**Miljøstyrelsens DCIS**



**Skabelon for it-beredskabsplan**

|  |  |
| --- | --- |
| Version |  |
| Dato |  |
| Godkendt af |  |

# *Indledning*

Indledningen skal slettes og er kun inkluderet for at give en vejledning til skabelonen.

## *Læsevejledning*

|  |  |
| --- | --- |
| *Rød kursiv* | Vejledende tekst, der forklarer, hvad afsnittet kan indeholde, hvilke overvejelser den enkelte forsyning kan gøre sig, tips og generel information. Dette skal fjernes i udmøntningen af politikken. |
| *Grøn kursiv* | Erstattes med relevant information/beskrivelser fx navn på forsyningsselskabet, it-system, roller mv. |
|  |  |
| Yderligere tekst | Teksteksempler på hvordan en it-beredskabsplan kan se ud i form af specifikke roller, afsnit og handlinger. Teksten kan redigeres, så den reflekterer forsyningsselskabets kontekst, organisering, strategi mv. |

Denne skabelon til en it-beredskabsplan er bygget op over en generisk struktur med generel information, vejledende tekstforslag og handlingsangivende aktiviteter. Skabelonen kan tjene som inspiration og eventuel optimering af forsyningens it-beredskabsplan, såfremt forsyningen allerede har en beredskabsplan. Hvis organisationen ikke på forhånd har en it-beredskabsplan, kan skabelonen benyttes.

## *Miljøstyrelsens DCIS-strategi: Initiativ 2 – It-beredskabsplan*

En nedskrevet og operationel it-beredskabsplan er et vigtigt element i arbejdet med cyber- og informationssikkerhed. En it-beredskabsplan skal bidrage til at sikre, at forsyningen ved, hvordan en hændelse håndteres. En it-beredskabsplan er en del-beredskabsplan og fungerer som en underliggende beredskabsplan til forsyningens overordnede beredskabsplan.

En it-beredskabsplan sikrer, at forsyningens ledelse og medarbejdere ved hvilke roller, ansvar og handlinger der er relevante i tilfælde af en hændelse.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

Indholdsfortegnelse

[*Indledning* 2](#_Toc167950546)

[*Læsevejledning* 2](#_Toc167950547)

[*Miljøstyrelsens DCIS-strategi: Initiativ 2 – It-beredskabsplan* 2](#_Toc167950548)

[1. Introduktion og formål 4](#_Toc167950549)

[2. Operationel planlægning 4](#_Toc167950550)

[3. Beredskabsorganisation 4](#_Toc167950551)

[3.1. Beredskabsorganisationens struktur 5](#_Toc167950552)

[4. Aktivering af it-beredskabsplanen 7](#_Toc167950553)

[4.1. Kontaktliste 8](#_Toc167950554)

[4.2. Mødested 8](#_Toc167950555)

[5. Action cards 9](#_Toc167950556)

[6. Vedligeholdelse af beredskabsplan 9](#_Toc167950557)

[6.1. Test 9](#_Toc167950558)

[6.1.2 Testhistorik 10](#_Toc167950559)

[6.1.3 Udeståender 10](#_Toc167950560)

[6.2 Opdatering af planer 10](#_Toc167950561)

[6.2.1 Versionshistorik 10](#_Toc167950562)

[6.3. Distribution og opbevaring 11](#_Toc167950563)

[7. Bilag/action cards 12](#_Toc167950564)

[7.1. Kontaktlister 12](#_Toc167950565)

[7.2. Systemoverblik 13](#_Toc167950566)

[7.3. Eskaleringsproces 13](#_Toc167950567)

[7.4. Kommunikationstjekliste 15](#_Toc167950568)

[7.5. Leverandørsamarbejde 16](#_Toc167950569)

[7.6. LAN-reetablering 17](#_Toc167950570)

[7.7. Virus- og hackerangreb 18](#_Toc167950571)

[7.8. Server-reetablering 19](#_Toc167950572)

[7.9. Hændelseslog 20](#_Toc167950573)

[7.10. Mailskabelon: Orientering til relevante interessenter og myndigheder 21](#_Toc167950574)

