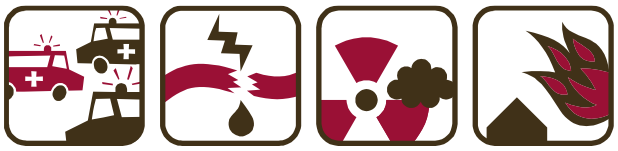
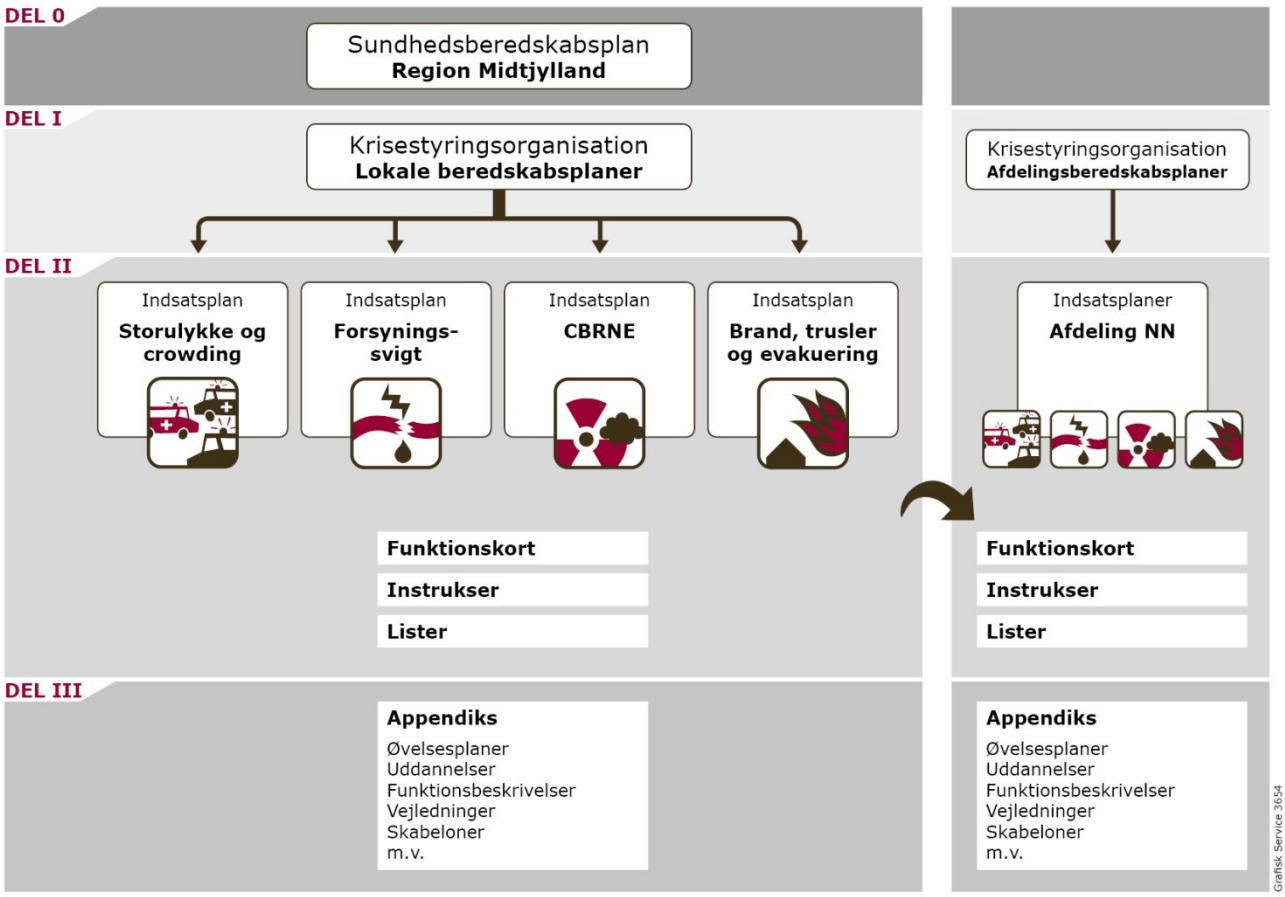


It beredskabsplan
It

DEL 1-2
It-beredskabsplan



Indholdsfortegnelse

Indhold

Vejledning

It-beredskabsplanen skal sikre, at Region Midtjylland opnår den mest optimale tilgængelighed til de forretningskritiske systemer og applikationer, når almindelig eller kritisk driftshåndtering ikke længere er tilstrækkelig.

