

**IT-BEREDSKABSPLAN**

SKABELON

**Indhold**

[IT-beredskabsplan 3](#_Toc133237686)

[Baggrund, formål og målsætninger 3](#_Toc133237687)

[Anvendelsesområde 3](#_Toc133237688)

[Hvor kan man finde planen? 3](#_Toc133237689)

[Afprøvning og implementering 3](#_Toc133237690)

[Opdatering 3](#_Toc133237691)

[Hændelsesevaluering 3](#_Toc133237692)

[Logbog og dokumentation 3](#_Toc133237693)

[Roller og ansvar 4](#_Toc133237694)

[IT-beredskabsorganisation 4](#_Toc133237695)

[Aktivering af IT-beredskabsplanen 4](#_Toc133237696)

[Kommunikation 4](#_Toc133237697)

[Intern kommunikation 4](#_Toc133237698)

[Ekstern kommunikation 4](#_Toc133237699)

[Bilag 1 Kontaktliste 5](#_Toc133237700)

[Kontaktliste 5](#_Toc133237701)

[Bilag 2: Hændelseshåndtering 6](#_Toc133237702)

[Når en hændelse indtræffer 6](#_Toc133237703)

[Situationsvurdering 6](#_Toc133237704)

[Instruks A – Hændelse XX 6](#_Toc133237705)

[Instruks B - Hændelse XX 6](#_Toc133237706)

[Instruks C - Hændelse XX 6](#_Toc133237707)

[Bilag 3: Uddannelses- og træningsplan 7](#_Toc133237708)

[Bilag 4: Tjekliste for hændelsesevaluering 8](#_Toc133237709)

[Om hændelsesevaluering 8](#_Toc133237710)

[Bilag 5: Begrebsafklaring 9](#_Toc133237711)

# IT-beredskabsplan

Det gælder om at være godt forberedt, når f.eks. et cyberangreb rammer, eller hvis drifte rammes af lynnedslag. Her er IT-beredskabsplanen et nøgleværktøj. Med en god beredskabsplan er virksomheden klar til at navigere, mens angrebet står på.

## Baggrund, formål og målsætninger

Beskriv baggrund og formål og evt. målsætninger med IT-beredskabsplanen. Vær opmærksom på, at IT-beredskabsplanen skal være i overensstemmelse med evt. overordnet beredskabsplan og politikker indenfor sikkerhed, drift mv, f.eks. informationssikkerhed.

## Anvendelsesområde

Beskriv IT-beredskabsplanens anvendelsesområde (kaldes også gyldighedsområde), herunder hvilke systemer der er omfattet og evt. undtagelser og/eller afgrænsninger. *​​​​​​​*

## Hvor kan man finde planen?

Her skal I beskrive, hvor og hvordan beredskabsplanen opbevares. Det er vigtigt, at planen altid er tilgængelig, også i situationer hvor man ikke kan tilgå planen digitalt.

## Afprøvning og implementering

Beskriv principperne for hvordan IT-beredskabsplanen skal afprøves, f.eks. i form af øvelser, samt uddannelse og træning af ansatte mv. Konkrete uddannelses- og træningsplaner kan tilføjes som bilag.

Der er mange måder at afprøve planen på. Hvis I har en plan på [www.digitaltberedskab.dk](http://www.digitaltberedskab.dk/), kan IT-beredskabsplanen afprøves vha. hændelsesstyringen på siden.

## Opdatering

Beskriv hvor ofte beredskabsplanen skal opdateres, og hvem der er ansvarlig for det. Anbefales mindst 1 gang årligt og ved ændringer, f.eks. i kontaktoplysninger, organisatoriske ændringer og risikovurderinger.

## Hændelsesevaluering

Beskriv retningslinjer for hvordan hændelser og øvelser skal evalueres. *​​​​​​​*

## Logbog og dokumentation

Beskriv krav til dokumentation af hændelseshåndteringen. Udarbejd evt. skabelon til hændelseslog i bilag.