1. Introduktion og formål   
*Her introduceres beredskabsplanen kort. I dette afsnit kan der tilføjes en beskrivelse af væsentlige forudsætninger for beredskabsplanen fx hvis udvalgte systemer/processer ikke er omfattet af denne beredskabsplan, henvisninger til andre beredskabsplaner i forsyningen eller hvis it-drift primært varetages af en leverandør.*

It-beredskabet i [*FORSYNINGEN*] og de tilhørende action cards er etableret på baggrund af risikovurderinger og det generelle trusselsbillede. Beredskabsplanen beskriver de operationelle tiltag og handlinger, som er relevante i en beredskabssituation.

I en beredskabssituation skal der først og fremmest tages udgangspunkt i de operationelle action cards. Overblik over action cards kan findes i afsnit 5, mens de enkelte action cards kan findes i bilag 7.3.-7.8.

# 2. Operationel planlægning

*Dette afsnit udgør første skridt for forsyningen, så forsyningen kan træffe beslutning om aktivering af beredskabet, reetableringsrækkefølgen samt hvilke systemer, der er de mest kritiske. Dette stiller krav til forsyningen om at have identificeret de kritiske it-systemer. Med i overvejelserne kan desuden være muligheden for at anvende alternative procedurer til it-understøttelsen (fx ø-drift), geografiske forskelle, forsyningsart eller dialog med leverandøren.*

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

For at sikre at beredskabsplanen opfylder forretningens behov, er det vigtigt at have forholdt sig til tidsmæssige målsætninger for reetablering, hvilket betyder, hvor længe [*FORSYNINGEN*] maksimalt kan have systemet ude af drift. I bilag 7.2. findes en systemliste hvori relevante informationer såsom kritikalitet, kontaktpersoner, forsyningsart mm. fremgår.

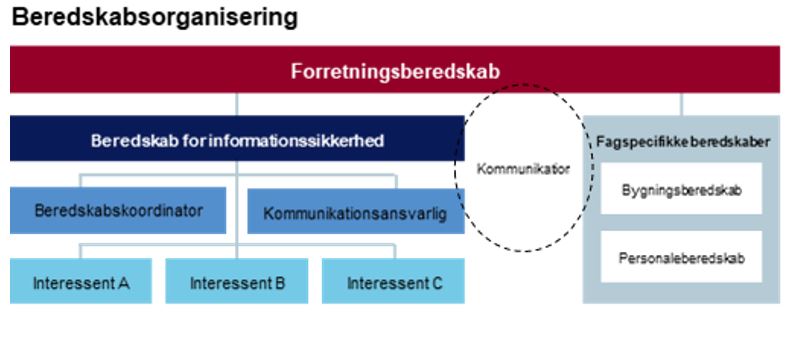
# 3. Beredskabsorganisation

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

*Størrelsen af beredskabsorganisationen afhænger af organisationens it-anvendelse og omfanget af opgaver i forbindelse med it-driften, som varetages internt i organisationen. Hvis organisationen selv varetager driften af en stor mængde it-systemer, vil der være behov for en tilsvarende stor beredskabsorganisation. Det bør fremgå eksplicit, hvis (og i så fald hvilke) leverandører varetager opgaver i forbindelse med beredskabssituation.*

I dette afsnit beskrives den organisation og bemanding, som skal mobiliseres i en beredskabssituation, og som skal sikre, at en hændelse håndteres.

*Såfremt det er relevant, kan der her indsættes et organisationsgram over beredskabsorganisationen i forsyningen. Nedenfor findes et eksempel på et organisationsdiagram for en beredskabsorganisation fra Sikkerdigital.dk.*



## 

## 3.1. Beredskabsorganisationens struktur

*Rollerne nedenfor er den type roller, der typisk indgår i håndteringen af en beredskabssituation. Der skal i udarbejdelsen af roller lægges vægt på, hvilke roller der er relevante i den enkelte forsynings kontekst. I forbindelse med udarbejdelse af rollerne skal det vurderes, i hvilket omfang, der er behov og mulighed for at anvende stedfortrædere/substitutter. Stedfortrædere/substitutter angives i den efterfølgende kontaktliste.*

