# It-beredskabspolitik

For

[organisation]

| Version | *Skabelon* |
| --- | --- |
| Dato | Januar 2022 |
| Godkendt af | [ledelsen] |

# Før du går i gang - vejledning til 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 beredskabspolitikken.

Skabelonen er beskrevet ud fra den antagelse, at organisationen ikke har en tidligere beredskabspolitik 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 beredskabspolitik 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 skabelonen 2](#_Toc361306042)

[1 Formål med it-beredskabspolitikken 4](#_Toc361306043)

[2 Udgangspunkt for it-beredskabet 4](#_Toc361306044)

[3 Afgrænsning og antagelser 5](#_Toc361306045)

[4 Målsætning for it-beredskabet 5](#_Toc361306046)

[5 Roller og ansvar 6](#_Toc361306047)

[6 Retableringsstrategier 7](#_Toc361306048)

[7 Eksterne leverandører 8](#_Toc361306049)

[8 Beredskabsscenarier 9](#_Toc361306050)

[9 Implementering af it-beredskabet 10](#_Toc361306051)

# Formål med it-beredskabspolitikken

Formålet med denne it-beredskabspolitik er at fastlægge de overordnede rammer for [*organisationens*] arbejde med og implementering af it-beredskabet. Politikken indeholder en beskrivelse af det ønskede niveau for it-beredskabet og er udtryk for [*organisationens*] forventninger og krav til hertil.

Den operationelle udmøntning af politikken beskrives særskilt i it-beredskabets planer.

[På Digitaliseringsstyrelsens hjemmeside findes et eksempel på en skabelon til en it-beredskabsplan, som kan anvendes af organisationer der helt eller delvist selv varetager it-driften. Derudover findes en skabelon til organisationer, som har udliciteret hele it-driften.]

[Opdelingen af it-beredskabet i en politik og en plan med et operationelt sigte skyldes hensynet til det løbende vedligeholdelsesarbejde, da politikken som udgangspunkt er mere langsigtet og dermed mindre vedligeholdelseskrævende end de operationelle planer.]

Beredskabet er ledelsens ansvar, og politikken godkendes af ledelsen.

# Udgangspunkt for it-beredskabet

It-beredskabet er udarbejdet med udgangspunkt i en risikovurdering, som er baseret på de forretningsmæssige behov eller krav. Sammenhængen mellem de forskellige elementer i beredskabet er illustreret i figuren nedenfor.



# Afgrænsning og antagelser

Nedenfor fremgår de afgrænsninger, [*organisationen*] har lagt til grund for omfang og indhold af it-beredskabet og de udarbejdede beredskabsplaner:

* [*At beredskabet kun gælder for bestemte geografiske områder, hvis organisationens opgaveløsning finder sted fra flere lokationer. Afgrænsningen konkretiseres*.]
* [*At beredskabet kun gælder for bestemte forretningsområder/opgavetyper. Afgrænsningen konkretiseres*.]
* [*At beredskabet kun gælder for en del af driften, fx systemer organisationen selv drifter. Afgrænsningen konkretiseres*.]
* [*At beredskabet kun gælder for en delmængde af de driftsleverandører, der anvendes. Afgrænsningen konkretiseres*.]
* [*At beredskabet kun gælder for infrastruktur og ikke applikationer, eller omvendt*.]

[Herudover kan der også være særlige ekstreme hændelsesscenarier (såkaldte ”Black Swans”) – kendetegnet ved meget lave sandsynligheder og meget ødelæggende konsekvenser – som organisationen ikke ønsker at tage højde for (pga. den meget lave sandsynlighed for forekomst af hændelser). Eksempler på sådanne scenarier bør, om muligt, anføres sammen med en beskrivelse af, hvordan risikoen ved det manglende beredskab håndteres (accept af risiko, overførsel/outsourcing, undgåelse).]

Beredskabet forventes at fungere effektivt under forudsætning af følgende antagelser:

* [*Det antages, at en katastrofe ikke samtidigt ødelægger organisationens og driftsleverandørens fysiske lokationer*.]
* [*Det antages, at en katastrofe ikke er sammenfaldende med flere af beredskabsledelsens nøgleaktørers fratræden fra deres stillinger*.]

# Målsætning for it-beredskabet

Med udgangspunkt i de forretningsmæssige behov i [*organisationen*] er en række elementer afgørende for, at beredskabet lever op til ledelsens målsætning for it-beredskabet. Elementerne er desuden grundlag for valg af retableringsstrategi.

