It-beredskabsplan

for

[*Organisation*]

[Denne skabelon til it-beredskabsplan er skrevet til en organisation, som har outsourcet hele driften af it-systemerne til en eller flere eksterne leverandører.

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

|  |  |
| --- | --- |
| Version | *Skabelon* |
| Dato | Juli 2018 |
| Godkendt af |  |

# Før du går i gang - vejledning til brug af skabelonen

Denne skabelon er bygget op over en generisk struktur med generel information og hints, vejledende tekstforslag og tekst og tabeller, som vil dække de flestes behov. Typografien i skabelonen er søgt anvendt på en måde, der letter opgaven med at udarbejde beredskabsplanen.

Skabelonen er beskrevet ud fra den antagelse, at organisationen ikke har noget tidligere beredskab at bygge på. Publikationen ”Vejledning til it-beredskab” gennemgår terminologien bag beredskabet og hvordan man lettest kommer i gang. Er principperne bag beredskabsarbejdet kommet ind under huden, vil man relativt hurtigt kunne udarbejde en første version af en plan.

Det kan ikke anbefales, at man bygger en beredskabsplan ud fra nærværende skabelon ved at bruge ’søg- og-erstat’-funktionen.

|  |  |
| --- | --- |
| Typografi | Anvendelse i praksis |
| Normal tekst | Kan anvendes som udgangspunkt for lokale beskrivelser og andet indhold, men bør erstattes med organisationens eget sprog. |
| [Gråtonet tekst i firkantede parenteser] | Generel information, hints eller anden hjælp til at udfylde skabelonen. Teksten bør slettes, inden planen bliver udgivet lokalt. |
| [*Kursiveret tekst i firkantede parenteser*] | Tekstforslag og inspiration til konkrete indholdselementer, som skal erstattes med lokalt indhold. |

Indholdsfortegnelse Side

[Før du går i gang - vejledning til brug af skabelonen 2](#_Toc361214852)

[I TILFÆLDE AF EN HÆNDELSE 5](#_Toc361214853)

[1 Indledning 6](#_Toc361214854)

[2 Operationel planlægning 7](#_Toc361214855)

[2.1 Tidsmæssige målsætninger for retablering 7](#_Toc361214856)

[2.1.1 Prioriteret systemliste 7](#_Toc361214857)

[2.2 Beredskabsorganisation 8](#_Toc361214858)

[2.2.1 Beredskabsorganisationens struktur 9](#_Toc361214860)

[2.2.2 Roller og ansvar 9](#_Toc361214861)

[2.2.3 Kontaktlister 10](#_Toc361214862)

[2.2.4 Mødested 11](#_Toc361214863)

[3 Handlingsplaner 12](#_Toc361214864)

[3.1 Forudsætninger 12](#_Toc361214865)

[3.2 Aktivering af beredskabsplanen 12](#_Toc361214866)

[3.3 Planer for beredskabsledelsen 14](#_Toc361214867)

[3.3.1 Eskalering 14](#_Toc361214868)

[3.3.2 Kommunikation 16](#_Toc361214869)

[3.4 Plan for driftsnedbrud hos leverandør 18](#_Toc361214870)

[4 Vedligeholdelse af beredskabet 20](#_Toc361214871)

[4.1 Test 20](#_Toc361214872)

[4.2 Testhistorik 20](#_Toc361214873)

[4.3 Udeståender 20](#_Toc361214874)

[4.4 Opdateringer af planer 21](#_Toc361214875)

[4.4.1 Versionshistorik 21](#_Toc361214876)

[4.4.2 Distribution og opbevaring 21](#_Toc361214877)

[5 Bilag 22](#_Toc361214878)

[5.1 Hændelsesjournal 22](#_Toc361214879)

[5.2 Tjekliste for normaliseret drift 23](#_Toc361214880)

[5.3 Hjælpeværktøjer på mødested 24](#_Toc361214881)

## I TILFÆLDE AF EN HÆNDELSE

Hvis du er den første der kontaktes i forbindelse med en handling, start med vurdering af om der kræves beredskabshandlinger, samt åbn hændelsesjournal:

* **afsnit 3.2 Aktivering af beredskabsplanen**
* **afsnit 5.1 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 retableringsplaner 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**

**afsnit 4.3 Udeståender**

# 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.

[Der er udarbejdet en skabelon for en it-beredskabsstrategi, som kan bruges sammen denne plan. Skabelonen er tilgængelig på Digitaliseringsstyrelsens hjemmeside.]