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 [*FORSYNINGEN*].

| **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, it-ledelsen samt ledere af berørte og relevante forretningsområder. Formanden er den til enhver tid øverst rangerende chef, som der først opnås kontakt til i tilfælde af en hændelse. Den chef, der først opnås kontakt til, kan dog delegere formandsposten til en anden chef.* |
| It-chef | *It-chefen ejer beredskabsplanen. It-chefen varetager endvidere en række specifikke opgaver i en krisesituation: Ledelse af retableringsaktiviteter, rapportering til beredskabsledelsen, intern kommunikation. It-chefen nedsætter relevante reetableringsteams.*  *Overvej om denne er relevant, hvis al it-drift er outsourcet. Forsyningsselskabets ledelse vil altid være øverste ansvarlige for cybersikkerheden og evt. manglende forsyning, men hvis leverandører varetager kritiske elementer skal deres rolle og tilhørende forpligtelser defineres i en den aftale/kontrakt, forsyningen har med leverandøren.* |
| It-beredskabskoordinator | *It-beredskabskoordinatoren opretter og vedligeholder hændelsesloggen, bistår ledelsen og sikrer koordinering af de enkelte aktiviteter.*  *Koordinatoren kan være organisationens it-sikkerhedskoordinator eller en person med stort indblik i organisationen, fx medlem af direktionssekretariatet.* |
| Kommunikationsansvarlig | *Den kommunikationsansvarlige varetager ekstern kommunikation med fx kunder, myndigheder (herunder DCIS-Vand), offentlighed og presse.*  *Organisationens eksterne interessenter skal informeres om situationen og de løbende fremskridt. Den kommunikationsansvarlige bør have kommunikative færdigheder og erfaring.* |
|  |  |
| Leverandørens roller/ad hoc/internt | *Hvis der er aftalt særlige roller med leverandøren, bør disse beskrives her. Det kan f.eks. være kontaktpersoner, koordinatorer mv. Det kan også være virksomheder, som hjælper med at afdække og håndtere hændelsen eller den interne økonomiafdeling til disponering af ressourcer.* |

# 4. Aktivering af it-beredskabsplanen

*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 skal 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 action cards benyttes, fx kommunikationsplanen af hensyn til håndtering af interessenter eller kommunikation med myndigheder. En væsentlig del af aktiveringen og styringen/ledelsen vil i en sådan situation bestå i at afgrænse indsatsen i forhold til planernes fulde omfang.*

It-beredskabet træder i kraft, når en hændelse ikke kan håndteres inden for rammerne af [*FORSYNINGENS*] normale processer og arbejdsgange. Selv hvis en hændelse ikke medfører aktivering af it-beredskabet, vil [*FORSYNINGEN*] i de tilfælde, hvor der er tale om et forsøg på at få uautoriseret adgang til computersystemer med den konsekvens, at der opstår en væsentlig trussel mod forsyningssikkerheden, fortsat orientere DCIS-Vand om hændelsen vha. af skabelonen i bilag 7.10.

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 seks kriterier (a til f) er opfyldt,
  + eller hvis flere kriterier vurderes i risiko for at blive opfyldt.

1. **Tidsmæssig udstrækning af hændelsen**

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

1. **Større datatab**

Såfremt det står klart, at der efter en hændelse er risiko for datatab, 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, 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.

1. **Særlige hændelser**

Særlige hændelser såsom:

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

1. **Ukendt årsag**

Hvis årsagen til hændelsen er ukendt, kan det være en indikation af en hændelse, der kræver aktivering af beredskabsplanen.

1. **Kriterier for kritiske systemer**

Hvis de tidsmæssige målsætninger (bilag 7.2.) for de meste kritiske systemer i forsyningen er i fare for at bliver overskredet, kan det være en indikation af en hændelse, der kræver aktivering af beredskabsplanen.