[Den overordnede målsætning for it-beredskabet fremgår desuden typisk af informationssikkerhedspolitikken.]

Følgende målsætninger skal opfyldes i beredskabet:

* [*Beredskabet skal begrænse skadevirkningerne af en katastrofe på it-understøttede forretningsprocesser.*]
* [*Beredskabet skal understøtte en smidig overgang til alternative driftsfaciliteter*.]
* [*Beredskabet skal understøtte smidig retablering af data og systemer efter en katastrofe*.]
* [*Beredskabet skal understøtte aktivering af alternative it-driftsscenarier i tilfælde af en katastrofe*.]
* [*Beredskabet skal understøtte at medarbejdere uddannes i håndtering af en katastrofe, der berører it-anvendelsen*.]
* [*Beredskabet skal understøtte, at der kan etableres et smidigt samarbejde med leverandører i tilfælde af en katastrofe, der berører organisationens it-anvendelse*.]
* [*Beredskabet skal understøtte, at efterfølgende vurdering og evt. kontrol af retableringsforløbet kan redegøres gennem fyldestgørende udfyldelse af hændelsesjournal/-log*.]

# Roller og ansvar

Ledelsen har det overordnede ansvar for beredskabet.

[I praksis vil det ofte være it-sikkerhedskoordinatoren og/eller beredskabskoordinatoren, der koordinerer de forskellige opgaver, som er forbundet med beredskabsstyringen.]

Beredskabsstyringen omfatter en række opgaver af meget forskellig karakter, og der er flere forskellige aktører, som bidrager til såvel planlægning, udarbejdelse og vedligeholdelse af beredskabet.

Dette afsnit beskriver roller og ansvar i relation til udarbejdelsen og vedligeholdelsen af de enkelte operationelle delelementer i beredskabsplanlægningen og de væsentligste planlægningsområder. For at lette vedligeholdelsen af den skrevne operationelle plan er opgaver og aktiviteter primært placeret i funktionelle enheder eller hos rolleindehavere frem for hos navngivne personer.

[Det anbefales helt overordnet at skelne mellem organisationens eget ansvar, det koncernfælles (på tværs af ministerområdet) ansvar og et leverandøransvar. Hvis der er behov for det, kan organisationens ansvar deles yderligere op (fx mellem en central it-funktion og en projektenhed). For at kunne gøre dette er det en forudsætning, at der er skabt overblik over serviceaftaler og eksisterende forpligtelser vedrørende beredskab.]

Nedenstående aktivitetsliste og ansvarsbeskrivelser præciserer, hvem der har ansvaret for de forskellige opgaver i forbindelse med planlægning og vedligeholdelse af [*organisationens*] it-beredskab.

[Aktiviteterne kan præciseres yderligere, hvis organisationen finder det nødvendigt.]

|  | **Organisationens ansvar** | **Koncernfælles ansvar** | **Leverandøransvar** |
| --- | --- | --- | --- |
| **Retningslinjer for aktivering af plan** |  |  | *Kriterier for aktivering af beredskabsplanen skal aftales med leverandøren. Begge parter kan have egne kriterier*. |
| **Planlægge retableringsteams** | *Organisationen skal varetage planlægningen af egne retableringsteams.* |  |  |
| **Planlægge kontaktlister** | *Alle parter har et ansvar for at sikre, at kontaktoplysningerne opdateres.* |  |  |
| **Definering af processer til beredskabsledelse** | *Definering af intern eskalering i myndigheden.* | *Definering af kriterier for, hvornår departementet skal inddrages i håndteringen af en beredskabssituation.* | *Inputgiver til, hvorledes leverandører skal inddrages i håndteringen af en beredskabssituation.* |
| **Definering af operationelle planer (hardware)** |  | *Koncern-it har ansvaret for systemer, som de drifter (system X, Y, Z).**Departementet har ansvar for at føre tilsyn.* | *Leverandør X har ansvar for outsourcede systemer X, Y og Z.* |
| **Definering af operationelle planer (software)** |  |  | *Leverandør X har ansvar for outsourcede systemer X, Y og Z.* |
| **Definering af operationelle planer (netværk)** | *Plan for retablering af netværkskomponenter, som supporteres af organisationen selv.* | *Plan for retablering af netværkskomponenter, som supporteres af koncern-it.* | *Plan for retablering af netværkskomponenter, som supporteres* af *leverandør.* |
| **Definering af operationelle detailprocedurer** |  |  |  |
| **Vedligehold af tekniske hjælpemidler (scripts mv.).** |  |  |  |

# Retableringsstrategier

Formålet med retableringsstrategien er at planlægge, hvordan systemet overordnet set retableres i en beredskabssituation med hensyn til de forretningsmæssige behov, der er i form af krav til tilgængelighed (Recovery Time Objective / RTO) og evt. tolerance for datatab (Recovery Point Objective / RPO).

