It-beredskabsplan

for

Sentinel Surveillance System

Denne it-beredskabsplan er skrevet til Sentinel Surveillance System der enten:

- har outsourcet største dele af driften af it-systemerne

Styring af beredskab og krav til beredskab til leverandører skal reguleres i leverandøraftaler og Service Level Agreements (SLA).

Version	*1.0*
Dato	November 2022
Godkendt af	NIL

Indhold

I TILFÆLDE AF EN HÆNDELSE

Hvis du er den første, der kontaktes i forbindelse med en hændelse, skal du begynde med at vurdere, om der kræves beredskabshandlinger. Herefter opretter du en hændelsesjournal.

- **afsnit 3.2 Aktivering af beredskabsplanen**
- **afsnit 6.9 Hændelsesjournal**

Hvis du vurderer, at der er relevant at iværksætte beredskabet, skal der eskaleres og mobiliseres, som beskrevet i retningslinjerne.

- **afsnit 3.3.1 Eskalering**

Herefter udføres relevante opgaver i henhold til de planer, der er omfattet af beredskabet:

- **afsnit 3 Handlingsplaner**

Vær specielt opmærksom på de forudsætninger og udeståender, der har indflydelse på om aktiviteterne kan gennemføres. Se

- **afsnit 3.1 Forudsætninger og**
- **afsnit 5.3 Udeståender**

1 Indledning

It-beredskabsplanen er den operationelle udmøntning af organisationens it-beredskabsstrategi. Strategien fastsætter de overordnede mål og rammer for styringen af beredskabet, mens planen beskriver de operationelle tiltag og handlinger, som er relevante i en beredskabssituation.

It-beredskabsplanen er opdelt i tre hoveddele ud over indledning og bilag.

I en beredskabssituation skal der først og fremmest tages udgangspunkt i de operationelle handlingsplaner. Handlingsplanerne indledes i afsnit 3 med beskrivelse af forudsætningerne for planen.

Nedenstående figur viser beredskabsplanens overordnede opbygning og hovedafsnit.

Område	**Afsnit**		**Beskrivelse**
Indledning	1	Kom godt i gang	Afsnittene beskriver opbygning og indeholder vejledning til selve skabelonen/planen.
Operationel planlægning	2.1	Tidsmæssige målsætninger	Dette delområde beskriver den planlægning, som er relevant for at kunne udføre de operationelle handlingsplaner i en beredskabssituation. Det er en forudsætning for planens effektivitet, at alle rolleindehavere kender indholdet.
	2.2	Beredskabsorganisation	
Operationelle handlingsplaner	3.1	Forudsætninger	Dette delområde beskriver de operationelle handlingsplaner, som skal anvendes i en beredskabssituation. Alle rolleindehavere skal kende til de handlingsplaner, hvor man har en rolle.
	3.2	Aktivering af beredskabet	
	3.3	Beredskabsledelse - Eskaleringsprocessen - Kommunikationsplan - Styring af leverandører - Anvend alternativ lokation	
	3.4	Hardwarerelaterede planer	
	3.5	Netværksrelaterede planer	
	3.6	Virus- eller hackerrelaterede planer	

Område		Afsnit			Beskrivelse
Detailinstrukser		4.x	Xxxx		Dette afsnit beskriver udvalgte elementer af handlingsplanerne i mere detaljeret form. Alle rolleindehavere skal kende til de dele, hvor han/hun har en rolle.
		4.y	Yyyy		
		4.z	Zzzz		
Vedligeholdelse		5.1 + 5.2	Test og testhistorik		Dette delområde beskriver de praktiske forhold omkring vedligeholdelse af beredskabsplanen og er primært til reference. Dog kan status på udeståender fra tidligere hændelser og tests have betydning for planens anvendelse i en beredskabssituation.
		5.3	Udeståender		
		5.4	Opdatering af planer		
Bilag		6.9	Hændelsesjournal		Afsnittene indeholder hjælpeværktøjer og information til brug i en beredskabssituation.
		6.10	Tjekliste til normaldrift		
		6.11	Hjælpeværktøjer / mødested		

Figur 1 - Skabelonens overordnede struktur.

2 Operationel planlægning

Operationel planlægning er dokumentation af Sentinel Surveillance System forarbejde, der er med til at sikre, at beredskabsplanen opfylder forretningens behov og beskriver mål og rammer for beredskabet i tilfælde af en hændelse.

2.1 Tidsmæssige målsætninger for retablering

I dette afsnit er anført de tidsmæssige mål for at retablere it-understøttelsen efter en alvorlig hændelse, betegnet Recovery Time Objective (RTO). Der er desuden angivet en prioritering af retableringsrækkefølgen, hvis ressourceknaphed eller tekniske afhængigheder forhindrer sideløbende retablering. RTO-værdierne afspejler de forretningsmæssige krav, som skal ses i lyset af:

- det sikkerhedsniveau Sentinel Surveillance System har besluttet
- de sikringsforanstaltninger, der er implementeret
- beredskabsplanens operationelle processer

Endvidere har følgende strategiske overvejelser været vurderet inden de endelige RTO-værdier for de kritiske systemer er lagt fast:

- muligheden for at anvende alternative procedurer til it-understøttelsen (f.eks. manuelle arbejdsgange, outsourcing mv.) – og i bekræftende fald om det er et argument for at forlænge den acceptable periode uden it-understøttelse eller for at nedprioritere retableringen af systemet
- evt. fordel ved ekstra satsning på forebyggelse af nedbrud (øge modstandsdygtigheden) i de særligt kritiske systemer, frem for ensidigt at have fokus på hurtig retablering.

2.1.1 Prioriteret systemliste

Prioritet	**Systemnavn**	**RTO**
1	Cloud filserver	*2 timer*

2	IoT eller OT produkter (Virksomhedens egne systemer & Industrirobotter) - Ej kendt hvorvidt SSS lagrer kundedata	*3 timer*
3	ERP (Enterprise Resource Planning - Microsoft Dynamics 365 Finance & Operations)	*12 timer*
4	Lagerstyring (integreret del af Microsoft Dynamics 365 Finance & Operations)	*12 timer*
5	Projekt- og produktionsstyring (Microsoft Dynamics 365 Project Operations & Microsoft Teams)	*12 timer*
6	Bogføring (Microsoft Dynamics 365 Business Central)	*24 timer*
7	CRM (Customer Relationship Management - Microsoft Dynamics 365 Sales)	*3 dage*

Det er afgørende at disse retableringsmål er aftalt med driftsleverandøren, således at leverandørens planer og prioriteringer kan afstemmes med organisationens.