Formålet med etablering af it-beredskabsplanen er understøttelse af den samlede drift af it, herunder den underliggende infrastruktur, på et passende og foruddefineret niveau med henblik på at minimere konsekvenserne af driftsafbrydelser som følge af nødsituationer eller katastrofer.

Forretningsområderne skal understøttes af it-beredskabsplanen med det formål at kunne håndtere kritiske arbejdsgange under en nødsituation eller katastrofe. Med henblik på at sikre den optimale patientbehandling, er det essentielt, at de mest kritiske it-systemer er tilgængelige. Hvis der opstår en hændelse, er det derfor vigtigt at kunne reetablere adgangen til disse systemer inden for den på forhånd definerede tidshorisont.

It-beredskabsplanen beskriver, hvad der ligger forud for igangsætning af et it-beredskab samt de forskellige faser i en it-beredskabssituation.

1. Alarmering og eskalering; 2. Aktivering Respons; 3. Inddæmning; 4. Kontrol og normalisering; 5. Afblæsning og Reetablering.

Faserne understøttes af Funktionskort, der kort og præcist gennemgår aktiviteter og opgaver. Funktionskortene anvendes som tjeklister og angivelser af formelle discipliner.

It-beredskabet indgår i Sundhedsberedskabsplan 2018-2021 under forsyningssvigt og aktiveres som lokalt beredskab i Region Midtjyllands krisestyringsorganisation. It-beredskabet bliver desuden løbende tilpasset angivelserne i DCIS Sund's beredskabsplan (Decentrale Cyber og Informationssikkerhedsenhed Sundhedsdata-styrelsen). DCIS Sund's varslingshåndbog og MISP håndbog er vedlagt som bilag.

Aktivering kan ligeledes ske ved eskalering gennem Incident Management via Major Incident processen eller ved akut aktivering.

Situation Manager kredsen indtager sammen med it-driftschefen rollen som it-beredskabsleder. Personkredsen kontaktes direkte ved hjælp af kontaktlister.

Alle bilag følger Major Incident processen med den tilføjelse, at en beredskabsrapport (problemrapport) skal udarbejdes ved aktivering af it-beredskab.

Fase 1 Alarmering og eskalering

Eskalering til it-beredskab sker gennem Incident Management via Major Incident processen til it-beredskabet eller ved akut aktivering. It-beredskabet kan også aktiveres af Region Midtjyllands Sundhedsberedskab via B-AMK og DCIS Sundhedsdatastyrelsens beredskabsplan.

Eskalation sker såfremt det vurderes, at hændelsens omfang og konsekvens har stor effekt på forretningen og patientsikkerheden eller hvis den regionale krisestab aktivere it-beredskabet som lokalt beredskab i Region Midtjyllands Sundhedsberedskab.

Vurderingskriterier kan blandt andet være, at genetablering ikke kan ske inden for en maksimal aftalt periode - Maximum Tolerable Periode of Disruption (MTPD), hvor konsekvensen for utilgængelighed bliver for stor for Region Midtjylland. MTPD er vejledende sat til max. 48 t. Eskalations vurdering kan også være flere samtidige kritiske nedbrud eller fysiske skader på kritisk infrastruktur, som ikke kan håndteres af almindelig drift eller kritisk driftshåndtering.

Akut aktivering er ekstraordinære hændelser, hvor Situation Manager vurderer eller et aktiveret Sundhedsberedskab kræver, straks aktivering af it-beredskabsplanen.

1.1 Snitflader og afhængigheder

It-beredskabsplanens procesejer er CISO, som er ansvarlig for den videre udvikling og vedligeholdelse af it-beredskabet.

It-beredskabsplanen revideres løbende og mindst en gang årligt.

