**Vejledning til anvendelse   
af Wired Relations’ skabeloner**A black background with black lines

Description automatically generated

Wired Relations’ skabeloner\* kan anvendes direkte i jeres arbejde med databeskyttelse og informationssikkerhed – men kan selvfølgelig også anvendes som inspiration til jeres eget materiale. I kan ændre efter behov, så det bliver præcis, som I ønsker det.

**OBS!** Der kan være afsnit, som ikke er relevante for alle virksomheder. Hvis dette er tilfældet, vil det tydeligt fremgå af teksten.

Der vil være steder i teksten, hvor der er lagt op til, at I indsætter virksomhedens navn eller andet. Dette vil i så fald være markeret jf. følgende: [*indsæt virksomhedens navn*].

|  | Tekstboksene i dokumentet indeholder opmærksomhedspunkter og gode råd. Vær opmærksom på, at tekstboksene bør fjernes fra den endelige udgave af den konkrete politik eller procedure. |  |
| --- | --- | --- |

I bunden af hver skabelon vil der fremgå en tabel, som giver et overblik over dokumentets version, seneste opdatering, samt hvem der har ansvaret for dokumentet.

|  | Her er nogle ekstra tips til brug af Wired Relations' skabeloner: |  |
| --- | --- | --- |
|  | * I kan tilføje eller fjerne sektioner, ændre ordlyd og tilføje virksomhedens eget logo og branding. |  |
|  | * Hold skabelonerne opdaterede. Krav til databeskyttelse og informationssikkerhed ændrer sig konstant, så det er vigtigt at sikre, at skabelonerne altid er opdaterede. |  |

**It-beredskabsplan**

**1. Formål**

It-beredskabsplanen skal sikre, at de it-afhængige forretningskritiske processer i [*indsæt virksomhedens navn*] kan reetableres på betryggende vis efter at en kritisk hændelse direkte eller indirekte har forhindret normal drift.

Selve it-beredskabsplanen indeholder rollebeskrivelser, instrukser og procedurer, som skal følges, såfremt beredskabet bliver aktiveret. Dette sikrer en klar ansvars- og rollefordeling, således at ansvarlige personer ved, hvad der skal gøres i en beredskabssituation.

**2. Afgrænsning**

It-beredskabsplanen omfatter it-anvendelsen hos [*indsæt virksomhedens navn*] på følgende lokalitet(er): *[Indsæt virksomhedens lokalitet(er)]*.

Hvis it-anvendelsen hos [*indsæt virksomhedens navn]*  helt eller delvist købes som en serviceydelse hos en 3. part i en outsourcingaftale, herunder også cloudløsninger, så skal [*indsæt virksomhedens navn]*  sikre sig, at der er aftalt og implementeret passende sikkerhedsforanstaltninger hos leverandøren i forhold til reetablering.

**3. Planlægning**

3.1 Målsætninger

[*Indsæt virksomhedens navn]* har fastsat tidsmæssige mål for reetablering af forretningskritiske It-services, som er omfattet af denne it-beredskabsplan, betegnet Recovery Time Objective (RTO). Systemlisten er ajourført og bliver løbende vedligeholdt i *[fx Wired Relations - alternativt kan systemlisten indsættes som tabel nedenfor eller i et bilag]* med angivelse af RTO (og evt. andre relevante kriterier) for det enkelte system.

|  | En forudsætning for at kunne fastsætte RTO-mål er, at kritiske it-systemer er identificeret, og at der har været en dialog med virksomhedens forskellige afdelinger/repræsentanter om, hvor længe it-understøttelsen kan undværes. Dette dialog finder typisk sted i forbindelse med gennemførelse af de løbende risikovurderinger.  RTO-målene afspejler de forretningsmæssige krav, som skal ses i lyset af det sikkerhedsniveau organisationen har besluttet, implementerede sikkerhedsforanstaltninger og beredskabsplanens operationelle processer.  Ved fastlæggelse af RTO-mål indgår bl.a. overvejelser om, hvorvidt der er mulighed for at anvende alternative procedurer til It-understøttelsen (f.eks. manuelle arbejdsgange) og hvilke aktuelle forebyggende foranstaltninger, der er implementeret i kritiske it-systemer for forbygge nedbrud (øge modstandsdygtigheden). |  |
| --- | --- | --- |

Reetablering er sket, når de enkelte services er tilgængelige for brugerne, og det er muligt at opretholde daglig It-driftsunderstøttelse af virksomheden.