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 |
| 3.4 | Driftsnedbrud hos leverandør |
| Vedligeholdelse |  | 4.1 | 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. |
| 4.3 | Udeståender |
| 4.4 | Opdatering af planer |
| Bilag |  | 5.1 | Hændelsesjournal |  | Afsnittene indeholder hjælpeværktøjer og information til brug i en beredskabssituation. |
| 5.2 | Tjekliste til normaldrift |
| 5.3 | Hjælpeværktøjer / mødested |

Figur 1 – Skabelonens overordnede struktur.

# Operationel planlægning

Operationel planlægning er dokumentation af [*organisationens*] forarbejde, der er med til at sikre, at beredskabsplanen opfylder forretningens behov og beskriver mål og rammer for beredskabet i tilfælde af en hændelse.

## 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 [*organisationen*] har besluttet
* de sikringsforanstaltninger, der er implementeret
* beredskabsplanens operationelle processer

[En forudsætning for at kunne opfylde RTO-værdierne er, at kritiske it-systemer er identificeret, og at der har været en dialog med repræsentanter for forretningen om, hvor længe it-understøttelsen kan undværes. Denne dialog kan f.eks. have fundet sted i forbindelse med gennemførelse af de periodiske risikovurderinger. Der er udarbejdet en skabelon for identificering af kritiske forretningsprocesser, som kan anvendes i sammenhæng med denne plan. Skabelonen er tilgængelig på Digitaliseringsstyrelsens hjemmeside]

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

### Prioriteret systemliste

|  |  |  |
| --- | --- | --- |
| **Prioritet** | **Systemnavn** | **RTO** |
| *1* | *System A* | *2 timer* |
| *2* | *System B* | *12 timer* |
| *3* | *System C* | *5 timer* |
| *4* | *System D* | *1 dag* |
| *5* | *System E* | *3 dage* |

[Organisationen kan vælge at supplere oversigten over RTO-værdier med en angivelse af den maksimale tolerance for datatab i hvert system. Denne værdi – kaldet Recovery Point Objective (RPO) – skal ligesom RTO være fastsat på baggrund af en dialog med forretningen. I en beredskabssituation vil RTO-værdierne være bestemmende for, hvilke datasæt der skal indlæses i forbindelse med den tekniske retablering.

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

|  |
| --- |
| Såfremt organisationen benytter Statens It som driftsleverandør, skal de tidsmæssige målsætninger indberettes ved brug af den dertil indrettede *systemindberetningsskabelon*, som også anvendes i beredskabssituationer. Ændringer til indberettede data skal ske ved at genindsende skabelonen med de nye værdier.  Aftalerne skal dokumenteres eksplicit i Statens It’s kundeaftalekompleks (Kundeaftale og Databehandleraftale), da Kundeaftalerne som standard ikke tager højde for særlige krav vedr. sikkerhed, og dermed ikke er dækkende for systemer med høj kritikalitet, eller systemer der indeholder data omfattet af Persondataloven eller som vurderes at være følsomme. |

## Beredskabsorganisation

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

[Organisationen kan vælge at fastholde den eksisterende organisationsstruktur, eller oprette en ny organisation særligt til it-beredskabets formål. I mange tilfælde vil det være mest hensigtsmæssigt at tage udgangspunkt i den eksisterende organisationsstruktur, da kommunikation, arbejdsgange mv. således allerede er indøvet.]

### Beredskabsorganisationens struktur



### Roller og ansvar

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 [*organisation*].

[Som udgangspunkt beskrives kun organisationens egen beredskabsorganisation, da det antages, at leverandøren selv varetager styringen i sin egen organisation. Hvis der er aftalt særlige forpligtelser med leverandøren, bør disse beskrives nedenfor.