It-beredskabet dækker Region Midtjyllands mest kritiske systemer, som defineret af Region Midtjyllands Risikovurdering (Forretningskritiske systemer) og Business Impact Assessment analyse (BIA). Kritiske systemer i it-beredskabet kategoriseres som livsgivende, livsunderstøttende eller administrativt system. Systemer i it-beredskabet skal godkendes af CISO og efterfølgende ITCG-kredsen.

Systemernes specifikationer skal være angivet i Region Midtjyllands ServiceNow CMDB. Mangelfulde informationer omkring de enkelte systemer eller manglende registrering af systemer på grund af manglende opfyldelse af CMDB kriterierne har indflydelse på it-beredskabets mulighed for understøttelse af systemerne i en beredskabssituation.

It-beredskabsplanen indgår i Region Midtjyllands Sundhedsberedskab. It-beredskabets mulighed for genskabelse afhænger af pågældende systems dokumentation af recovery planer samt tilgængeligheden af planerne. Ansvaret påhviler overordnet systemejer.

1.2 Eskalering af hændelser

Ved hændelser, der påvirker en eller flere systemer benyttes nedenstående eskaleringsprocedurer.

- Almindelig drift eller kritisk driftshåndtering 's evne til at håndtere situationen
- Tidsfaktor
- Omfang af datatab (tabstolerance)
- Graden af påvirkning (procentdel af infrastrukturprocentdel af ansatte, der kan udføre deres arbejde)
- Særlige hændelser (naturkatastrofer, brud i forsyning, terrorisme, krig, sabotage, strejke, undtagelsestilstand)
- MTPD overskridelse (maksimale periode, hvor konsekvensen af services utilgængelighed bliver for stor for Region Midtjylland)

Eskalering af hændelser sker i overensstemmelse med ITSCM (IT Service Continuity Management) dokumenterede processer.

Formidling skal ske i forhold til angivelser i Sundhedsberedskabet og It-beredskabsplanens Funktionskort.

1.3 Systemer

Risikovurderingen er en årlig proces i Region Midtjylland, hvor forretningskritiske systemer bliver genstand for en konsekvens-, sårbarheds- og trusselsvurdering. Vurderingerne samles i en afsluttende risikorapport som foreligges Informationssikkerhedsudvalget. Risikovurderingen bidrager efterfølgende til en revurdering af Business Impact Assessment (BIA) listen som bidrager vejledende til prioritering og håndtering af de kritiske systemer. Risikovurderingsmøderne bliver afholdt med systemejer, repræsentanter i forretningen, it og informationssikkerhedsfunktionen.

Infrastrukturafhængigheder:
Der er en række infrastrukturkomponenter, som systemerne og deres indbyrdes forbindelser er afhængige af. Disse listes som:

Strøm, vand, køl	Netværkskabling	Lan / WLan	DNS, DHCP, AD, Filstruktur
Tids-synkronisering	Virtualisering	Storage / SAN	Telefoni funktioner IP, mobil og DECT
Backup	Eksterne netværk	System og Applikationer	Regionsnet
Fælles It Platform	BSK (Bruger Stamdata Katalog)	Datacentre	Citrix

Systemer og kategorisering:
Systemerne kategoriseres i forhold til hvorvidt systemet er livsgivende (Kategori A), livsunderstøttende (Kategori B) eller et administrativt forretningssystem (Kategori C og D). ServiceNow er undtagelsen, da det er et understøttende system i forhold til it-beredskabshåndtering.
Bemærk i øvrigt at BSK og telefoni betragtes som et kritisk infrastrukturkomponent og derfor optræder såvel som infrastrukturkomponent og som system.