3.2 Beredskabets præmisser

For systemer, der er omfattet af it-beredskabsplanen, skal nedenstående punkter være udført og opdateret:

* Backup på diske (diskbackup), herunder licensnøgler mm.
* Kopi af de tekniske systembeskrivelser
* Administratorpasswords og andre vigtige brugernavne og passwords.
* Kopi af driftsinstruktioner

*[Indsæt evt. flere relevante punkter, såsom*

* *Kopi af it-leverandøraftaler / driftsaftaler*
* *Kopi af liste med prioritering af systemer (Hvilke systemer der skal genetableres først)]*

*[Beskriv hvor ovenstående er opbevaret, fx i brandsikret skab i en anden brandzone end it-systemerne og/eller på en ekstern sikker lokalitet].*

|  | Hensigten er at disse information altid skal være tilgængelig, selv hvis de elektroniske versioner ikke er det. Man bør i videst muligt omfang opbevare en sådan kopi uden for virksomhedens primære kontor/lokalitet. Husk at disse informationer er fortrolige og derfor skal beskyttes og adgangsstyres. |  |
| --- | --- | --- |

3.3. Aktivering af it-beredskabet

It-beredskabet aktiveres, når en hændelse ikke kan håndteres inden for rammerne af *[indsæt virksomhedens navn]* normale processer og arbejdsgange.

Beredskabet skal aktiveres, når *[Definér kriterierne for, hvornår it-beredskabet skal aktiveres]*

|  | Det er altid en konkret vurdering, hvorvidt it-beredskabet skal aktiveres, men typisk vil følgende kriterier kunne anses som pejlemærker, f.eks. hvis ét af følgende kriterier er opfyldt eller hvis flere kriterier vurderes at være i risiko for at blive opfyldt.  Inspiration til fastlæggelse af kriterier:   * **Tidsmæssig udstrækning af hændelse**   + Hvis der er risiko for at en hændelse ikke kan håndteres og løses inden for de ramte aktivers Recovery Time Objective (RTO), er der tale om en krise, hvor it-beredskabet skal aktiveres * **Større datatab**   + Hvis en hændelse har en sådan karakter, at der kan opstå større datatab end virksomhedens tabstolerance, kan det være indikation af en krise, der kræver iværksættelse af it-beredskabet. * **Graden af påvirkning**   + Hvis en større del af virksomhedens it-infrastruktur er berørt af en hændelse, kan det indikere en krise, der kræver aktivering af it-beredskabet. * **Særlige hændelser**   + Naturkatastrofer (jordskælv, oversvømmelse mv.) kan kræve aktivering af it-beredskabet   Det er væsentligt, at det er kommunikeret til medarbejderne, hvilken rapporteringskanal, der skal anvendes i tilfælde af, at der er konstateret en hændelse (eller at der er mistanke om det). |  |
| --- | --- | --- |

**4. Beredskabsorganisationen**

|  | I små virksomheder kan alle rollerne være samlet i “Direktøren”. I mellemstore virksomheder kan rollerne være fordelt ud på forskellige personer, f.eks. en koordinator, it-chef, kommunikationsansvarlig mv.  Forskellige roller og ansvar som kan indgå i en beredskabsorganisationen er beskrevet i nedenstående tabel.  **Denne tabel skal tilpasses til virksomhedens konkrete situation og organisering.** |
| --- | --- |