## 4.1. Kontaktliste

Kontaktlisterne er udgangspunktet for mobilisering af beredskabsorganisationen, men kan også anvendes i forhold til den øvrige interne og eksterne kommunikation. Herunder findes kontaktoplysninger på medlemmer af beredskabsorganisationen i [*FORSYNING*]:

Kontaktlisten nedenfor skal afspejle beredskabsorganisationen i afsnit 3.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Kontaktliste for beredskabsorganisation** | | | | | |
| Rolle | Primær/substitut | Navn | Adresse | E-mail | Tlf. | Alternativ tlf. og e-mail |
| *It-beredskabskoordinator* | Primær | Anders Andersen | Andersvej 1, Anders | XX | XX | XX |
| Substitut | XX | XX | XX | XX | XX |
| *It-chef* | Primær | XX | XX | XX | XX | XX |
| Substitut | XX | XX | XX | XX | XX |
| *Kommunikationsansvarlig* | Primær | XX | XX | XX | XX | XX |
| Substitut | XX | XX | XX | XX | XX |

Øvrige kontaktlister kan findes i bilag 7.1.

## 4.2. Mødested

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

# 5. Action cards

*Forsyningen kan anvende action cards til at assistere i en beredskabssituation. Action cards kan anvendes som tjeklister til, hvordan en hændelse håndteres. De oplistede action cards er ikke udtømmende og skal tilpasses den enkelte forsynings kontekst, hvorfor det ligeledes bør overvejes, om der er behov for andre action cards end de allerede oplistede.*

Beredskabsorganisationen anvender operationelle action cards, som tages i brug i en beredskabssituation. Formålet med action cards er at assistere beredskabsorganisationen med at huske de procedurer, som skal udføres i en beredskabssituation. Action cards findes i bilag 7.3.-7.9. Herunder findes et samlet overblik over action cards:

Eskaleringsproces  
(bilag 7.3)

Kommunikationstjekliste  
(bilag 7.4)

Leverandørsamarbejde  
(bilag 7.5)

LAN-retablering  
(bilag 7.6)

Server-reetablering  
(bilag 7.8)

Virus- og hackerangreb  
(bilag 7.7)

Action cards er udformet som tjeklister og kan derfor også bruges som forløbsjournal. Som et alternativ kan det tomme hændelseslog-ark i bilag 7.9. anvendes.

# 6. Vedligeholdelse af beredskabsplan

## 6.1. 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. I nedenstående skema er det beskrevet, hvilke typer tests der foretages med hvilken frekvens.

| **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 action cards, hvor et eller flere systemer retableres med udgangspunkt i retableringsplaner.* |

### 6.1.2. Testhistorik

I nedenstående tabel er beredskabets tests og afprøvninger noteret.

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

### 6.1.3. 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.*

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

## 6.2. 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.

### 6.2.1. 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* |

## 6.3. 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 (it-chefen jf. afsnit 3.1) er ansvarlig for distribution af opdateringer til alle modtagere af planen.

|  |  |  |  |
| --- | --- | --- | --- |
| **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* | *2 kopier i aflåst skab – nøgle hos NN* |

# 7. Bilag/action cards

## Kontaktlister

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Kontaktliste for beredskabsorganisation** | | | | | |
| Rolle | Primær/substitut | Navn | Adresse | E-mail | Tlf. | Alternativ tlf. og e-mail |
| *It-beredskabskoordinator* | Primær |  |  |  |  |  |
| Substitut |  |  |  |  |  |
| *It-chef* | Primær |  |  |  |  |  |
| Substitut |  |  |  |  |  |
| *Indsæt roller i overensstemmelse med afsnit 3.1* |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Kontaktliste for forretning** | | | | | |
| Forretningsområde | Primær/substitut | Navn | Adresse | E-mail | Tlf. | Alternativ tlf. og e-mail |
| *Driftsleder - 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 |  |  |  |  |  |
|  |  |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Kontaktliste for eksterne kontakter** | | | |
| Rolle | Primær/substitut | Navn | E-mail | Tlf. |
| *CFCS’ situationscenter* | Primær | Vagt | cfcs@cert.cfcs.dk | 33325580 |
| *DCIS-Vand* | Primær | Vagt (mandag-fredag kl. 8-16) | dcis@mst.dk | 61369725 |
| *Indsæt andre roller (fx kommune, brancheorganisation, Datatilsynet eller lign.)* |  |  |  |  |

