser. Før oversikt over interessenter som skal holdes oppdatert.	**<u>Under hendelsen:</u>** Motta varslinger fra Sykehuspartner om IKT-beredskapssituasjon. Være Sykehuspartners kontaktperson ved foretaket. Ved IKT-beredskapssituasjon: Varsle foretakets beredskapsledelse/ledelse innenfor IKT. Styre egne IKT-ressurser for å sikre at Sykehuspartner får nødvendig lokalkunnskap i en beredskapssituasjon. Bistå Sykehuspartner med praktiske oppgaver, slik som å skaffe til veie arbeidsplasser og andre nødvendige ressurser som krever lokalkunnskap. Ved IKT-beredskapssituasjoner: Holde interessenter i foretaket informert om status på hendelsen. Bistå klinikken i å legge til rette for gjennomføring av nødrutiner, og å vurdere konsekvensen disse i forhold til videre problemløsning. Eksempelvis kan en nødrutine være å kopiere bilder til minnepenn hvis nettverket er nede. Men, dersom årsaken til at nettverket er nede er virus som sprer seg via minnepenn, kan konsekvensen være at viruset sprer seg til andre systemer og nettverk, og nødrutinen bør derfor ikke gjennomføres Iverksette relevante nødrutiner. Eksempel: Pasientjournalsystem nede → Skrive ut rapporter fra server, distribuere manuelt. **<u>Etter hendelsen:</u>** Delta på debriefingsmøte med Sykehuspartner og internt i foretaket.

Vedlegg B: Referanser

08-00446-205 Prosedyre for risikovurdering_0995.docx 292405_1_0.docx

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

Vedlegg C: Mal

Hensikt:

Omfang:

Ansvar:

Håndtering:

Aktiviteter som er uavhengige av konsekvensscenarioer:		
Aktivitet	**Ansvarlig**	**Kommentar/beskrivelse**
Varsling		
Varsle Sykehuspartner	Den som oppdager kritiske hendelse på IKT.	Kundesenteret/ Brukerstøtte på dagtid eller til lokal vakt utenfor avtalt arbeidstid. Kontaktinfo: <legg inn riktig for ditt foretak>
Varsle akuttmottak/AMK	IKT-beredskapskoordinator eller Sykehuspartner.	
Varsle berørte kliniske miljøer		
Varsle ledelse/beredskaps-ledelsen		
Varsle teknisk i foretaket		
Varsle mediekontakt i foretaket		
Aktiviteter under hendelsen		
Sette beredskapsnivå		
Utnevne operativ innsatsleder og iverksette nødrutiner		
Prioritering av tjenester og beslutninger utenfor IKT-beredskapskoordinators myndighet		
Informere internt i foretaket om status i		

hendelsen		
Kommunikasjon med pasienter		
Informasjon fra foretak til media		
Bistå i problemløsning innenfor strøm, kjøling osv.		
Eskalere til Helse Sør-Øst RHF		
Aktiviteter etter hendelsen		
Delta i debrief		

Konsekvensscenarioer (identifisert i risikovurderinger):

1. Svikt i personsøkersystem -> personell kan ikke tilkalles over personsøkersystem

<Dersom det er spesielle rutiner som gjelder for akkurat det scenarioet, kan det beskrives her. Ellers gjelder aktivitetene som beskrevet i tabellen over.>

Aktivitet	**Ansvarlig**	**Kommentar/beskrivelse**
Iverksettelse av nødrutiner	<Enhet/rolle> *Eksempel: Akuttmottak*	<Link til nødrutine> *Eksempel: Kontakte nødvendig personell på mobiltelefoner*

2. Svikt i telefonisystem -> personell kan ikke tilkalles over ordinært telefonisystem

<Dersom det er spesielle rutiner som gjelder for akkurat det scenarioet, kan det beskrives her. Ellers gjelder aktivitetene som beskrevet i tabellen over.>

Aktivitet	**Ansvarlig**	**Kommentar/beskrivelse**
Iverksettelse av nødrutiner	<Enhet/rolle> *Eksempel: Akuttmottak*	<Link til nødrutine> *Eksempel: Kontakte nødvendig personell på mobiltelefoner*

Tiltakskort IKT-beredskapskoordinator:

Se vedlegg A.

Versjonskontroll

Versjonsnummer:	Årsak til endring:
Versjon 0.1	MEØ: Dokument opprettet
Versjon 0.2	MEØ: Oppdatert etter innspill fra prosjektgruppa
Versjon 0.3	MEØ: Oppdatert med forvaltningsrammeverk og mal
Versjon 0.4	MEØ: oppdatert etter avklaringer i regional delplan
Versjon 0.5	MEØ: Oppdatert etter innspill fra Gry Sundberg
Versjon 0.9	MEØ: Klart for utsendelse til IS-forummedlemmer.
Versjon 0.91	MEØ: Oppdatert etter innspill fra prosjektgruppa
Versjon 0.92	MEØ: Oppdatert etter innspill fra foretakene og RHFet
Versjon 1.0	MEØ: Ferdigstilt dokument
Versjon 1.1	TP: Oppdatering ved revidering mars/april 2014