4.1. Roller og ansvar

Roller og ansvar/opgaver i beredskabsorganisationen er beskrevet herunder for at præcisere og synliggøre, hvilke opgaver hver rolle har i en beredskabssituation.

| **Rolle** | **Opgaver** |
| --- | --- |
| It-beredskabsledelse | *[Eksempel på beskrivelse: It-beredskabsledelsen er øverste instans i forhold til alle beslutninger, der vedrører den operationelle håndtering af en beredskabsmæssig krise. It-beredskabsledelsen fungerer som forum for drøftelse af væsentlige ledelsesmæssige beslutninger vedrørende den operationelle håndtering af den beredskabsmæssige krise.]* |
| It-beredskabs-  koordinator | *[Eksempel på beskrivelse: It-beredskabskoordinatoren opretter og vedligeholder hændelsesloggen, bistår ledelsen og sikrer koordinering af de enkelte aktiviteter.]* |
| Kommunikations-  ansvarlig | *[Eksempel på beskrivelse: Virksomhedens eksterne interessenter skal informeres om situationen og de løbende fremskridt. Beskriv evt. hvem virksomhedens interessenter er, f.eks. medarbejdere, kunder, samarbejdspartnere].* |
| Reetableringsteams | *[Reetableringsteams er teknisk orienterede medarbejdere, som forestår reetablering af it-systemerne i henhold til de operationelle planer og detailplanerne, og desuden har ansvar for at sikre, at forløbet dokumenteres i hændelsesjournaler]* |
| Leverandørens roller | *[Hvis der er aftalt særlige roller med leverandøren, bør disse beskrives her, det kan f.eks. være kontaktpersoner hos leverandøren]* |

Nedenfor findes kontaktlisten på beredskabsorganisationen, men også den øvrige del af virksomheden, som kan tænkes at blive involveret.

4.2 Kontaktlister

| **Kontaktliste for beredskabsorganisationen** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Rolle** | **Stilling** | **Navn** | **Adresse** | **Email / Tlf** | |
| *It-beredskabsledelsen* | *fx CEO* |  |  |  | |
|  | *fx IT-chef* |  |  |  | |
|  | *fx DPO* |  |  |  | |
|  |  |  |  |  | |
|  |  |  |  |  | |
| *It-beredskabs-*  *koordinator* | *fx Informations-*  *sikkerheds-*  *koordinator* |  |  |  | |
| *Kommunikationsansvarlig* | *fx Pressechef* |  |  |  | |
|  |  |  |  |  | |

| **Kontaktliste for øvrig del af virksomheden** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Rolle** | **Stilling** | **Navn** | **Adresse** | **Email / Tlf** | |
| *Afdeling A* | *fx kontorchef* |  |  |  | |
| *Afdeling B* | *fx kontorchef* |  |  |  | |
|  |  |  |  |  | |
|  |  |  |  |  | |

| **Kontaktliste for leverandører** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Rolle** | **Stilling** | **Navn** | **Adresse** | **Email / Tlf** | |
| *Driftsleverandør A* | *[indsæt]* |  |  |  | |
| *Driftsleverandør B* | *[indsæt]* |  |  |  | |
| *Netværksleverandør* | *[indsæt]* |  |  |  | |
|  |  |  |  |  | |

4.3 Mødested for beredskabsorganisationen

Hvis det ikke er muligt for beredskabsorganisationen at mødes på virksomhedens normale lokation *[indsæt mødested på virksomhedens lokation]*, når beredskabsplanen bliver aktiveret, er der aftalt et alternativt mødested.

*[Indsæt alternativt mødested].*

**5. Alarmering og vurdering**

Al alarmering inden for normal arbejdstid sker til *[Indsæt relevant kontaktpunkt],* som vurderer alvorligheden af det opståede problem.