Kategori A	Kategori B	Kategori C	Kategori D
•ServiceNow •BSK •Labka II •Apovision (MS, 17 og online) •Midt EPJ •RIS~ •PACS~ •Prosang~ •LUNA •Impax~ •Klinisk Logistisk* •Præhospital systemer*	•Bosted (EG Incorp og Sensum) •Service Logistik~ •eBOP /EDI •Lindpro flexcall* •Ascom* •MADS •Testo Saveris Professional CFR •e-Dok •BMS •PICIS •Scandiatransplant	•AS2007 (CGI) •Post og Kalender (MS Outlook og web) •ØS indsigt •RM Telefon*i~ •Intranet RM •EPI-server •Silkeborg Løn •Intranettet (EPI) •Adgangs-system*	•BI (MS og Tableau) •ESDH, fil og print (Emne-, Klient- og Personalesager) •RM Indkøb (ILM)

~indeholder flere specificerede subsystemer i ServiceNow.
* Fælles betegnelse som indeholder flere systemer som specificeret nedenunder

***Præhospital systemer:**

- Præhospital Patientjournal (P-VIT PPJ)
- Logis IDS, Prod.
- Den Landsdækkende Helikopterordning (SimaTech DLH)
- Radiosystem (IHM Alarm OperMain (112 DOA); SINE radiokommunikation og backup)
- AMK vagtcentral støttesystemer (ADO (Overvågning af alle kørsler))

***Klinisk Logistisk**

- Anywhere, CIS, CIS Integrationslayer; IDF Config tool samt snitflader og integrationer (CCL).

***RM Telefoni**

- Trio Call Manager; Trio Enterprise Agent og Trio Enterprise Client*;
- Avaya
- Cisco IP Communicator
- IPT
- Netwise NOW 2007; Alarmtelefon Motorola; CTIOS Client
- Mobil Telefoni

***Ascom**

- Alarm Agent AUH; DNV; HEV; Horsens og Viborg
- Overfaldsalarm Mosetoft og AUH Produktion
- Alarmmanagement Randers
- Patientkald RH Hammel
- Unite AUH og Horsens

***Lindpro Flexcall Patientkald**

- AUH (NBG – muligvis udfaset?)
- HE Horsens

***Adgangssystem:**

- Unilock – HEM; AUH; HEV; Horsens; Randers
- ARX, CGI – adgangskontrol DNV Gødstrup
- Symmetry (S8600) – G4S
- Salto SPACE

Support

Kritiske systemer, kategoriseret som SLA 1, har 24/7/365 support.

Det betyder omgående reaktionstid i henhold til gældende overenskomst på vagtområdet.

< 30 min.	Konstateret, registreret og påbegyndt fejlretning med orientering til relevant personale i it-drift.
< 60 min.	Områdeledere for produktgruppen er orienteret.
< 120 min.	It-driftschef og it-direktør (og dermed Formand for it-beredskabet) er orienteret.

Yderligere eskalering følger forretningsmodel og øvrige beskrivelser i nærværende dokument.

Maximum Tolerable Period of Disruption (MTPD) dækker over den maksimale aftalte periode, hvor konsekvensen af services utilgængelighed bliver for stor for Region Midtjylland og som vejledende er sat til 48 t.

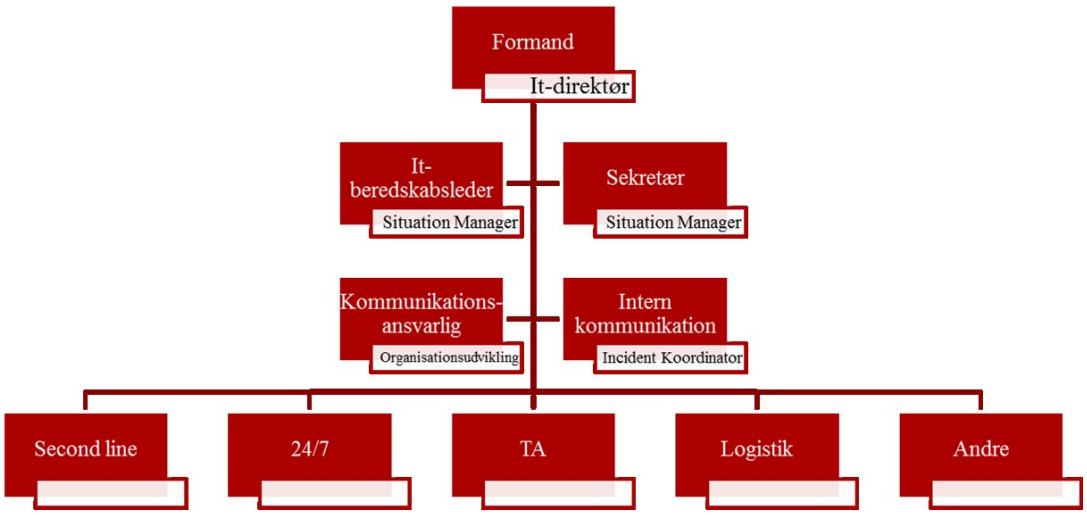
Det bemærkes at it-beredskabets system liste p.t. indeholder 34 systemer herunder 22 systemer som betragtes livsgivende eller understøttende. Der kan være flere relaterede systemer til de enkelte systemer (markeret med ~)