## Systemoverblik

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Prioritet** | **Systemnavn** | **Kritikalitet** | **Forsyningsart/anlæg** | **Tidsmæssig målsætning** | **Kontaktperson hos leverandør** | **Interne superbrugere** |
| 1 | *System A* | *A* |  | *2 timer* |  |  |
| 2 | *System B* | *B* |  | *12 timer* |  |  |
| 3 | *System C* | *A* |  | *5 timer* |  |  |
| 4 | *System D* | *A* |  | *1 dag* |  |  |
| 5 | *System E* | *B* |  | *3 dage* |  |  |

## Eskaleringsproces

*Sørg for at opdatere hændelsesloggen (bilag 7.9) løbende.*

| **Nr.** | **Handling** | **Ansvar** | **Tid** |
| --- | --- | --- | --- |
| 1 | **Modtag notifikation**  Når en notifikation om en potentiel hændelse modtages, skal følgende oplysninger forsøges fremskaffet:   * Typen af hændelsen * Eventuelle tilskadekomne personer * Omfanget af skaden * Hvilke eksterne leverandører er involveret | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 1.1 | **Start hændelseslog**  Brug kolonne i nærværende tabel, eller anvend tom skabelon i bilag 7.9. | Modtager af notifikation | Start:  Slut: |
| 2 | **Bekræft notifikation**  Få notifikationen bekræftet hvis nødvendigt. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 3 | **Indledende vurdering af omfang**  Foretag en indledende vurdering af skadesomfanget. Skade på informationssystemer vurderes af it-chefen eller it-beredskabskoordinatoren, evt. understøttet af leverandører, som har driftsansvaret på dele af systemporteføljen. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 3.1 | **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 7.1. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 4 | **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 4, om it-beredskabet skal aktiveres.  Driftsleverandører varsles om mulig beredskabssituation. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 5 | **Aktivering af it-beredskab**  Aktiver it-beredskabet. Beslutningen om at aktivere it-beredskabet skal kommunikeres til beredskabsorganisationen. Informer om kendte udeståender jf. afsnit 6.1.3. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 6 | **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 3.1 | Start:  Slut: |
| 7 | **Information til interessenter**  Øvrige relevante interessenter informeres om it-beredskabet. Anvend evt. mailskabelon i bilag 7.10. til at informere relevante interessenter. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 8 | **Fastlæg omfanget af skaden**  Foretag en nærmere registrering af de berørte it-systemer. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 8.1 | **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. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |

## Kommunikationstjekliste

*Sørg for at opdatere hændelsesloggen (bilag 7.9) løbende.*

| **Nr.** | **Handling** | **Ansvar** | **Tid** |
| --- | --- | --- | --- |
| 1 | **Udarbejd tidsplan**  Der udarbejdes en tidsplan for ekstern og intern kommunikation. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 2 | **Indsaml information**  Al information, som er påkrævet for intern og ekstern kommunikation, samles hos den kommunikationsansvarlige. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 3 | **Beslut kommunikationskanal**  For hver enkel intern og ekstern kommunikation fastlægges kommunikationskanalen. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 4 | **Udarbejd eksterne meddelelser**  Udarbejd meddelelser til ekstern kommunikation, og få disse godkendt af beredskabsledelsen. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 5 | **Oversæt relevant dokumentation**  Hvis der er behov for at vedlægge dokumentation, foretages eventuelt oversættelse heraf. | Fastlægges jf. afsnit 3.1 | 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 3.1 | Start:  Slut: |
| 7 | **Responder på spørgsmål**  Svar på eventuelle spørgsmål med fokus på de mest kritiske spørgsmål og interessenter. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |

## Leverandørsamarbejde

*Sørg for at opdatere hændelsesloggen (bilag 7.9) løbende.*

| **Nr.** | **Handling** | **Ansvar** | **Tid** |
| --- | --- | --- | --- |
| 1 | **Undersøg leverandørforhold**  Det undersøges, hvilke opgaver som er outsourcet til en ekstern leverandør. Anvend gerne systemoverblik i bilag 7.2. | Fastlægges jf. afsnit 3.1 | 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 7.1. | Fastlægges jf. afsnit 3.1 | 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 3.1 | 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 3.1 | 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 3.1 | Start:  Slut: |