Kontaktnummer: xxxx xxxx

(Se også kontaktinformationer i pkt. 4.2)

Ved skader på de fysiske rammer, kontaktes *[Indsæt relevant kontaktpunkt]*

inden for normal arbejdstid. Den bygningsansvarlige orienteres herefter, og træffer den endelige beslutning.

Al alarmering om alvorlige hændelser uden for normal arbejdstid sker til *[Indsæt relevant kontaktpunkt]*, som herefter vurderer problemets omfang.

Alarmering om en alvorlig hændelse skal sendes videre til *[indsæt ansvarligt kontaktpunkt, fx it-beredskabsledelsen, jf. pkt. 4.1]*, som træffer den endelige beslutning om aktivering af beredskabet.

5.1. Vurdering

*[indsæt ansvarligt kontaktpunkt, fx it-beredskabsledelsen, jf. pkt. 4.1]* vurderer situationen og undersøger internt (eller hos leverandøren), hvor lang tid, der skal bruges på at reetablere skaderne, og bestemmer ud fra kriterierne, jf. pkt. 3.3. om it-beredskabet skal aktiveres.

Driftsleverandører varsles om en mulig beredskabssituation.

**6. Vedligeholdelse af it-beredskabsplanen**

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.

*[Beskriv, hvordan I tester it-beredskabsplanen].*

|  | Det bør ud fra en konkret vurdering fastsættes, hvilken testtype og omfang der er nødvendig.  Et eksempel kan være, at lave en skrivebordstest én gang årligt. Denne test foretages ud fra et foruddefineret scenarie. Ved en skrivebordstest afprøves dele af it-beredskabsplanen f.eks. eskaleringsprocessen og at kontaktlister er korrekte. Ved en skrivebordstest foretages der ikke afbrydelser i it-driften.  Udover en skrivebordstest kan man også udføre en fuld test på en eller flere handlingsplaner, hvor et eller flere systemer reetableres. Dette kan f.eks. foretages hvert andet eller tredje år.  Hvis der konstateres mangler/udeståender i forbindelse med test af it-beredskabsplanen og i perioden mellem konstatering og udbedring, er det væsentligt at den pågældende mangel/udeståender fremgår af it-beredskabsplanen, da det kan have afgørende betydning for beredskabsorganisationen under en eventuel hændelse. Mangler/udeståender kan med fordel fremgå af fx bilag til it-beredskabsplanen. |
| --- | --- |

Alle tests af it-beredskabsplanen dokumenteres, herunder eventuelle fundne udeståender og plan for udbedring/opdatering.

6.2 Opdatering af It-beredskabsplanen

Opdatering af It-beredskabsplanen skal ske mindst en gang om året i forlængelse af den årlige test af it-beredskabsplanen. It-beredskabsplanen bør også opdateres, hvis der sker væsentlige ændringer i anvendelsen af it, leverandørskifte, omstruktureringer eller ændringer i beredskabsorganisationen.

6.3 Udlevering og opbevaring

It-beredskabsplanen skal opbevares, så den altid er tilgængelig i en beredskabssituation, hvilket betyder, at det ikke er tilstrækkeligt at opbevare den elektronisk. Hvert medlem af beredskabsorganisationen bør opbevare et fysisk eksemplar af planen. Den der er ansvarlig for at vedligeholde it-beredskabsplanen er samtidig ansvarlig for at udlevering af senest opdaterede version til alle modtagere.

Overblik over udleverede kopier kan vedligeholdes nedenfor:

| **Modtager** | **Rolle** | **Lokation/opbevaring** | **Bemærkninger** |
| --- | --- | --- | --- |
| *Navn* | *Fx CEO* | *[Indsæt adresse og placering]* | *[Fx opbevares fysisk]* |
|  |  |  |  |
|  |  |  |  |

**7. Konkrete handleplaner**

Handleplaner skal assistere beredskabsorganisationen i at håndtere en konkret hændelse, herunder at huske alle de procedurer og punkter, som skal udføres i tilfælde af at beredskabet aktiveres.