I aktiveret it-beredskab vil livsgivende og livsunderstøttende systemer have primær prioritet ud fra en generel betragtning. ServiceNow vil undtagelsesvis ligeledes have en primær prioritering på grund af dens anvendelse ved aktiveret it-beredskab eller betydning ved øvrige beredskaber.

1.4 Organisation

It-beredskabet indgår som lokalt beredskab i Region Midtjyllands Sundhedsberedskab som aktiveret er styrende i forhold til Krisestyringsorganisation herunder håndtering af beredskabssituationen. It-beredskabet indgår understøttende.

It-beredskabsorganisationen:



- Formand: It-direktør (Medlem af Præhospitalets krisestyringsorganisation og Regionale krisestab)
- Stedfortræder: CISO (It-sikkerhedschef)
- It-beredskabsleder: It-driftschef / Situation Manager
- Sekretær: Situation Manager
- Kommunikationsansvarlig: Organisationsudvikling
- Intern Kommunikation: Incident Koordinator
- Second line (+Third line): Netværk; Server & Storage; Backup; Applikationer; Klienter; Produkter; 24/7 og overvågning m. fl.
- TA: Teknisk Afdeling
- Logistik: Vand, mad, papir m.m. (udpeges af it-beredskabsleder)
- Andre: Eksterne leverandører; supportere med mere.

It-beredskabsledelsen kan mødes på følgende lokationer, hvor OPA 34 som udgangspunkt fungerer som primær kommandocentral.

- Aarhus: Olof Palmes Allé 34, Mødelokale 22, 8200 Aarhus N.
  Olof Palmes Allé 15, Mødelokale 17, 8200 Aarhus N
- Viborg: Skottenborg 26, Mødelokale C4, 8800 Viborg
  Holstebro Lægårdvej 12G, Mødelokale 6-2, 6. sal, 7500 Holstebro

Mødelokalet fungerer som kommandocentral for it-beredskabet. Mødedeltagerne kan om muligt deltage fra flere forskellige mødelokaler.

It-beredskabsplanen forefindes følgende steder:

- ServiceNow, SecureAware og Bered-'skabet' (OPA 34, lok. 22) samt midtX
- Formanden for it-beredskabet, stedfortræder (CISO) og ITCG.
- Situation Managers herunder ekstern placering (MI)
- Procesejer, Procesansvarlig og procesmanager, it-stab, Ledelsessekretariatet
- Sundhedsberedskabet e-dok.

Fase 2 Aktivering og respons

(Funktionskort 1, 2, 3, 4, 5, 6, 8 & 12)

Under krisestyring vurderes hændelsens omfang og konsekvens for patientsikkerhed og forretningen. Problemløsning identificeres og igangsættes.

2.1 Beredskabsproces - initiering

Godkendelse af it-beredskabsplanens aktivering sker ved Formanden for it-beredskabet eller dennes stedfortræder.

Initiering sker på en af følgende måder:

- Major Incident.
- Aktivering af Sundhedsberedskabets operationsberedskab trin 3.
- Akut med godkendelse via tilgængeligt medie (Telefon, video o. a.)
- Akut uden godkendelse ved f. eks. fysiske skader på systemer og/eller flere samtidige nedbrud.
- Akut med eller uden godkendelse på baggrund af DCIS Sundhedsdatastyrelsens henvendelse.

Akut aktivering uden godkendelse kan ekstraordinært ske ved hændelser, hvor Situation Manageren vurderer, at der kræves straks aktivering. Formanden for it-beredskabet skal informeres hurtigst muligt.