2.2 Beredskabsorganisation

Dette afsnit beskriver den organisation og bemanding, som skal mobiliseres i en beredskabssituation, og som skal sikre, at nødplanerne kan føres ud i livet.

Organisationsmodel

Vores it-beredskabsorganisation tager udgangspunkt i den eksisterende organisationsstruktur for at sikre:

- Kendte kommunikationsveje
- Indøvede arbejdsgange
- Klare ansvarsfordelinger

2.2.1 Beredskabsorganisationens struktur

Roller og nøglepersoner

Rollerne i beredskabsorganisationen og de opgaver, som er aftalt skal udføres i en beredskabssituation, er præciseret herunder for at synliggøre en optimal tildeling af rollerne i forhold til organiseringen og kompetencerne i Sentinel Surveillance System.

Beredskabsleder

- Navn/rolle: Andre Andersen / CEO
- Ansvar: Overordnet koordinering og beslutningskompetence
- Kontakt: 12 34 56 78 / aan@sentinel.dk

It-beredskabskoordinator

- Navn/rolle: Bo Bojesen / CISO
- Ansvar: Operationel ledelse af it-beredskabet
- Kontakt: 12 34 56 79 / bob@sentinel.dk

Systemansvarlige

Navn/rolle: Casper Carlsen / Systemarkitekt

- Ansvar: Liste over de kritiske systemer/nøglesystemer, bemandingsliste og de systemansvarlige.
- Kontakt: 12 34 56 70 / cac@sentinel.dk

Kommunikations- og dokumentationsansvarlig

- Navn/rolle: Dennie Danielsen / Jura-Chef
- Ansvar: Intern dokumentation samt kommunikation under krise (internt+eksternt)
- Kontakt: 12 34 56 71 / ded@sentinel.dk

Produktionsansvarlig

- Navn/rolle: Frederik Fetterlein / Produktionschef
- Ansvar: Produktionen i Tyrkiet kører efter planen
- Kontakt: 1337 1337 / ffe@sentinel.dk

Bemanding

- Bemandningslist:
- Bilag X: Liste over retableringsteams på tilkaldevagt og Systemansvarlige

- Eskaleringsmodel:
- Bilag X: Model der beskriver hvornår og hvordan der eskaleres

Eksterne leverandører

Følgende opgaver varetages af eksterne leverandører i en beredskabssituation:

Leverandør	Opgave/system	Kontakt	SLA
Microsoft Dynamics 365	ERP Lagerstyring Projekt- og produktionsstyring Bogføring CRM	88 88 88 88	30 min
Microsoft OneDrive/SharePoint	Cloud filserver	88 88 88 89	30 min

Interne opgaver

Følgende opgaver varetages internt af organisationen:

- Liste over interne opgaver og ansvar
- First line support
- Koordinering med eksterne leverandører

2.2.2 Mødested

Produktionschefen er lokaliseret i Tyrkiet, hvilket gør det umuligt at få fysisk fremmøde, derfor er produktionschefen online under hele forløbet.

Mødested for it-beredskabsledelsen				
Type	Bygningsnavn	Adresse	Lokale	Fastnet telefon
Primær DK	*HQ KBH*	*Gothersgade 11*	*Mødelokale 4*	*11 22 33 44*
Sekundær DK	*Frederiksberg*	*Drømmehave 13*	*Stuen*	*55 66 77 88*

Primær TY	*Ankara*	*Storegade 25*	*Mædelokale 3*	*66 77 88 55*
Secundær TY	*Bursa*	*Lillegade 64*	*Mødelokale 9*	*22 33 44 11*

Krav til lokalet:

Artikel	**Kommentar**
Beredskabsplan i papirformat	
Beredskabsplan på USB-stik	
Ekstra hændelseslog	25 Printkopier
Papir og skriveredskaber	
2x Tavle, stor + farver	
Ekstra strømskinner	Normal og edb-stik
Kan rumme min. 15 personer	
Adgang til remote lyd/videoforbindelse	
Mulighed for tilkobling af PC til skærmdeling	
Internet adgang	min. 5G
Printer + printerpapir	

3 Handlingsplaner

I dette afsnit beskrives de operationelle handlingsplaner, som skal tages i brug i en beredskabssituation. Formålet med handlingsplanerne er at assistere beredskabsorganisationen med at huske de procedurer, som skal udføres i en beredskabssituation.

Handlingsplanerne er udformet som tjeklister og kan derfor også bruges som forløbsjournal. Som et alternativ kan tomme hændelsesjournalark i bilag 6.9 anvendes.

Hvis der er et behov for uddybende detailinstrukser, er der refereret til disse i afsnit 4.

Nr.	Handling	Ansvar	Tid (min)
1	**Kontakt retableringsteam** Kontakt retableringsteamet, hvis det ikke allerede er sket. Retableringsteamet bør flytte til den alternative driftslokation.	Systemarkitekt	Start:x Slut: x + 45
2	**Kontakt alternativ møde lokation** Kontakt den alternative møde lokation og aftal flytningen.	It-beredskabskoordinator	Start:x Slut:x + 5
3	**Flyt til alternativ møde lokation** Foretag flytningen til den alternative møde lokation.	It-beredskabskoordinator	Start: x Slut: x + 5
4	**Vurdér om infrastruktur kan genbruges** Foretag en vurdering af, om noget af den eksisterende infrastruktur kan genbruges på den alternative lokation.	Beredskabsleder	Start: x + 30 Slut: x + 120
5	**Kontrollér driftsmiljø** Kontroller at driftsmiljøet på den alternative lokation er i overensstemmelse med behovet for det udstyr, der ønskes opsat.	Systemarkitekt	Start: x Slut: x + 45
6	**Vurder behov for yderligere udstyr mv.** Vurder om der er behov for at anskaffe yderligere udstyr eller foretage ændringer på driftslokationen, f.eks. hævning af gulve, adgangskontrol mv.	It-beredskabskoordinator	Start: x Slut: NIL
7	**Anskaf og installer backup** Fremskaf backup og installer denne i udviklingsmiljøet.	It-beredskabskoordinator	Start: x Slut: x + 180

2	**Fastlæg datatab og informer brugere** Fastlæg omfanget af datatabet (RPO) og informer brugerne om, hvor stort et tidsrum, der mangler i systemet.	Fastlægges jf. afsnit 2.2	Start: Slut:
3	**Ret Server Entry** Tilret udviklingsmiljøet, så dette nu er produktionsmiljø.	Fastlægges jf. afsnit 2.2	Start: Slut:

4	**Implementer almindelige driftskontroller** Implementer de almindelige driftskontroller og konfigurationer såsom backup, overvågning mv.	Fastlægges jf. afsnit 2.2	Start: Slut:
5	**Informer it-beredskabskoordinator** Informer it-beredskabskoordinatoren når systemet er retableret.	Fastlægges jf. afsnit 2.2	Start: Slut:

[I denne skabelon er der inkluderet handlingsplaner for områderne beredskabsledelse og svigt af systemer eller infrastruktur, som fysisk er placeret hos en ekstern leverandør. Handlingsplanerne i skabelonen er kun eksempler. Organisationen skal med udgangspunkt i en risiko- og konsekvensvurdering udarbejde de nødvendige handlingsplaner.]