Hændelsesforløbet dokumenteres i hændelsesloggen (bilag 6)

Handleplanerne er udelukkende et understøttende redskab, og det er vigtigt, at beredskabsorganisationen altid vurderer den konkrete situation og iværksætter de nødvendige tiltag.

De konkrete handleplaner findes i bilag 1-5. En skabelon til hændelsesloggen findes i bilag 6.

|  | Eksempler på konkrete handleplaner fremgår af bilag 1-5 nedenfor. De skal tilrettes til den konkrete virksomhed.  Der kan være behov for yderligere handlingsplaner, f.eks:   * Plan for ny lokation (skal sikre en hurtig og effektiv overgang til ny lokation) * Plan for reetablering af hardware (skal understøtte processen i at fremskaffe nyt udstyr til at reetablere it-driften). * Plan for reetablering af netværk (Skal sikre at adgang til netværk genoprettes i tilstrækkeligt omfang)   Der kan også være behov for at udarbejde tjeklister, fx tjekliste for normaliseret drift. |
| --- | --- |

**Bilag 1 - Fysiske hændelser, der sætter kontoret ud af drift (EKSEMPEL)**

**Beskrivelse:**

Handleplanen beskriver det fysiske beredskab og it-beredskab, der skal etableres hvis *[Indsæt virksomhedens navn]* lokaler bliver helt eller delvist ødelagt, i en sådan grad, at de almindelige processer ikke kan håndtere reetablering af it-driften.

Det kan f.eks. være resultatet af brand, vandskade, eksplosion mv.

**Dokumentation:**

Ved aktivering af beredskabet skal al aktivitet logges til brug for efterfølgende dokumentation - brug hændelsesloggen i bilag 6. Det er også vigtigt at evt. identificerede svagheder/sårbarheder i it-beredskabet eller systemer beskrives. Det evalueres om dette giver anledning til ændringer i systemer eller procedurer.

**Forudsætninger:**

*[Beskriv hvilke forudsætninger, der er gældende for denne handleplan. Der vil oftest være forhold, der er nødvendige for at kunne gennemføre handlingsplanen, fx udstyr, aftaler, fysiske lokationer, logistiske forhold eller kompetencer. Et eksempel kan være “Den basale infrastruktur (telefoni, internet mv.] er tilgængelig”]*

| **Nr.** | **Opgaver / aktioner** | **Ansvar** | |
| --- | --- | --- | --- |
| 1 | Sikre personale, lokaler, udstyr og andre aktiver. Måske skal der tages kontakt til udlejer, eller andre interessenter | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 2 | **Aktiver midlertidig lokation**  Hvis der er behov for at rykke til ny lokation, skal dette aktiveres. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 3 | **Kommunikation**  Alle medarbejdere skal informeres om situationen og det skal afklares, om medarbejdere skal arbejde hjemmefra, indtil den midlertidige lokation er reetableret.  Telefoner skal evt. viderestilles til andre telefoner. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 4 | **Skader på primær lokation skal udbedres** | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 5 | **It-drift reetableres**  Ved reetablering af serverrum skal det afklares, om der kan laves restore af it-systemer på samme udstyr eller om der skal fremskaffes nyt udstyr. *(Evt. skal der udarbejdes særskilt plan for anskaffelse af hardware)* | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 6 | **Kontrol af at primær lokation kan benyttes og at It-drift er reetableret**   * Alt er klar til brug * Netværksforbindelser er genetableret. * De nødvendige systemer og data er tilgængelige * Lokalerne opfylder arbejdsmiljølovens krav inden ibrugtagning. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |

**Bilag 2 - It-hændelser, der påvirker et centralt system (EKSEMPEL)**

**Beskrivelse:**

Handleplanen beskriver det beredskab, der skal etableres, hvis et centralt it-system bliver helt eller delvist utilgængeligt og at driften ikke ser ud til at kunne reetalberes indenfor det pågældende it-systems fastlagte Recovery Time Objective (RTO).