Hvis I har en plan på [www.digitaltberedskab.dk](http://www.digitaltberedskab.dk/), kan I gå til hændelsesloggen efter hændelsens afslutning for at se, hvordan håndteringen forløb, hvilken kommunikation der var undervejs, og hvem der deltog i forløbet.

# Roller og ansvar

## IT-beredskabsorganisation

Beskriv hvem, der har hvilke roller, opgaver og ansvarsområder i forb.m. en beredskabshændelse. Jeres beslutninger om den valgte beredskabs- og krisestyringsorganisation skal afspejles i konkrete instrukser for de ansvarlige (indsættes som bilag).

Hvis der i forvejen er defineret en beredskabsorganisation i den ordinære beredskabsplan, kan man med fordel benytte en lignende struktur indenfor IT-beredskabet. Husk også at udpege stedfortrædere i tilfælde af, at personer, som er en del af IT-beredskabet, er fraværende.

## Aktivering af IT-beredskabsplanen

Beskriv hvornår og hvordan IT-beredskabsplanen aktiveres. Hvis der i den ordinære beredskabsplan er beskrevet en procedure for mobilisering af krisegruppen, kan I henvise til denne.

# Kommunikation

## Intern kommunikation

Beskriv retningslinjer for intern krisekommunikation. Hvis retningslinjerne for krisekommunikation allerede er beskrevet i den ordinære beredskabsplan, kan I henvise til denne.

## Ekstern kommunikation

Beskriv retningslinjer for ekstern krisekommunikation. Hvis retningslinjerne allerede er beskrevet i den ordinære beredskabsplan, kan man henvise til denne.

# Bilag 1 Kontaktliste

## Kontaktliste

Indsæt kontaktliste med oplysninger på medlemmer af IT-beredskabsgruppen samt evt. IT-leverandører og øvrige parter, som man kan få brug for at kontakte i forbindelse med en IT-beredskabshændelse. *​​​​​​​*Husk også at have stedfortrædere/alternative kontaktpersoner med på listen i tilfælde af, at man ikke kan få fat på den primære person.

Interne medlemmer af IT-beredskabsgruppen

|  |  |  |  |
| --- | --- | --- | --- |
| **Funktion** | **Person** | **Tlf.nr.** | **E-mailadresse** |
| Driftsansvarlig | Navn Navnesen | +45 XX XX XX XX | navn@domæne.dk |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Eksterne parter

|  |  |  |  |
| --- | --- | --- | --- |
| **Virksomhed** | **Rolle** | **Ansvar** | **Kontaktoplysning** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Bilag 2: Hændelseshåndtering

Her skal I beskrive de instrukser, I skal følge ved en hændelse på IT-området.

I anbefales at lave instrukserne i samarbejde med en IT-sikkerhedsekspert.

Hvis I bruger en IT-sikkerhedsplatform og/eller [www.digitaltberedskab.dk](http://www.digitaltberedskab.dk/), skal beredskabsplanen og instrukserne til hændelseshåndtering tilpasses dette.

## Når en hændelse indtræffer

Beskriv alarmeringsprocedurer, når en beredskabshændelse indtræffer. Førsteindsatsen fremgår af instrukserne.

## Situationsvurdering

Udarbejd en procedure for hvordan I vurderer omfanget af situationen/hændelsen.

Sørg for at beskrive:

* de processer der er påvirket af hændelsen
* i hvilket omfang de er påvirket
* den estimerede tidsramme for nøddrift af de tilhørende systemer.

Den person, der vurderer situationen og laver vurderingen, afhænger af den situation/hændelse, I er udsat for.

## Instruks A – Hændelse XX

Beskriv skridt for skridt hvad I konkret vil gøre, når en specifik hændelse indtræffer. Det kan f.eks. være et DDOS-angreb.