3.2 Forudsætninger

It-beredskabet for Sentinel Surveillance System er etableret på baggrund af risikovurderinger og det generelle trusselsbillede. Der er i den sammenhæng områder, der bevidst er set bort fra i beredskabet, og derfor skal beredskabsledelsen altid vurdere situationen og ikke blindt følge teksten. Endvidere bygger beredskabet på nogle overordnede forudsætninger, som er nævnt herunder. Handlingsplanernes specifikke forudsætninger fremgår af de konkrete planer.

Desuden skal det vurderes, om eventuelle udeståender jf. afsnit 5.3 giver anledning til justeringer af beredskabsforløbet.

Nr.	Handling	Ansvar	Tid
1	**Undersøg leverandørforhold** Det undersøges, hvilke opgaver som er outsourcet til en ekstern leverandør.	Fastlægges jf. afsnit 2.2	Start: Slut:
2	**Kontakt leverandør** Hvis ikke dette allerede er sket, fx i tilfælde af det er leverandøren der har konstateret og informeret om hændelsen, tages kontakt til leverandøren. Kontaktoplysningerne findes i afsnit 6.1	Fastlægges jf. afsnit 2.2	Start: Slut:
3	**Vurder situationen** Status gennemgås, og situationen vurderes i samarbejde med leverandøren. Hvis leverandøren	Fastlægges jf. afsnit 2.2	Start: Slut:

Nr.	Handling	Ansvar	Tid
	har behov for adgang til organisationens lokation, aftales det, hvordan adgangen finder sted.		
4	**Planlæg indsatsen** Planlæg opgaver og aftal det videre forløb. Er it-systemerne outsourcet, planlægges indsatsen i samarbejde med leverandøren.	Fastlægges jf. afsnit 2.2	Start: Slut:
5	**Kommunikation og kontakter** Planlæg hvordan kommunikationen med leverandøren skal foregå, og oplys kontaktoplysninger til eventuelle øvrige parter som leverandøren skal kommunikere med.	Fastlægges jf. afsnit 2.2	Start: Slut:

[Ved udarbejdelsen af de konkrete handlingsplaner er beskrivelse af planernes forudsætninger et vigtigt element. Ved stort set alle retableringsaktiviteter, uanset om de er af teknisk eller mere blød karakter, vil der være forhold, der er nødvendige at have opfyldt for at gennemføre retableringen, fx udstyr, aftaler, fysiske lokaliteter, logistiske forhold eller kompetencer.

Et afsnit til oplistning af sådanne forudsætninger bør indgå i indledningen af alle handlingsplaner]

- [*Kommandocentralen er ikke omfattet af hændelsen*]
- [*Den basale infrastruktur (telefoni, Internet mv.) er tilgængelig*]
- [*Minimum halvdelen af de udførende medarbejdere i beredskabet er til rådighed*]
- [*For SIT-kunder gælder, at Statens It's beredskab er ikke berørt af hændelsen*]

3.3 Aktivering af it-beredskabsplanen

It-beredskabet træder i kraft, når en hændelse ikke kan håndteres inden for rammerne af [*organisationens*] normale processer og arbejdsgange.

[Kriterierne for aktivering af it-beredskabet skal defineres og beskrives, så det er klart, under hvilke omstændigheder it-beredskabet skal aktiveres, og hvem der kan aktivere det.]

Bemærk: Hændelser, hvor løsningen er kendt, og den normale drift kan genoprettes inden for den fastsatte tidsgrænse, bør normalt ikke medføre aktivering af it-beredskabet.

Aktivering og mobilisering iværksættes, hvis der:

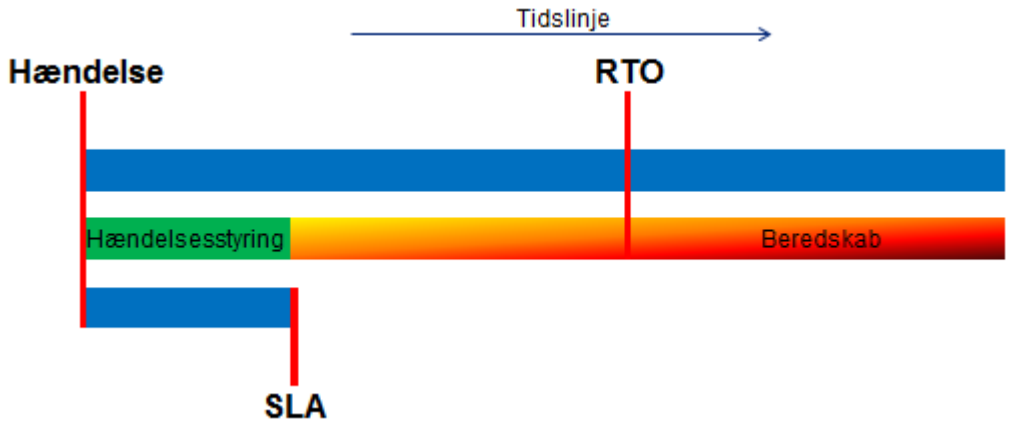
- er sikkerhed for, at et af følgende fire kriterier (a til d) er opfyldt,
- eller hvis flere kriterier vurderes i risiko for at blive opfyldt.