**Dokumentation:**

Ved aktivering af beredskabet skal al aktivitet logges til brug for efterfølgende dokumentation - brug hændelsesloggen i bilag 6. Det er også vigtigt at evt. identificerede svagheder/sårbarheder i it-beredskabet eller systemer beskrives. Det evalueres om dette giver anledning til ændringer i systemer eller procedurer.

**Forudsætninger:**

*[Beskriv hvilke forudsætninger, der er gældende for denne handleplan. Der vil oftest være forhold, der er nødvendige for at kunne gennemføre handlingsplanen, fx udstyr, aftaler, fysiske lokationer, logistiske forhold eller kompetencer. Et eksempel kan være “Den basale infrastruktur (telefoni, internet mv.] er tilgængelig”]*

| **Nr.** | **Opgaver / aktioner** | **Ansvar** | |
| --- | --- | --- | --- |
| 1 | **Aktivering af it-beredskabet**  Relevant personale indkaldes/sammensættes | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 2 | **Luk det berørte system** | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 3 | **Restore**   * Det afklares, om man kan lave en restore af it-systemet på samme udstyr eller om det skal ske på andet udstyr, der i så fald fremskaffes. Evt. kan it-systemmiljøet genetableres i et virtuelt miljø hos en it-leverandør. * Parallelt hermed udarbejdes et tidsestimat for genetablering af normal drift. Estimatet revurderes løbende og dette, samt status, udmeldes til relevante interessenter (ledelsen, medarbejdere, osv.). | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 3.1 | **Aktivér drift**  Ved hjælp af restore aktiveres driften af de berørte systemer herefter, og det tjekkes at:   * Systemerne er klar til drift * Data ikke er ødelagte * Netværksforbindelser er genetableret.   Under arbejdet med at reetablere drift af det berørte system, indsamler it-beredskabsteamet evt. dokumentation for problemet, der måtte være relevant for den efterfølgende vurdering af årsagen til problemet, ud over hvad der allerede findes i logs mv. | *[indsæt ansvarlig, jf. afsnit 4.1]*  *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 4 | **Kommunikation**  Når problemet er udbedret, og alt er klar til drift igen, udmeldes dette til relevante interessenter (ledelsen, medarbejdere, osv.), | *[indsæt ansvarlig, jf. afsnit 4.1]* | |

**Bilag 3 - Virus- og hackerangreb (EKSEMPEL)**

**Beskrivelse:**

Handleplanen beskriver det beredskab, der skal etableres, hvis it-infrastruturen bliver kompromitteret af et virus- eller hackerangreb.

**Dokumentation:**

Ved aktivering af beredskabet skal al aktivitet logges til brug for efterfølgende dokumentation - brug hændelsesloggen i bilag 6. Det er også vigtigt at evt. identificerede svagheder/sårbarheder i it-beredskabet eller systemer beskrives. Det evalueres, om dette giver anledning til ændringer i systemer eller procedurer.

**Forudsætninger:**

*[Beskriv hvilke forudsætninger, der er gældende for denne handleplan. Der vil oftest være forhold, der er nødvendige for at kunne gennemføre handlingsplanen, fx udstyr, aftaler, fysiske lokationer, logistiske forhold eller kompetencer. Et eksempel kan være “Den basale infrastruktur (telefoni, internet mv.] er tilgængelig”]*