For de it-systemer i [*organisationen*], der i risikovurderingen er identificeret som forretningskritiske, er der defineret retableringsstrategier jf. nedenstående tabel.

Retableringsstrategi for [*organisationens*] systemer med lavere prioritering fremgår af de operationelle beredskabsplaner.

[Retableringsstrategier kan fx være: At have dublerede systemer (”hot site”), at have et fuldt setup stående parat (”cold site”), at retablere fra backup på udstyr fra test/udviklingsmiljøer eller på udstyr jf. aftale om hurtig levering fra leverandøren, eller blot hurtigst muligt. Det afgørende er, at den valgte retableringsstrategi kan leve op til de behov som er fastlagt. Hvis der er usikkerhed herom, bør der foretages en test af det planlagte beredskab.]

| **System** | **RTO** | **RPO** | **Retableringsstrategi** |
| --- | --- | --- | --- |
| *System A* | *3 dage* | *24 timer* | *Systemet driftes af ekstern leverandør, og der er indgået en aftale om, at leverandøren foretager daglig backup, som opbevares geografisk adskilt fra produktionsområdet. I en beredskabssituation er det aftalt, at leverandøren retablerer systemet fra backup.* |
| *System B* | *1 time* | *1 time* | *Systemet driftes af ekstern leverandør, og der er indgået aftale om, at leverandøren supporterer en spejlet løsning på fysisk adskilte driftslokationer, således at der i en beredskabssituation foretages failover til den fungerende lokation. Leverandøren foretager desuden daglig backup, som opbevares adskilt fra produktionsområdet.* |

# Eksterne leverandører

[*Organisationens*] krav til sikkerhed og tilgængelighed skal opfyldes, også selvom [*organisationen*] er afhængig af eksterne leverandører. Derfor skal det som en del af beredskabet sikres, at leverandørerne kan leve op til de sikkerhedskrav til beskyttelse af data og det serviceniveau i forhold til tilgængelighed, som [*organisationen*] forventer.

I forhold til fortroligheden af data skal det sikres, at leverandøren er bekendt med [*organisationens*] klassifikationsniveauer, og hvilke krav til håndteringen af data det medfører. I en beredskabssituation kan det være nødvendigt at ændre eller omgå de normale sikringsforanstaltninger, og leverandøren skal derfor være særlig opmærksom på, hvilke krav der er til beskyttelse af fortroligheden.

[*Organisationens*] konkrete krav til retableringsmål (RTO, RPO mv.) fremgår af driftsaftalerne og er beskrevet i it-beredskabsplanen. Løbende kontrol af om leverandøren kan efterleve disse krav udføres jf. de konkrete aftaler og består af en eller flere af følgende kontroller:

* SLA-aftaler samt aftaleforhold, der forpligter leverandører til et højt kvalitets- og sikkerhedsniveau (fx efterlevelse af ISO-standarder)
* periodevise revisionserklæringer
* via periodiske test og målinger
* løbende rapportering af resultater

|  |
| --- |
| For kunder i Statens It skal kravene fremgå af Kundeaftaler og evt. Databehandleraftale, og det er afgørende at systemernes kritikalitet og datas kategorisering jf. Persondataloven er oplyst. En standard Kundeaftale opfylder ikke kravene for retablering af kritiske systemer eller håndtering af persondata, men kræver eksplicit kravstillelse. |

# Beredskabsscenarier

I dette afsnit er der en oversigt over de beredskabsscenarier, som [*organisationen*] anser som mulige konsekvenser ud fra trusselsbilledet, og som den operationelle beredskabsplan skal kunne håndtere. Scenarierne indikerer hvilke operationelle delplaner, der skal defineres i beredskabsplanen og aktiveres i en beredskabssituation.