[Nedenfor er beskrevet kriterier, der kan bruges som pejlemærker for, om en given hændelse skal kategoriseres som en beredskabsmæssig krise. Det er dog væsentligt at pointere, at en krise til hver en tid kan erklæres af beredskabsledelsen på grundlag af en konkret vurdering. Selvom hændelsen ikke umiddelbart opfylder kriterierne for at iværksætte det fulde beredskab, kan dele af de operationelle handlingsplaner benyttes, fx kommunikationsplanen af hensyn til håndtering af interessenter. En væsentlig del af aktiveringen og styringen/ledelsen vil i en sådan situation bestå i at afgrænse indsatsen i forhold til planernes fulde omfang.]

a. Tidsmæssig udstrækning af hændelsen

Hvis det står klart, at en hændelse ikke kan håndteres og løses inden for de ramte aktivers serviceaftaler (SLA'er) for almindelig udbedring af hændelser, kan det være en indikation af en krise, der kræver aktivering af beredskabsplanen.

Hvis der er risiko for, at en hændelse ikke kan håndteres og løses inden for de ramte aktivers RTO, er der utvivlsomt tale om en krise, der kræver aktivering af beredskabsplanen, jf. illustrationen herunder.



b. Større datatab

Såfremt det står klart, at der efter en hændelse er risiko for datatab, der er større end tabstolerancerne, jf. RPO-værdierne, kan det være en indikation af en krise, der kræver aktivering af beredskabsplanen.

c. Graden af påvirkning

Hvis en stor del af infrastrukturen (servere, switche, etc.) er berørt af en hændelse, kan det være en indikation af en krise, der kræver aktivering af beredskabsplanen.

Det samme gør sig gældende, hvis en stor procentdel af medarbejdernes mulighed for at udføre deres arbejde er umiddelbart berørt af en hændelse.

d. Særlige hændelser

Særlige hændelser såsom:

- Naturkatastrofer (oversvømmelse, jordskælv, brand mv.) kan kræve umiddelbar aktivering af beredskabsplanen
- Brud i forsyningen af el, der går væsentligt ud over nødstrømskapaciteten
- Terrorisme, krig, sabotage, strejker

3.4 Planer for beredskabsledelsen

Handlingsplanerne for beredskabsledelse skal sikre, at der er tilstrækkelige organisatoriske og ledelsesmæssige rammer for it-beredskabet.

[Dette bør som minimum indebære, at de nedenstående områder planlægges og beskrives.]

3.4.1 Eskalering

Til at sikre struktureret initiering af beredskabsprocessen i forbindelse med en hændelse, anvendes nedenstående plan for eskalering.

[Formålet med eskaleringsprocessen er at guide ledelsen fra det tidspunkt, hvor en potentiel katastrofe identificeres, og indtil it-beredskabet er iværksat.

I forbindelse med bekræftelse af notifikation skal hændelsesjournalen startes. Hændelsesjournaler er vigtige redskaber i opfølgningsaktiviteter, fx erfaringsopsamling og forsikringsspørgsmål.

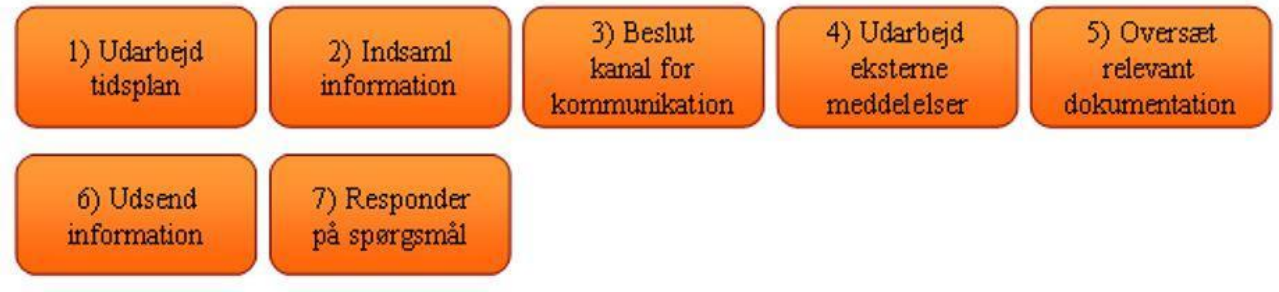
Processen kan bestå af følgende aktiviteter:]

Se yderligere i skabelon for eskaleringsproces i bilag 6.2.

3.4.2 Kommunikation

Kommunikation er en afgørende faktor for at kunne håndtere en beredskabssituation effektivt. I nedenstående plan er der taget hensyn til både den interne og eksterne kommunikation. Kontaktoplysningerne fremgår af tabel i afsnit 6.1

[Organisationen bør på forhånd have klarlagt, hvilke interessenter, det kan være relevant at kommunikere med i en beredskabssituation samt have en plan for håndtering af kommunikationen.]



Se i bilag 6.3 om kommunikationstjeklisten

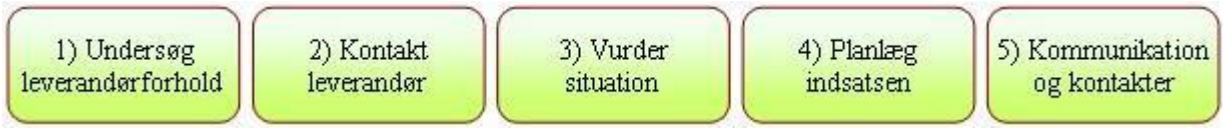
3.4.3 Plan for driftsnedbrud hos leverandør

Ved nedbrud hos en af [*organisationens*] driftsleverandører, skal det aftalte beredskab iværksættes så snart det vurderes nødvendigt. Nedenstående aktiviteter har til formål at varsko den konkrete leverandør og at sikre dialogen med leverandøren i hele beredskabssituationen.

[Når en eller flere leverandører varetager driften af kritiske it-systemer eller infrastruktur, skal det sikres, at it-beredskabet koordineres så effektivt som muligt. Nedenfor er angivet et eksempel på, hvordan en handlingsplan herfor kan opbygges. Handlingsplanen bør tilpasses de relevante

leverandører og de aftaler, som er indgået. Herunder skal planen tage højde for, om udstyret er fysisk placeret eksternt hos leverandøren eller internt i organisationens lokaler.]

For kunder i Statens It er kontaktinformationer og -kanaler beskrevet i kundeaftalerne. Det er afgørende, at eventuelle særlige processer der anvendes i en beredskabssituation fremgår af kundeaftalerne.



Se yderligere i bilag 6.4 vedrørende samarbejde med leverandøren.

3.4.4 Ibrugtagning af alternativ driftslokation

Følgende er kun relevant for de organisationer, der selv har drift af it-systemer og evt. har outsourcet visse tjenester eller systemer til en eller flere eksterne leverandører.

Formålet med denne handlingsplan er at sikre en hurtig og effektiv overgang til en alternativ driftslokation.