| **Nr.** | **Opgaver / aktioner** | **Ansvar** | |
| --- | --- | --- | --- |
| 1 | **Aktivering af it-beredskabet**  Relevant personale indkaldes/sammensættes. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 2 | **Indledende vurdering**  Først laves en vurdering af, om man bør starte med ekstra logning samt sporing (capture af trafik og memory dumps). Dette for at kunne være sikker på,   * 1) hvad der foregår, * 2) få bedre spor af hvem der har skaffet sig adgang samt * 3) for at være sikker på, at der ikke er en logisk bombe.   Derudover vurderes, om det kan være et internt angreb, hvor det kan være aktuelt at isolere en person eller en gruppe fra det videre arbejde.  Hvis det vurderes forsvarligt, isoleres netværk med inficerede systemer, dvs. netværksforbindelsen afbrydes og om muligt sættes virtuelle systemer i pause. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 3 | **Vurdering af omfang**  Der foretages en vurdering af angrebets omfang, herunder om det vil være muligt at reetablere drift på andet udstyr, der i så fald fremskaffes. Evt. kan it-systemmiljøet genetableres i et virtuelt miljø hos en it-leverandør.  Det vurderes også, hvordan it-sikkerheden kan opretholdes eller genoprettes, herunder håndtering af sikkerhed indtil normal drift er genetableret. Hvis det er nødvendigt, kontaktes tele-/internetleverandøren og/eller relevante myndigheder for at få assistance. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 4 | **Tidsestimat for genetablering**  Der udarbejdes et foreløbigt tidsestimat for genetablering af normal drift. Estimatet revurderes løbende og dette, samt status, udmeldes til relevante interessenter (ledelsen, medarbejdere, osv.). | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 5 | **Orientering til interessenter**  Det sikres, at der foretages en passende orientering til relevante eksterne interessenter, herunder orientering af evt. kunder hvis sikkerhed kan være blevet påvirket. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 6 | **Håndtering**  Der foretages vurdering af de inficerede systemer og indsamles eksempler på virussen, angrebsmønstret mv. Såfremt virussen kendes og der findes en eksisterende oprydningsrutine, forsøges virussen fjernet, ellers bruges eksterne antivirus samarbejdspartnere til at afhjælpe infektionen.  Sideløbende foretages gennemgang af logs fra firewall, proxy, systemlogs mv., for at finde frem til infektionskilden. Vurderes det, at infektionskilden kan identificeres som en ekstern kunde/samarbejdspartner, skal denne adviseres om angrebet. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 7 | **Gennemgang af systemer**  Når angrebet er neutraliseret skal alle systemer gennemgås for at tjekke, at:   * Systemerne er klar til drift (overvej backup af systemer inden evt. restore) * Data ikke er ødelagte * Netværksforbindelser er genetableret. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |

**Bilag 4 - Hændelser der påvirker cloud-services (EKSEMPEL)**

**Beskrivelse:**

Handleplanen beskriver det beredskab, der skal etableres, hvis en eller flere cloudbaserede it-services bliver helt eller delvist utilgængelige og driften ikke ser ud til at kunne reetableres inden for Recovery Time Objective (RTO).

**Dokumentation:**

Ved aktivering af beredskabet skal al aktivitet logges til brug for efterfølgende dokumentation - brug hændelsesloggen i bilag 6. Det er også vigtigt at evt. identificerede svagheder/sårbarheder i it-beredskabet eller systemer beskrives. Det evalueres, om dette giver anledning til ændringer i systemer eller procedurer.

**Forudsætninger:**

*[Beskriv hvilke forudsætninger, der er gældende for denne handleplan. Der vil oftest være forhold, der er nødvendige for at kunne gennemføre handlingsplanen, fx udstyr, aftaler, fysiske lokationer, logistiske forhold eller kompetencer. Et eksempel kan være “Den basale infrastruktur (telefoni, internet mv.] er tilgængelig”]*