## LAN-reetablering

*Sørg for at opdatere hændelsesloggen (bilag 7.9) løbende.*

|  |  |  |  |
| --- | --- | --- | --- |
| 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 3.1 | Start:  Slut: |
| 2 | **Kontakt eventuelle leverandører**  Kontakt leverandøren og vurder situationen. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 3 | **Iværksæt undersøgelse af årsagen til nedbruddet**  Assister leverandøren med at identificere årsagen til nedbruddet. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 4 | **Planlæg retableringen**  Planlæg hvordan der retableres. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 5 | **Foretag retablering**  Foretag den planlagte retablering, f.eks. udskiftning af defekt hardware. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 6 | **Informer it-beredskabskoordinator**  Informer it-beredskabskoordinatoren og kommuniker til øvrige interessenter. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |

## Virus- og hackerangreb

*Sørg for at opdatere hændelsesloggen (bilag 7.9) løbende.*

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | **Handling** | Ansvar | Tid |
| 1 | **Vurder situationen**  Vurder situationen. Hvis der er risiko for, at data kan blive kompromitteret, afbrydes internetforbindelsen. | Fastlægges jf. afsnit 3.1 | 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 3.1 | Start:  Slut: |
| 3 | **Iværksæt undersøgelse**  Iværksæt en undersøgelse af angrebet. Undersøgelsen skal bl.a. skabe en tidslinje over hændelsen fra de første IoC’er (Indicators of Compromise) til recovery. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 4 | **Skift adgangskoder**  Det vurderes, om adgangskoder bør skiftes. | Fastlægges jf. afsnit 3.1 | 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 3.1 | Start:  Slut: |
| 6 | **Kontakt leverandører**  Hvis de ramte områder driftes eksternt, kontakt leverandørerne. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 7 | **Kontakt myndigheder**  Det skal vurderes, om der skal foretages politianmeldelse, og om der er andre myndigheder, som bør kontaktes, herunder DCIS-Vand | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 8 | **Informer interessenter**  Eventuelle øvrige interessenter informeres. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |

## Server-reetablering

*Sørg for at opdatere hændelsesloggen (bilag 7.9) løbende.*

| **Nr.** | **Handling** | **Ansvar** | **Tid** |
| --- | --- | --- | --- |
| 1 | **Anskaf og installer backup**  Fremskaf backup og installer denne i udviklingsmiljøet. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 2 | **Fastlæg datatab og informer brugere**  Fastlæg omfanget af datatabet og informer brugerne om, hvor stort et tidsrum, der mangler i systemet. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 3 | **Ret Server Entry**  Tilret udviklingsmiljøet, så dette nu er produktionsmiljø. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 4 | **Implementer almindelige driftskontroller**  Implementer de almindelige driftskontroller og konfigurationer såsom backup, overvågning mv. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |
| 5 | **Informer it-beredskabskoordinator**  Informer it-beredskabskoordinatoren når systemet er retableret. | Fastlægges jf. afsnit 3.1 | Start:  Slut: |

## Hændelseslog

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

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

## 

## Mailskabelon: Orientering til relevante interessenter og myndigheder

Orientering vedrørende cyberhændelse i [*FORSYNING*] [*xx.xx.2024*]

**Til:** [*DCIS-Vand*]

**Cc:** [*Fx brancheorganisationer, kommune eller lignende*]

[*FORSYNINGEN*] er udsat for en cyberhændelse. Der er tale om [*indsæt angrebstype, hvis kendt*]. Den sårbarhed, der er blevet udnyttet i forbindelse med cyberhændelsen, er relateret til [*indsæt udstyr og produktserie*]. Sårbarheden gør det muligt at [*indsæt beskrivelse*].

**Status**

Status er, at [*indsæt beskrivelse, herunder om hvilke initiativer, der er sat i gang og hvornår problemet forventes løst, hvis kendt*]. Vi følger situationen og vil sende yderligere information, hvis vi bliver bekendt med nye og relevante informationer.