Se bilag 6.5 for skabelon til handlingsplan.

3.5 Hardware-relaterede planer

Afsnit 3.4 samt underafsnit er kun relevant for de organisationer, der selv har drift af it-systemer og evt. har outsourcet visse tjenester eller systemer til en eller flere eksterne leverandører.

I situationer, hvor det eksisterende hardware eller infrastruktur ikke kan genbruges, skal der fremskaffes nyt udstyr til at retablere it-driften. I de efterfølgende planer fremgår de respektive løsninger og afledte retableringsaktiviteter.

[Jo hurtigere fremskaffelsen af hardware skal foregå, jo større omkostninger vil der være forbundet hermed. Det er derfor vigtigt, at organisationen vælger en strategi, som er effektiv i forhold til behovet for retablering.

Nedenfor er angivet et eksempel med udgangspunkt i en strategi om at benytte eksisterende udstyr fra et udviklingsmiljø. Ved udarbejdelse af handlingsplanerne bør der tages hensyn til alle de relevante typer kritisk udstyr, herunder både servere, pc'er, enkeltstående komponenter mv.]

3.5.1 Server [eksempel]

Retableringsstrategi: Produktionsserveren retableres til udviklingsmiljøet, som er placeret fysisk adskilt fra produktionsserveren.

Se bilag 6.6 for skabelon til server-retableringsstrategi.

3.6 Netværksrelaterede planer

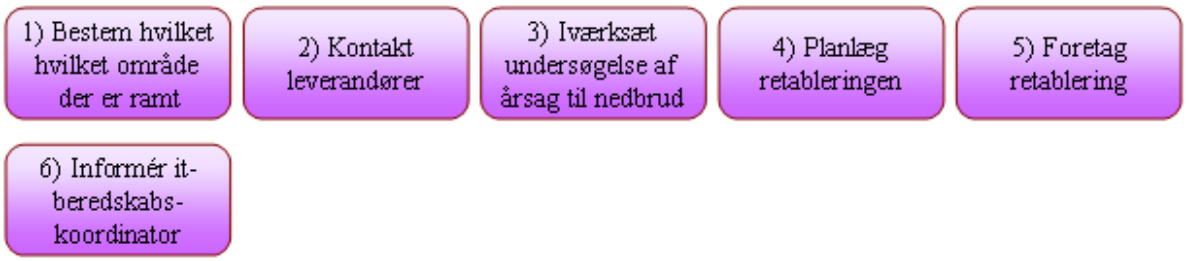
Handlingsplanerne for netværk skal sikre, at netværkskommunikationen kan genoprettes i tilstrækkeligt omfang inden for de fastsatte behov.

[Det er vigtigt, at organisationen vælger en strategi, som er effektiv i forhold til behovet for retablering.

Nedenfor er angivet et eksempel med udgangspunkt i en strategi om at benytte ekstern leverandør til drift af LAN miljøet.]

3.6.1 LAN [eksempel]

Retableringsstrategi: LAN drift er outsourcet til ekstern leverandør. Leverandøren er ansvarlig for retablering.



Se bilag 6.7 for skabelon til LAN-retableringsstrategi.

3.7 Handlingsplan for virus- eller hackerangreb

Handlingsplanen for virus- eller hackerangreb skal sikre en effektiv indsats i tilfælde af virusangreb eller hackerangreb.

[I sådanne situationer er der sjældent fra begyndelsen et klart overblik over hændelsens omfang, og planen er derfor et vigtigt støttepunkt i processen.

Organisationen bør bl.a. overveje, i hvilke situationer man vil/kan lukke internetforbindelsen, hvilke muligheder der er for at indsamle beviser mv.

CFCS udarbejder løbende vejledninger, der med fordel kan tages udgangspunkt i.]

Se bilag 6.8 for skabelon til handlingsplan for virus- og hackerangreb

4 Detailinstrukser

I dette afsnit findes de detaljerede instrukser mv., som er nødvendige i forhold til de operationelle handlingsplaner, beskrevet.

Instrukserne kan være relevante i flere sammenhænge, og der er henvisninger i de konkrete handlingsplaner. Instrukserne omfatter følgende områder:

[Hvilke instrukser, der er behov for afhænger af den konkrete beredskabsplanlægning, og strukturen i detailinstrukser beror på en individuel vurdering, som bør foretages af det personale der skal anvende instrukserne i en beredskabssituation. Eksempler på detailinstrukser fremgår herunder.]

- *[Oversigt over systemversioner]*

- *[Hardware specifikationer]*
- *[Genstartsprocedurer og rækkefølge]*
- *[Netværksdiagrammer]*
- *[Miljøkrav til datacenter]*

[*4.x Oversigt over systemversioner*]

[*4.y Hardware specifikationer*]

[…]

5 Vedligeholdelse af beredskabsplanen

5.1 Test

It-beredskabsplanen skal afprøves mindst en gang om året for at sikre, at den er effektiv, og at beredskabsorganisationen har kendskab til den. Planen skal desuden altid afprøves, hvis der foretages væsentlige ændringer i planen eller i organisationens it-anvendelse.

[Test af beredskabet bør aftales med leverandøren. Leverandøren bør altid foretage periodiske test af beredskabet. Her vil fokus særligt være på den tekniske retablering, og evnen til at efterleve organisationens behov i form af RTO og RPO. Men beredskabet bør også afprøves samlet for at sikre, at kommunikationen med organisationen fungerer effektivt i en krisesituation.

Valget af testtype og omfanget af testen skal planlægges i forhold til det konkrete behov. Følgende eksempel beskriver, hvordan afprøvningen kan planlægges.]

Frekvens	**Testtype**	**Omfang**
Årligt	*Skrivebordstest*	*Der foretages en skrivebordstest med udgangspunkt i et foruddefineret scenarie. Skrivebordstesten skal bl.a. afprøve eskaleringsprocessen og sikre, at kontaktoplysninger mv. er korrekte. Der foretages ikke afbrydelser i it-driften.*
Hvert 3. år	*Fuld test*	*Der foretages en fuld test af en eller flere handlingsplaner, hvor et eller flere systemer retableres med udgangspunkt i leverandørens retableringsplaner.*

5.2 Testhistorik

I nedenstående tabel er beredskabets tests og afprøvninger noteret herunder.

[Registreringerne bør indeholde overordnet testresultat og dokumenthenvisning til den fulde testrapport. Hvis det er relevant opbevares rapporterne på en måde der muliggør adgang til disse i en beredskabssituation, da mere detaljerede erfaringer her fra evt. kan bruges under en virkelig hændelse.]