| **Nr.** | **Opgaver / aktioner** | **Ansvar** | |
| --- | --- | --- | --- |
| 1 | **Aktivering af it-beredskabet**  Relevant personale indkaldes/sammensættes. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 2 | **Vurdering af omfang**  Der foretages en vurdering af problemets omfang, herunder hvad der skal til for at man kan reetablere den berørte drift og om det er nødvendigt at etablere alternative løsninger. Hvis det er nødvendigt kontaktes tele-/internetleverandøren og/eller relevante myndigheder for at få assistance.  Vurderes det at være nødvendigt at etablere en alternativ løsning, håndteres det i første omgang - se step 3. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 3 | **Restore**  Det afklares om man kan lave en restore af it-systemet på samme udstyr eller om det skal ske på andet udstyr, der i så fald fremskaffes. Evt. kan it-systemmiljøet genetableres i et virtuelt miljø hos en it-leverandør.  Under arbejdet med at reetablere drift af de berørte systemer indsamler it-beredskabsteamet evt. dokumentation for problemet, der måtte være relevant for den efterfølgende vurdering af årsagen til problemet, ud over hvad der allerede findes i logs mv. |  | |
| 4 | **Tidsestimat for genetablering**  Der udarbejdes et foreløbigt tidsestimat for genetablering af normal drift. Estimatet revurderes løbende og dette, samt status, udmeldes til relevante interessenter (ledelsen, medarbejdere, osv.). | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 5 | **Kommunikation**  Når problemet er udbedret, og alt er klar til drift igen udmeldes dette til relevante interessenter (ledelsen, medarbejdere, kunder osv.). | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 6 | **Gennemgang af systemer**  Når de berørte systemer er klar til drift igen, skal alle systemer gennemgås for at tjekke, at:   * Systemerne er klar til drift (overvej backup af systemer inden evt. restore) * Data ikke er ødelagte * Netværksforbindelser er genetableret. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |

**Bilag 5 - Kommunikation**

**Beskrivelse:**

Handleplanen beskriver en kommunikationsplan, der kan følges i tilfælde af at et beredskab aktiveres.

**Dokumentation:**

Ved aktivering af beredskabet skal al aktivitet logges til brug for efterfølgende dokumentation - brug hændelsesloggen i bilag 6. Det er også vigtigt at evt. identificerede svagheder/sårbarheder i it-beredskabet eller systemer beskrives. Det evalueres om dette giver anledning til ændringer i systemer eller procedurer.

**Forudsætninger:**

*[Beskriv hvilke forudsætninger, der er gældende for denne handleplan. Der vil oftest være forhold, der er nødvendige for at kunne gennemføre handlingsplanen, fx udstyr, aftaler, fysiske lokationer, logistiske forhold eller kompetencer. Et eksempel kan være “Den basale infrastruktur (telefoni, internet mv.] er tilgængelig”]*

| **Nr.** | **Opgaver / aktioner** | **Ansvar** | |
| --- | --- | --- | --- |
| 1 | **Udarbejd tidsplan**  Der udarbejdes en tidsplan for ekstern og intern kommunikation. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 2 | **Indsaml information**  Al information, som er påkrævet for intern og ekstern kommunikation, samles hos den kommunikationsansvarlige. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 3 | **Beslut kommunikationskanal**  For hver enkelt intern og ekstern kommunikation fastlægges kommunikationskanalen. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 4 | **Udarbejd eksterne meddelelser**  Hvis der skal kommunikeres eksternt, udarbejdes materiale hertil, som godkendes af beredskabsledelsen. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 5 | **Oversæt relevant dokumentation**  Hvis der er behov for at vedlægge dokumentation, foretages eventuelt oversættelse heraf. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 6 | **Udsend information**  Sørg for, at al intern og ekstern kommunikation udsendes samtidigt, hvis dette er påkrævet, og at budskaberne er ens. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |
| 7 | **Responder på spørgsmål**  Svar på eventuelle spørgsmål med fokus på de mest kritiske spørgsmål og interessenter. | *[indsæt ansvarlig, jf. afsnit 4.1]* | |

### 

### 

### 

### 

### 

### 

### 

**Bilag 6 - Hændelseslog (EKSEMPEL)**

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

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

### **Dokumentinformation**

| Dokumentversion |  |
| --- | --- |
| Dato for udgivelse af denne version |  |
| Ansvarlig |  |
| Status |  |