[I beredskabsmæssig henseende fokuseres traditionelt på scenarier, der vedrører tilgængeligheden af it-understøttelsen. Principielt er der dog ikke noget i vejen for, at lade beredskabsplanen omfatte scenarier, der vedrører tab af integritet og/eller fortrolighed. Hændelser i disse kategorier kan sagtens have en alvorlighed, der kræver aktivering af den ”undtagelsestilstand”, som beredskabsplanen er udtryk for. Scenarierne kan enten beskrives med udgangspunkt i den trussel (brand, hackerangreb, etc.), der udløser katastrofen eller med udgangspunkt i konsekvensen af hændelsesforløbet (eller begge dele). Følgende er eksempler på scenarier beskrevet med udgangspunkt i konsekvensen.]

| **Scenarie** | **Primære trusler** |
| --- | --- |
| *Svigt af en enkelt komponent i it-infrastrukturen, som udgør ”single point of failure” (SPOF), hvorved der udløses et hændelsesforløb af beredskabsmæssig karakter.* | *Fejlende hardware, menneskelige fejl* |
| *Svigt af netværksinfrastruktur, hvorved en hel lokation afskæres fra it-understøttelse.* | *Fejlende hardware, hackerangreb* |
| *Svigt af centrale servere, hvorved kritiske systemer bliver utilgængelige, og væsentlige opgaver ikke kan løses.* | *Malware, hackerangreb, sabotage* |
| *Fysisk ødelæggelse af serverrum, hvorved kritiske systemer bliver utilgængelige, og væsentlige opgaver ikke kan løses.* | *Naturfænomener, terrorisme, sabotage* |
| *Forsyningssvigt, hvorved kritiske systemer bliver utilgængelige, og væsentlige opgaver ikke kan løses.* | *Naturfænomener, terrorisme, sabotage, menneskelige fejl* |
| *Ødelæggelse af fysiske lokationer, hvorved kritiske systemer bliver utilgængelige, og væsentlige opgaver ikke kan løses.* | *Naturfænomener, terrorisme* |
| *Brud på fortrolighed af følsomme personoplysninger, hvorved borgere udsættes for risiko for identitetstyveri eller andre væsentlige indskrænkninger i deres handlefrihed.* | *Hackerangreb, konfigurationsfejl* |

[Det anbefales at præcisere ovenstående generiske scenarier, så de er bedst muligt målrettet mod den enkelte organisations forhold. Fx at udpege komponenter, som på forhånd er kendt som SPOF’er[[1]](#footnote-1) eller udpege fysiske lokationer, der er særligt kritiske.]

# Implementering af it-beredskabet

Kommunikation og implementering i [*organisationen*]sker efter "top-down" princippet, hvor ledelsen og it-sikkerhedskoordinatoren har ansvaret for at kommunikere videre til de medarbejdere, som indgår i beredskabsorganisationen.

Kommunikationen spiller en vigtig rolle og skal sikre, at både den operationelle plan og fremtidige opdateringer hertil formidles effektivt og direkte.

Målet med kommunikationen er at:

* gøre medarbejdere opmærksomme på, at der eksisterer en it-beredskabsplan, hvad den indeholder, og hvordan den vil kunne påvirke medarbejderen i en beredskabssituation,
* informere beredskabsorganisationen og it-afdelingen om opdateringer til beredskabsplanen, når det er relevant,
* skabe en distributionskanal for den opdaterede beredskabsplan og sikre og forbedre it-beredskabssituationen.

En god implementering af beredskabsplanen viser sig i en beredskabssituation, hvor kommunikationen og håndteringen af beredskabet:

* er præcis og rettidig,
* sikrer tilstrækkelig information til medarbejdere, brugere, samarbejdspartnere og pressen,
* sikrer konsistens i informationen om hvilke systemer, der er berørte, hvilken konsekvens situationen medfører, forventninger til retableringstidsrammen mv..

[Modtagerne af informationen vil variere fra situation til situation, men relevant information til brugerne er af særlig vigtighed. På Digitaliseringsstyrelsens hjemmeside findes en *Vejledning til kommunikation i en beredskabssituation*, som beskriver dette nærmere.]

1. Single Point Of Failure. Komponenter i it-infrastrukturen, der, hvis de svigter, via en kaskade-effekt vil betyde udbredt brud på tilgængeligheden til informationsaktiver. [↑](#footnote-ref-1)