Instruksen skal sikre en effektiv indsats og skal fungere som et vigtigt støtteelement i processen, fordi der sjældent er et klart overblik over hændelsens omfang fra start af. I bør f.eks. overveje, i hvilke situationer I vil/kan lukke internetforbindelsen, hvordan I kan indsamle beviser m.v.

## Instruks B - Hændelse XX

## Instruks C - Hændelse XX

# Bilag 3: Uddannelses- og træningsplan

Beskriv konkrete tiltag i forhold til uddannelse og træning af medarbejderne (øvelsesaktiviteter) i virksomheden og evt. en oversigt over planlagte og gennemførte øvelser.

Øvelser kan foregå på flere forskellige måder. For eksempel:

* **Procedureøvelser** af kortere varighed-2 timer, hvor en eller flere procedurer i jeres IT-beredskab afprøves.
* **Dilemmaøvelser** af 1-4 timers varighed, hvor relevante deltagere samles og gennemspiller et opstillet scenarie.
* **Krisestyringsøvelser** af 4-8 timers varighed, hvor deltagerne skal løse IT-beredskabsopgaver ud fra et opstillet scenarie, sideløbende med deres almindelige arbejde.

|  |  |  |
| --- | --- | --- |
| **Beskrivelse af øvelse** | **Tidspunkt** | **Initialer** |
|  | DD/MM-ÅÅÅÅ | XXX |
|  |  |  |
|  |  |  |
|  |  |  |

# Bilag 4: Tjekliste for hændelsesevaluering

## Om hændelsesevaluering

Efter en hændelse, skal der altid gennemføres en evaluering af hændelsen og indsatsen.

Hændelsesevalueringen skal bl.a. beskrive hændelsens forløb, de opnåede erfaringer og planlagt opfølgning med en tidsplan for opfølgningen. Hav evt. tjeklister for at gøre evalueringen mere overskuelig og for at sikre, at I husker at få alt relevant med.

Det kan f.eks. være relevant at overveje:

* Er der behov for genanskaffelser af udstyr til personale?
* kan – og skal – systemer der ikke er omfattet af IT-beredskabsplanen reetableres?
* Er det nødvendige personale til rådighed for normal drift?
* Skal der indgås nye aftaler med leverandører?

# Bilag 5: Begrebsafklaring

|  |  |  |  |
| --- | --- | --- | --- |
| **DA** | **EN** | **Forklaring** | **Forkortelse** |
| Styring af  Fortsat Drift  (Forretnings-  kontinuitet) | Business  Continuity  Management | Et ledelsessystem til at styre og imødegå risikoen for pludselige produktions- eller leverancestop og til at varetage organisationens primære funktioner under og efter en kritisk hændelse. | BCM |
| Plan for  Fortsat Drift  (Forretnings-  kontinuitet) | Business  Continuity  Plan | En plan der kortlægger procedurer for respons, nøddrift og genopretning af virksomhedens normale drift i tilfælde af en kritisk hændelse. | BCP |
| Konsekvens-  analyse af forstyrrelser på driften (BIA) | Business  Impact Analysis | Analyse til systematisk at identificere og evaluere, hvilken konsekvens forstyrrelser af kritiske aktiviteter vil/kan have på forretningen. | BIA |
| Risiko-  Reduceringsplan (Strategi for fortsat drift) | Risk Reduction Plan | En plan der kortlægger, hvordan identificerede risici kan reduceres. | RRP |
| Maksimal  tolereret nedetid | Maximum  Tolerable Downtime | Den tid det ville tage for konsekvenser (der opstår som følge af ikke at levere et produkt/tjeneste eller udføre en aktivitet) at blive uacceptable. | MTD |
| Krav til  genopretningstid | Recovery Time Objective | Den målsatte tid for at genoprette kritiske aktiviteter og ressourcer efter et udfald. | RTO |
| Tolerance for  datatab | Recovery Point Objective | Den mængde data der maksimalt kan tolereres at gå tabt i tilfælde af en driftsforstyrrelse. | RPO |