I forbindelse med udarbejdelse af rollerne skal det vurderes, i hvilket omfang, der er behov og mulighed for at anvende stedfortrædere. Stedfortrædere angives i den efterfølgende kontaktliste.

Et eksempel på typiske beredskabsmæssige roller og opgaver er angivet nedenfor]

| **Rolle** | **Opgaver** |
| --- | --- |
| It-beredskabsledelse | *[It-beredskabsledelsen er øverste myndighed i forhold til alle beslutninger, der vedrører den operationelle håndtering af en beredskabsmæssig krise. Beredskabsledelsen fungerer som forum for drøftelse af væsentlige ledelsesmæssige beslutninger vedrørende den operationelle håndtering af den beredskabsmæssige krise.*  *I en krisesituation nedsættes altid en ledelsesgruppe, som består af den øverste (tilgængelige) chef samt ledere af relevante forretningsområder. Hvis organisationen har en ansvarlig for it-driften, bør denne ligeledes indgå i ledelsen. Formanden er den til enhver tid øverst rangerende chef.]* |
| It-beredskabskoordinator | *[It-beredskabskoordinatoren opretter og vedligeholder hændelsesjournalen, bistår ledelsen og sikrer koordinering af de enkelte aktiviteter.*  *Koordinatoren kan være organisationens it-sikkerhedskoordinator eller en person med stort indblik og organisationstalent, fx medlem af direktionssekretariatet.]* |
| Kommunikationsansvarlig | *[Organisationens eksterne interessenter skal informeres om situationen og de løbende fremskridt. Afhængig af organisationens forretningsområder vil både kunder, offentlighed og presse være omfattet af interessenterne.*  *Den kommunikationsansvarlige bør have tilsvarende rolle i det daglige grundet behovet for kommunikative færdigheder og ikke mindst erfaring.]* |
| Leverandørens roller | *[Hvis der er aftalt særlige roller med leverandøren, bør disse beskrives her. Det kan f.eks. være kontaktpersoner, koordinatorer mv.]* |

### Kontaktlister

Kontaktlisterne er udgangspunktet for mobilisering af beredskabsorganisationen, men kan også anvendes i forhold til den øvrige interne og eksterne kommunikation:

[Kontaktlisterne bør omfatte hele beredskabsorganisationen, men også relevante kontaktpersoner i den øvrige forretning samt eksterne leverandører bør indgå.

Når kontaktlisterne udarbejdes, bør der tages højde for, at de almindelige kommunikationskanaler kan være utilgængelige, således at der angives flere kontaktmuligheder for deltagerne, herunder prioriterede telefonnumre til nøglepersoner i staten.]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Kontaktliste for it-beredskabsorganisation** | | | | | |
| Rolle | Primær/substitut | Navn | Adresse | E-mail | Tlf. | Alternativ tlf. og e-mail |
| *It-beredskabskoordinator* | Primær |  |  |  |  |  |
| Substitut |  |  |  |  |  |
|  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Kontaktliste for organisationen** | | | | | |
| 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** | | | | | |
| Leverandør | Primær/substitut | Navn | Adresse | E-mail | Tlf. | Alternativ tlf. og e-mail |
| *Driftsleverandør – servere* | Primær |  |  |  |  |  |
| Sekundær |  |  |  |  |  |
| *Driftsleverandør – pc’er* | Primær |  |  |  |  |  |
| Sekundær |  |  |  |  |  |
| *Leverandør – applikation A* | Primær |  |  |  |  |  |
| Sekundær |  |  |  |  |  |
| *Netværksleverandør - LAN* | Primær |  |  |  |  |  |
| Sekundær |  |  |  |  |  |
|  |  |  |  |  |  |  |

|  |
| --- |
| Hvis organisationen anvender Statens It som driftsleverandør, skal de i tilfælde af en beredskabssituation kontaktes på telefon: 7231 0001 eller via Serviceportalen (<http://serviceportalen.statens-it.dk/>) |

### Mødested

Herunder er det angivet, på hvilken adresse medlemmerne af beredskabsledelsen skal møde op, hvis de bliver mobiliseret i en beredskabssituation. Ud over et lokale på [organisationens] faste lokation, er der etableret et alternativt mødested i tilfælde af bygninger eller infrastruktur er beskadiget:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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* |

På mødestederne skal forefindes basale hjælpeværktøjer jf. bilag 5.3

# 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 5.1 anvendes.

[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.]