Ved eskalering via forretningsprocesser vurderes hændelsens omfang i forhold til konsekvens for forretningen og patientsikkerheden. Eskalering sker som defineret i Major Incident processen.

Situation Manager vurderer i dialog med Formanden for it-beredskabet aktivering af it-beredskabet, hvorefter it-beredskabslederen (Situation Manager og/eller it-driftschef) indkalder it-beredskabsledelsen (It-beredskabslederen, Sekretær, Incident Koordinator, Kommunikationsansvarlig og evt. Logistik ansvarlig).

Der opereres med MTPD (Maximum Tolerable Period of Disruption) som en vurdering af den periode services maksimalt må være utilgængelige inden konsekvensen for Region Midtjylland vurderes at være for stor.

Formanden for it-beredskabet forestår ledelses-information under et it-beredskab herunder sikring af orientering af direktionen. Direktion orienteres hurtigst muligt.

Ved aktivering af Sundhedsberedskabets operationsberedskab forestår Formanden for it-beredskabet dialogen med kriseledelsen som defineret af Sundhedsberedskabet herunder eventuel mødeaktivitet.

It-beredskabet alarmerer AMK-vagtcentral ved nedbrud som kræver aktivering af it-beredskabsplanen og informerer DCIS Sundhedsdatastyrelsen (AMK og DCIS skal løbende orienteres om situationen).

Beskrevet tidsforløb:

Tidsforløb	Aktivitet/Handling
0 - 30 min.:	Initiering og aktivering af it-beredskab.
30 - 60 min.:	It-beredskabsplan er aktiveret; It-beredskabsledelsen er samlet; Funktionskort følges; Udarbejdelse af plan.
60 - 120 min.:	Håndtering med efterfølgende opsummerende tidsplan.
Normalisering (Return)	Sker ved overdragelse til Major Incident processen.

2.2 Alarmering

(Funktionskort 1, 2, 3, 4 & 12)

Hvis eskaleringsprocedurerne resulterer i, at it-beredskabsplanen skal aktiveres, skal følgende retningslinjer følges:

1. Formanden for it-beredskabet aktiverer it-beredskabsplanen og erklærer en it-beredskabssituation – jævnfør Funktionskort 1 & 2

2. It-beredskabslederen indkalder it-beredskabsledelsen – jævnfør Funktionskort 3

3. It-beredskabslederen er nu styrende i forhold til beredskabet og styrer den efter it-beredskabsplanen og gældende procedurer – jævnfør Funktionskort 2

4. It-beredskabsledelsen varetager deres respektive roller, som defineret i organisationsdiagram og efter it-beredskabslederens delegering – jævnfør Funktionskort 2 & Funktionskort 4

5. It-beredskabsledelsen alarmerer AMK-vagtcentral jævnfør Funktionskort 1 og 2.

6. Formanden for it-beredskabet orienterer ledelseslaget herunder direktion.

7. It-beredskabsledelsen foreståår information til DCIS Sundhedsdatastyrelsen.

2.3 Situations håndtering

Funktionskort 2, 5 & 6

1. Hvis situationen tillader det, og menneskers liv og helbred ikke er i fare, forsøges begrænsning af skaderne f.eks. ved brug af brandslukningsudstyr, pumper, nedlukning og fjernelse af it-udstyr.

2. Der foretages en situationsvurdering over hvilke processer, der er påvirket af hændelsen og i hvilket omfang. En estimeret tidsramme for nøddriften af disse systemer udfærdiges - jævnfør Funktionskort 6

3. It-beredskabslederen vurderer situationen; Hændelseslog udfyldes/opdateres i samarbejde med it-beredskabsledelsen og nødvendige kompetencer indkaldes – jævnfør Funktionskort 2 & Funktionskort 5

4. Der føres løbende en log over situationsvurdering, hændelsesforløb og afsluttende notat i Hændelseslog – jævnfør Funktionskort 2.

2.4 Kommunikation

Funktionskort 8

Organisationsudvikling er ansvarlig for it ekstern kommunikation inden for Region Midtjylland. Incident Koordinator er ansvarlig for it intern kommunikation.

Incident koordinator er fysisk placeret i 24/7.