Dato	**Testtype**	**Område**	**Resultat**	**Rapport / placering**

dd.mm.åå	*Skrivebord*	*Eskalering ifm. overgravet netværkskabel*	*Generelt ok internt, men forvirring omkring leverandørkontakt*	*ITBtest.org.åå01.final / X-drev + USB v/mødested*

5.3 Udeståender

[I forbindelse med afprøvninger konstateres typisk mangler eller uhensigtsmæssigheder i planen eller beredskabet, og indtil eventuel udbedring er foretaget og dokumenteret (ændret beredskab, ændret plan, eller accepteret risiko), kan viden om sådanne udeståender være af afgørende betydning for beredskabsorganisationen under en eventuel hændelse.

Det kan eksempelvis være, at planen forudsætter tilstedeværelse af en konkret hardwarekomponent, som endnu ikke er anskaffet. Dette forhold skal fremgå af oversigten.]

Dato	Kapitel	Ansvarlig	Udestående
dd.mm.åå	*3.4 – nedbrud hos leverandør*	*NN*	*Eksempel: Leverandørens kontaktinformationer er ikke opdateret grundet virksomhedsoverdragelse pr. dd.mm.åå*

5.4 Opdatering af planer

It-beredskabsplanen skal opdateres mindst en gang om året i forlængelse af den årlige afprøvning. Planen bør desuden opdateres, hvis der sker væsentlige ændringer i it-anvendelsen (f.eks. en ny leverandør), beredskabsorganisationen mv.

5.4.1 Versionshistorik

Version	Dato	Ansvarlig	Ændringsbeskrivelse	Godkendt	Distribueret
0.1	*dd.mm.åå*	*NN*	*Første udkast*	*n/a*	*n/a*
0.2	*dd.mm.åå*	*NN*	*Navne og planstruktur fastlagt*	*n/a*	*Projektgruppe*
0.9	*dd.mm.åå*	*NN*	*Plan foreligger klar til test*	*Kontorchef*	*Modtagerliste*
1.0	*dd.mm.åå*	*NN*	*Justeret i henhold til testresultater*	*Direktør*	*Modtagerliste*

5.4.2 Distribution og opbevaring

It-beredskabsplanen skal opbevares, så den altid er tilgængelig i en beredskabssituation. Hvert medlem af beredskabsorganisationen bør opbevare et fysisk eksemplar af planen. Den vedligeholdelsesansvarlige er ansvarlig for distribution af opdateringer til alle modtagere af planen.

[I denne oversigt skal angives den præcise lokation for opbevaring af kopier af beredskabsplanen (adresse, evt. boksnummer mv.).]

Modtager	**Rolle**	**Lokation / opbevaring**	**Bemærkninger**
Navn 1	*Direktør*	*Adresse og placering*	*Kun elektronisk kopi*
Navn 2	*Kontorchef*	*Adresse og placering*	
Sted A	*Kommandocentral*	*Adresse og placering*	*3 kopier i aflåst skab – nøgle hos NN*

6 Bilag

Kontaktlister

	Kontaktliste for beredskabsorganisation					
Rolle	Primær/substitut	Navn	Adresse	E-mail	Tlf.	Alternativ tlf. og e-mail
It-beredskabskoordinator	Primær					
	Substitut					
It-chef (Hvis relevant)	Primær					
	Substitut					

	Kontaktliste for forretning					
Forretningsområde	Primær/substitut	Navn	Adresse	E-mail	Tlf.	Alternativ tlf. og e-mail
Kontorchef - afdeling A	Primær					
	Substitut					

	Kontaktliste for andre beredskaber i organisationen					
Plan	Primær/substitut	Navn	Adresse	E-mail	Tlf.	Alternativ tlf. og e-mail
Evakueringsplan	Primær					

	Substitut					
Forretningsberedskab	Primær					
	Substitut					
Forretningsnødplan A	Primær					
	Substitut					
Forretningsnødplan B	Primær					
	Substitut					

	Ekstern kontaktliste					
Rolle	Primær/substitut	Navn	Adresse	E-mail	Tlf.	Alternativ tlf. og e-mail
Driftsleverandør – servere	Primær					
	Substitut					
Driftsleverandør – pc'er	Primær					
	Substitut					
Leverandør – applikation A	Primær					
	Substitut					
Netværksleverandør - LAN	Primær					
	Substitut					
CFCS' situationscenter	Primær	Vagt		cfcs@cert.cfcs.dk	33325580	

Hvis organisationen anvender Statens It som driftsleverandør, skal de i tilfælde af en beredskabssituation kontaktes på telefon: 72310001 eller via Serviceportalen (http://serviceportalen.statens-it.dk/)

Eskaleringsproces

Nr.	Handling	Ansvar	Tid
1	**Modtag notifikation** Når en notifikation om en potentiel katastrofe modtages, skal følgende oplysninger forsøges fremskaffet: ● Typen af hændelsen ● Eventuelle tilskadekomne personer ● Omfanget af skaden ● Hvilke eksterne leverandører er involveret	Fastlægges jf. afsnit 2.2	Start: Slut:
1.1	**Start hændelsesjournal** Brug kolonne i nærværende tabel, eller anvend tom skabelon i bilag 6.9	Modtager af notifikation	Start: Slut:
2	**Bekræft notifikation** Få notifikationen bekræftet hvis nødvendigt.	Fastlægges jf. afsnit 2.2	Start: Slut:
3	**Evakuer medarbejdere** Hvis evakuering er nødvendig, så følg planen for evakuering af bygningen.	Fastlægges jf. afsnit 2.2	Start: Slut:
4	**Kontakt Alarmcentralen** Kontakt Alarmcentralen hvis nødvendigt.	Fastlægges jf. afsnit 2.2	Start: Slut:
5	**Indledende vurdering af omfang** Foretag en indledende vurdering af skadesomfanget. Skade på bygninger mv. bør vurderes af de bygningsansvarlige, mens skade på informationssystemer vurderes af it-chefen eller it-beredskabskoordinatoren, evt. understøttet af leverandører, som har driftsansvaret på dele af systemporteføljen.	Fastlægges jf. afsnit 2.2	Start: Slut:
5.1	**Vurder notifikation af øvrige beredskaber** Hvis it-beredskabet er iværksat som det første, kan det være relevant at notificere andre dele af koncernens beredskab. Se oversigt i afsnit 6.1	Fastlægges jf. afsnit 2.2	Start: Slut:

Nr.	Handling	Ansvar	Tid
6	**Incident evaluering / eskalering til leverandør** Vurder situationen og undersøg hos leverandøren, hvor lang tid der skal bruges på at retablere skaderne, og bestem ud fra kriterierne i afsnit 3.2, om it-beredskabet skal aktiveres. Driftsleverandører varsles om mulig beredskabssituation	Fastlægges jf. afsnit 2.2	Start: Slut:
7	**Aktivering af it-beredskab** Aktiver it-beredskabet. Beslutningen om at aktivere it-beredskabet skal kommunikeres til beredskabsorganisationen. Informer om kendte udeståender jf. afsnit 5.3.	Fastlægges jf. afsnit 2.2	Start: Slut:
8	**Organisér beredskabsledelsen** Med udgangspunkt i den besluttede beredskabsorganisation mobiliseres beredskabsledelsen. Beredskabsledelsen vurderer situationen og igangsatte aktiviteter bekræftes eller tilpasses. Beredskabsledelsen konsolideres og fastholdes til beslutning om normalisering er truffet.	Fastlægges jf. afsnit 2.2	Start: Slut:
8.1	**Aktiver plan for driftsnedbrud hos leverandør** Udveksling af kontaktdetaljer, kommunikationsmønster og evt. aftaler for ekstern kommunikation i beredskabsforløbet. Aktivering foregår i henhold til aftaler. Se afsnit 3.3.3	Fastlægges jf. afsnit 2.2	Start: Slut:
9	**Information til interessenter** Øvrige relevante interessenter informeres om it-beredskabet. Igangsæt plan for kommunikation jf. afsnit 3.3.2	Fastlægges jf. afsnit 2.2	Start: Slut:
10	**Fastlæg omfanget af skaden** Medmindre skadens omfang er åbenlys, f.eks. ved tab af en hel bygning, foretages en nærmere registrering af de berørte aktiver. Se desuden handling nr. 5 og 5.1.	Fastlægges jf. afsnit 2.2	Start: Slut:

Nr.	Handling	Ansvar	Tid
10. 1	**Påbegynd planlægning af normalisering** For at minimere perioden med nedsat driftsfunktionalitet i beredskabssituationen og unødige omkostninger, igangsættes i relevant omfang planlægning af aktiviteter til normaliseret drift. Anvend evt. tjekliste i bilag 6.10	Fastlægges jf. afsnit 2.2	Start: Slut:

Kommunikationstjekliste

Nr.	Handling	Ansvar	Tid
1	**Udarbejd tidsplan** Der udarbejdes en tidsplan for ekstern og intern kommunikation.	Fastlægges jf. afsnit 2.2	Start: Slut:
2	**Indsaml information** Al information, som er påkrævet for intern og ekstern kommunikation, samles hos den kommunikationsansvarlige.	Fastlægges jf. afsnit 2.2	Start: Slut:
3	**Beslut kommunikationskanal** For hver enkel intern og ekstern kommunikation fastlægges kommunikationskanalen. Hvis organisationen anvender Statens It som driftsleverandør, skal kommunikationskanalen koordineres med Statens It's beredskab. Desuden skal konkrete aftaler i den forbindelse fremgå af kundeaftalen.	Fastlægges jf. afsnit 2.2	Start: Slut:
4	**Udarbejd eksterne meddelelser** Udarbejd meddelelser til ekstern kommunikation, og få disse godkendt af beredskabsledelsen.	Fastlægges jf. afsnit 2.2	Start: Slut:
5	**Oversæt relevant dokumentation** Hvis der er behov for at vedlægge dokumentation, foretages eventuelt oversættelse heraf.	Fastlægges jf. afsnit 2.2	Start: Slut:
6	**Udsend information** Sørg for, at al intern og ekstern kommunikation udsendes samtidigt, hvis dette er påkrævet, og at budskaberne er ens.	Fastlægges jf. afsnit 2.2	Start: Slut:
7	**Responder på spørgsmål** Svar på eventuelle spørgsmål med fokus på de mest kritiske spørgsmål og interessenter.	Fastlægges jf. afsnit 2.2	Start: Slut:

Leverandørsamarbejde

Nr.	Handling	Ansvar	Tid
1	**Undersøg leverandørforhold** Det undersøges, hvilke opgaver som er outsourcet til en ekstern leverandør.	Fastlægges jf. afsnit 2.2	Start: Slut:
2	**Kontakt leverandør** Hvis ikke dette allerede er sket, fx i tilfælde af det er leverandøren der har konstateret og informeret om hændelsen, tages kontakt til leverandøren. Kontaktoplysningerne findes i afsnit 6.1	Fastlægges jf. afsnit 2.2	Start: Slut:
3	**Vurder situationen** Status gennemgås, og situationen vurderes i samarbejde med leverandøren. Hvis leverandøren har behov for adgang til organisationens lokation, aftales det, hvordan adgangen finder sted.	Fastlægges jf. afsnit 2.2	Start: Slut:
4	**Planlæg indsatsen** Planlæg opgaver og aftal det videre forløb. Er it-systemerne outsourcet, planlægges indsatsen i samarbejde med leverandøren.	Fastlægges jf. afsnit 2.2	Start: Slut:
5	**Kommunikation og kontakter** Planlæg hvordan kommunikationen med leverandøren skal foregå, og oplys kontaktoplysninger til eventuelle øvrige parter som leverandøren skal kommunikere med.	Fastlægges jf. afsnit 2.2	Start: Slut:

Skabelon til handlingsplan

Nr.	Handling	Ansvar	Tid
1	**Kontakt retableringsteam** Kontakt retableringsteamet, hvis det ikke allerede er sket. Retableringsteamet bør flytte til den alternative driftslokation.	Fastlægges jf. afsnit 2.2	Start: Slut:
2	**Kontakt alternativ driftslokation** Kontakt den alternative driftslokation og aftal flytningen.	Fastlægges jf. afsnit 2.2	Start: Slut:
3	**Flyt til alternativ driftslokation** Foretag flytningen til den alternative driftslokation.	Fastlægges jf. afsnit 2.2	Start: Slut:
4	**Fremskaf backup mv.** Fremskaf backup og øvrige nødvendige aktiver, som har været opbevaret på en ekstern lokation, f.eks. adgangskoder, nøgler mv.	Fastlægges jf. afsnit 2.2	Start: Slut:
5	**Vurdér om infrastruktur kan genbruges** Foretag en vurdering af, om noget af den eksisterende infrastruktur kan genbruges på den alternative lokation.	Fastlægges jf. afsnit 2.2	Start: Slut:
6	**Viderestil telefonopkald** Foretag viderestilling af telefonopkald, så de kan modtages på den alternative lokation.	Fastlægges jf. afsnit 2.2	Start: Slut:
7	**Kontrollér driftsmiljø** Kontroller at driftsmiljøet på den alternative lokation er i overensstemmelse med behovet for det udstyr, der ønskes opsat.	Fastlægges jf. afsnit 2.2	Start: Slut:
8	**Vurder behov for yderligere udstyr mv.** Vurder om der er behov for at anskaffe yderligere udstyr eller foretage ændringer på driftslokationen, f.eks. hævning af gulve, adgangskontrol mv.	Fastlægges jf. afsnit 2.2	Start: Slut:

Skabelon til server-retableringsstrategi

Nr.	Handling	Ansvar	Tid
1	**Anskaf og installer backup** Fremskaf backup og installer denne i udviklingsmiljøet.	Fastlægges jf. afsnit 2.2	Start: Slut:
2	**Fastlæg datatab og informer brugere** Fastlæg omfanget af datatabet (RPO) og informer brugerne om, hvor stort et tidsrum, der mangler i systemet.	Fastlægges jf. afsnit 2.2	Start: Slut:
3	**Ret Server Entry** Tilret udviklingsmiljøet, så dette nu er produktionsmiljø.	Fastlægges jf. afsnit 2.2	Start: Slut:
4	**Implementer almindelige driftskontroller** Implementer de almindelige driftskontroller og konfigurationer såsom backup, overvågning mv.	Fastlægges jf. afsnit 2.2	Start: Slut:
5	**Informer it-beredskabskoordinator** Informer it-beredskabskoordinatoren når systemet er retableret.	Fastlægges jf. afsnit 2.2	Start: Slut:

LAN-retableringsstrategi

Nr.	Handling	Ansvar	Tid
1	**Bestem hvilket områder der er ramt** Foretag en undersøgelse af, hvilke områder som er ramt af nedbrud.	Fastlægges jf. afsnit 2.2	Start: Slut:
2	**Kontakt eventuelle leverandører** Kontakt leverandøren og vurder situationen.	Fastlægges jf. afsnit 2.2	Start: Slut:
3	**Iværksæt undersøgelse af årsagen til nedbruddet** Assister leverandøren med at identificere årsagen til nedbruddet.	Fastlægges jf. afsnit 2.2	Start: Slut:
4	**Planlæg retableringen** Planlæg hvordan der retableres.	Fastlægges jf. afsnit 2.2	Start: Slut:
5	**Foretag retablering** Foretag den planlagte retablering, f.eks. udskiftning af defekt hardware.	Fastlægges jf. afsnit 2.2	Start: Slut:
6	**Informer it-beredskabskoordinator** Informer it-beredskabskoordinatoren og kommuniker til øvrige interessenter.	Fastlægges jf. afsnit 2.2	Start: Slut:

Skabelon til handlingsplan for virus- og hackerangreb

Nr.	Handling	Ansvar	Tid
1	**Vurder situationen** Vurder situationen. Hvis der er risiko for, at data kan blive kompromitteret, afbrydes internetforbindelsen.	Fastlægges jf. afsnit 2.2	Start: Slut:
2	**Luk systemer** Vurder om der er behov for at lukke systemer for at undgå spredning af angrebet. Informer relevante systemejere, brugere mv.	Fastlægges jf. afsnit 2.2	Start: Slut:
3	**Iværksæt undersøgelse** Iværksæt en undersøgelse af angrebet. Kontakt evt. GovCERT.	Fastlægges jf. afsnit 2.2	Start: Slut:
4	**Skift adgangskoder** Det vurderes, om adgangskoder bør skiftes.	Fastlægges jf. afsnit 2.2	Start: Slut:
5	**Aktiver ekstra systemlogning** Det vurderes, om der bør iværksættes ekstra logning af systemer og netværk for at opklare og indsamle beviser om hændelsen.	Fastlægges jf. afsnit 2.2	Start: Slut:
6	**Kontakt leverandører** Hvis de ramte områder driftes eksternt , kontakt leverandørerne.	Fastlægges jf. afsnit 2.2	Start: Slut:
7	**Kontakt myndigheder** Det skal vurderes, om der skal foretages politianmeldelse, og om der er andre myndigheder, som bør kontaktes, herunder GovCERT (jf. dog handling nr.3.	Fastlægges jf. afsnit 2.2	Start: Slut:
8	**Informer interessenter** Eventuelle øvrige interessenter informeres.	Fastlægges jf. afsnit 2.2	Start: Slut:

Hændelsesjournal

Beredskabsplan: _____ Startdato: ___ / ___ - 20___

Start	Slut	Noteret af	Aktivitet	Evt. godk.

Tjekliste for normaliseret drift

[Drift i et beredskabs-setup er generelt begrænsende i forhold til både funktionalitet og effektivitet, og desuden omkostningstungt. Derfor bør der tidligt i forløbet nedsættes en kompetent gruppe medarbejdere, der har til opgave at udarbejde en forsvarlig plan for at sikre hurtig returnering til normal drift.

Der bør udarbejdes en liste med relevante aktiviteter i forhold til organisationens specifikke forhold, men herunder er oplistet nogle inspirationspunkter.]

- □ Fungerer de fysiske rammer for normal drift?
- □ Er det nødvendige personale til rådighed for normal drift?
- □ Er der behov for genanskaffelser af udstyr til personale?
- □ Har nogen forretningsområder ligget stille – hvad skal til for at få disse i drift?
- □ Kan – og skal – systemer der ikke er omfattet af it-beredskabet retableres?
- □ Skal der information til eksterne interessenter om normaliserede/ændrede procedurer?
- □ Skal der indgås nye aftaler med leverandører?

Mødested og hjælpeværktøjer på mødested

Mødested for it-beredskabsledelsen				
Type	Bygningsnavn	Adresse	Lokale	Fastnet telefon
Primær	*Slottet*	*Præcis entydig adresse.*	*Mødelokale v/DIR*	*11 22 33 44*
Sekundær	*Skuret*	*Præcis entydig adresse.*	*Lokale 4081*	*55 66 77 88*

Hjælpeværktøjer:

Artikel	**Kommentar**
Beredskabsplan i papirformat	
Beredskabsplan på USB-stik	
Ekstra hændelseslog	25 Printkopier
Papir og skriveredskaber	
Ekstra strømskinner	Normal og edb-stik
osv.	