## Forudsætninger

It-beredskabet for [*organisation*] er etableret på baggrund af risikovurderinger og det generelle trusselsbillede, og planerne er testet i henhold til testhistorikken i afsnit 4.2. 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 4.3 giver anledning til justeringer af beredskabsforløbet.

[Ved udarbejdelsen af de konkrete handlingsplaner, er beskrivelse af planernes forudsætninger et vigtigt element. Ved stort set alle retableringsaktiviteter, uanset om disse 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*]

## Aktivering af 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:

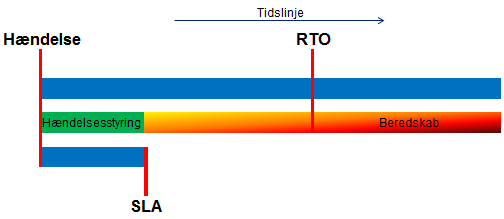
* + enten er sikkerhed for, at et af følgende fire kriterier (a-d) er opfyldt,
  + eller hvis flere kriterier vurderes i risiko for at blive opfyldt.

[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.]

1. **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.



1. **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.

1. **Graden af påvirkning**

Hvis en stor del af infrastrukturen (servere, switche m.v.) 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.

1. **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

## 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.]

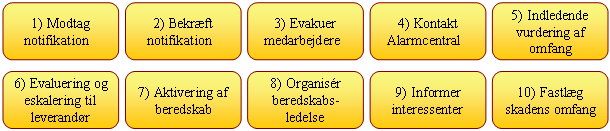
### Eskalering

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.]

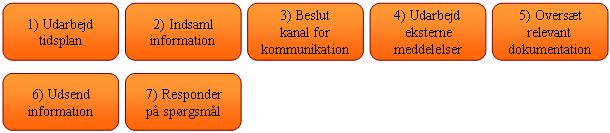


| **Nr.** | **Handling** | **Ansvar** | **Tid** |
| --- | --- | --- | --- |
| 1 | **Modtag notifikation**  Når en notifikation om en potentiel katastrofe modtages, skal følgende oplysninger forsøges fremskaffet:   * Typen af hændelsen * Eventuelle tilskadekomne personer * Omfanget af skaden * Hvilke 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 5.1. | 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-beredskabskoordinatoren eller den leverandør, som har driftsansvaret. | 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 kontaktliste i afsnit 2.2.3 | Fastlægges jf. afsnit 2.2 | Start:  Slut: |
| 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.  Driftsleverandøren 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 4.3. | 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 3.4. | 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: |
| 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 5.2. | Fastlægges jf. afsnit 2.2 | Start:  Slut: |

### 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 2.2.3.

[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.]



| **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, og 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: |

## 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. |



| **Nr.** | **Handling** | **Ansvar** | **Tid** |
| --- | --- | --- | --- |
| 1 | **Undersøg leverandørforhold**  Det undersøges, hvilken leverandør den ramte it-understøttelse er outsourcet til. | 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 2.2.3. | 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 indsatsen i samarbejde med leverandøren, og aftal det videre forløb. | 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: |

# Vedligeholdelse af beredskabet

## 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.* |

## 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 herfra 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* |

## 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* |

## Opdateringer 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.

### 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* |

### 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* |

# Bilag

## Hændelsesjournal

Beredskabsplan: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Startdato: \_\_\_ / \_\_\_ - 20\_\_\_

| **Start** | **Slut** | **Noteret af** | **Aktivitet** | **Evt. godk.** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Tjekliste for normaliseret drift

[Drift i et beredskabssetup 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?

## Hjælpeværktøjer på mødested

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