Kommunikationskanaler ved it-nedbrud skal anvendes (forefindes i håndbøger til Major Incident og It-beredskabet).

Formanden for it-beredskabet holder ledelseslaget samt sikre orientering af direktionen.

Der gøres opmærksom på, at DCIS Sundhedsstyrelsen skal holdes orienteret om situationen (jævnfør Funktionskort 2, 8 og kontaktliste It-beredskabsledelsens kontaktliste).

DCIS SDS Varsel Vagt: +45 4041 1911; DCISvarsel@sundhedsdata.dk

Ved mistanke om it-sikkerhedshændelser kan CFCS Cybersituationscenter kontaktes.

CFCS SitCen: +45 3332 5580; cert@cert.cfcs.dk

Kommunikation v. organisationsudvikling skal informere Koncern Kommunikation ved enhver aktivering af it-beredskabet herunder også Præhospitalets Kommunikationsafdeling.

Hvis Sundhedsberedskabet aktiveres har Koncern Kommunikationschefen ansvaret for krisekommunikationen. Koncern kommunikationschefen råder over samtlige af koncernens kommunikationsressourcer og kommunikationsansatte.

Fase 1 Alarm → Fase 2 Aktivering → Fase 3 Inddæmning → Fase 4 Kontrol → Fase 5 Afblæse og reetablering

Fase 3 Inddæmning

Etablering af nøddrift

(Funktionskort 6)

Forretningen kontaktes med henblik på etablering af nøddrift og nøddriftsprocedurer for berørte systemer, så forretningen kan fortsætte sin daglige drift – dog under mere begrænsede forhold.

3.1 Scenarier og strategier

Respektive nøddriftsprocedurer for det/de berørte systemer følges.

Forefindes der ikke nøddriftsprocedurer eller er nøddriftsprocedurerne ikke tilgængelige, skal forhåndenværende dokumentation for det enkelte system følges. Angivelser i dokumentation skal følges. Opmærksomheden skal henledes på, at det er differentieret i forhold til det enkelte system, hvem der skal kontaktes og hvor det er dokumenteret.

Fase 1 Alarm → Fase 2 Aktivering → Fase 3 Inddæmning → **Fase 4 Kontrol** → Fase 5 Afblæse og reetablering

Fase 4 Kontrol og normalisering

(Funktionskort 6, 7, 9, 10 & 13)

Fasen 'Normalisering' omfatter at it-beredskabet foretager en hændelsesoverdragelse til Major Incident processen.

4.1 Normaliseringsbeskrivelse

Funktionskort 9

Rent praktisk sker 'Normalisering' ved. at it-beredskabsledelsen overdrager det videre forløb til Major Incident processen som herefter følger angivelser for Major Incident processen.

Major Incident vil forestå genetablering af fysiske rammer herunder serverrum, strøm, køling og fysisk sikkerhed. Ligeledes genetablering af hardware og software samt platforme og infrastruktur herunder AD, DNS, DHCP og tidssynkronisering. Systemer og konfiguration genetableres, inden data og processer bliver genetableret.

Potentielle områder:

Fysiske rammer (serverrum, strøm, køling, fysiske lokaler)

Hardwaremiljø (HW, udstyr, kommunikationslinjer)

Platform (VMWare, Citrix m.m.)

Infrastruktur (AD, DNS, DHCP)

Systemer (OS, applikationer, storage)

Konfiguration (nødvendige forbindelser)

Data og processer (evt. forretningsprocesser)

4.2 Genetablering

(Funktionskort 7)

Genetablerings processerne håndteres inden for rammerne af Major Incident processen, og normaliseringen sker efter angivelserne dokumenteret af Major Incident.

It-beredskabet overdrager normaliseringen til Major Incident processen, som efterfølgende vurderer, hvilke ressourcer der forsat er behov for.

Overdragelsen sker afstemt med Formanden for it-beredskabet.

4.3 Afslut nødplaner

(Funktionskort 6 & Funktionskort)

De manuelle nødplaner afsluttes, og forretningens afdelinger bedes anvende it-systemerne fremadrettet i koordination med Major Incident processen.

4.4 Afslut beredskab

(Funktionskort 13)

It-beredskabslederen og Formanden for it-beredskabet kan i samråd med it-beredskabsledelsen beslutte om it-beredskabet skal afsluttes, og normaliseringsprocessen skal overdrages til Major Incident Processen. Beslutningen orienteres til systemejerne.

4.5 Beredskabslog afsluttes

(Funktionskort 10)

Beslutninger og handlinger fra it-beredskabshændelsen diskuteres i it-beredskabsledelsen på et møde organiseret af it-beredskabslederen. Formålet er at evaluere på beredskabsindsatsen for at identificere områder, hvor processen kan blive forbedret. Beredskabslog er en hændelsesanalyse.

Fase 5 Afblæsning og Reetablering

(Funktionskort 11)

Efter afslutning af it-beredskabet skal der ske en evaluering af hændelse samt eventuel opdatering af it-beredskabsplanen i forhold til forbedringsmuligheder.

Analysen omhandler analyse af årsagen for hændelsen, hvordan den blev håndteret, samt hvordan beredskabet fungerede.

5.0 Problem

(Funktionskort 11)

Når it-beredskabsplanen har været aktiveret skal der efter afslutning udarbejdes en problemanalyse. Problemanalyse er en udvidelse af kerneårsagsanalysen, som Major Incident processen har implementeret. Problemanalyse skal sendes til Problem Manageren, som videreformidler analysens resultat til Informationssikkerhedsfunktionen med henblik på sagsfremstilling i Informationssikkerhedsudvalget.

5.1 Eksterne myndigheder

Når it-beredskabsplanen har været aktiveret skal der efter afslutning tilsikres, at relevante myndigheder er informeret om hændelsen i overensstemmelse med regulative bestemmelser.

Der skal især være opmærksomhed på Databeskyttelsesforordningens artikel 33 og 34 (underretning) herunder underretning af DPO funktion i Region Midtjylland og Datatilsynet; NIS direktivet § 6 (underretning) i forhold til indmeldte systemer og at DCIS sundhedsdatastyrelsen holdes orienteret.

Revisionshistorik 2020

20.8.2020	1.7	Korrektioner af sætninger samt systembetegnelser. Uddybende forklaringer. Max. antal systemer fjernet. Kommunikationsrolle for Formanden af it-beredskabet. Angivelse af BSK opmærksomhed – infrastruktur og system. Systemer og Subsystemer opdateret og præciseret. Fælles system begreb anvendelse udspecificeret	JKR
16.8.2019	1.6.0	It-beredskabs dokument lagring rettet Systemrettelser Konsekvensrettelser Korrekturrettelser	JKR
10.1.2019	1.5.7	Angivelse af tilpasning af it-beredskabsplan til DCIS Sundhedsdatastyrelsens beredskabsplan. Konsekvensrettelser.	JKR
26.11.2018	1.5.6	Konsekvensrettelser og korrektur.	JKR
26.11.2018	1.5.5	Grafisk ændring	JKR
05.4.2018	1.5.4	Korrektur og konsekvensrettelser	JKR
11.1.2018	1.5.3	Fase 1 s. 4 Alarmering og eskalering samt Snitflader og afhængigheder tilføjes forpligtelse til notifikation til AMK vagtcentral 70 124 124. Kerneårsagsanalyse erstattes af hændelsesanalyse og problem.	JKR
11.1.2018	1.5.2	Fasebeskrivelse ændret i overensstemmelse med "Sammenhængende beredskab" Action Cards betegnelse ændret til Funktionskort	JKR
11.1.2018	1.5.1	Tekstkorrektion	JKR
20.4.2017	1.5	Nye overskrifter tilpasset sundhedsberedskabet. Tekst tilpasset sundhedsberedskabet.	JKR
16-12-2016	1.4.1	Layout tilpasning	JKR
16.12.2016	1.4	Mindre tekst korrektion	JKR
8.12.2016	1.3	Præciserende tekst.	JKR
	1.2	Præcisering af skriftelige rettelser og korrektioner	JKR
17.8.2016	1.1	Skriftelige rettelser og korrektioner m. forklarende tekst	JKR
06.7.2016	1.0	Oprindeligt dokument	JKR