Skabelon for IT-beredskabspolitik (Mellemstor virksomhed)

Følgende dokument er en skabelon til udarbejdelse af en IT-beredskabspolitik. IT-beredskabspolitikken sætter rammerne for jeres kriseberedskabsarbejde og indeholder alle de informationer som I skal bruge for at fastsætte organisering og vedlige holde kriseberedskabet i ’fredstid’. Dokumentet er én af flere skabelon-dokumenter, som indgår i det IT-sikkerhedsmateriale, som alle organisationer bør have ift. overholdelse af NIS2.

Vi har i Lakeside lavet en række skabeloner, som du er velkommen til at bruge. Skabelonerne er tiltænkt SMV’er med produktion, men kan sagtens bruges af organisationer uden produktion (OT). Skabelonerne er udarbejdet med udgangspunkt i små og mellemstore forsyningsselskaber.

* IT-sikkerhedspolitik
* IT-sikkerhedshåndbogen
* OT-leverandørpolitik, og leverandør tjeklister
* Risikostyringspolitik og Risikolog
* Hændelseshåndteringsproces og Hændelseslog
* Kriseberedskabspolitik, -planer og -skabeloner

Alle skabeloner kan findes og downloades på [www.lakeside.dk/publikationer](http://www.lakeside.dk/publikationer)

**Sådan bruger du skabelonen**

* Tekster med gråt og i firkantede klammer er vejledningstekster, som slettes ved endt redigering.
* <organisation> er en dokument-egenskab. Den kan rettes under Filer / Egenskaber / Brugerdefineret (nederste tekstboks) og derefter opdatere alle felter i hele dokumentet (vælg alt og højreklik).
* Alle tekster kan ændres efter behov og som tilpasning til din organisation. Alle tekster med gult bør du ændre eller som minimum forholde dig til.
* Kontaktinformation og organisation skal opdateres i sidehoved og sidefod. OBS! Organisation og logo på forsiden er også i en sidefod.

Dato | Version x.x

it-beredskabspolitik

termer

|  |  |
| --- | --- |
| Begreb eller forkortelse i teksten  | Beskrivelse |
| OT | Operationel teknologi (OT) refererer til hardware og software, der bruges til at overvåge og kontrollere fysiske enheder, processer og infrastruktur i forskellige industrier, herunder energisektoren. Udtrykket bruges til at skelne mellem traditionelle informationsteknologi (IT) systemer og industrielle kontrolsystemer. |
| SaaS | Software som en service (Software-as-a-Service) er en softwareløsning, der er betalt efter forbrug hos en cloudtjenesteudbyder. Man lejer brugen af software, og brugere kan oprette forbindelse til den via internettet, typisk vha. en webbrowser. Al underliggende infrastruktur, middleware, appsoftware samt alle appdata findes i tjenesteudbyderens datacenter. Tjenesteudbyderen administrerer hardwaren og softwaren og vil, med den rette serviceaftale, sikre tilgængeligheden af og sikkerheden for både appen og dine data. |
| SLA | Service Level Agreement (SLA) er en aftale mellem kunde og serviceudbydere, der definerer nødvendige tjenester og det forventede serviceniveau. |
| SPOF | Single Point Of Failure. Komponenter i IT/OT-infrastrukturen, der, hvis de svigter, via en kaskade-effekt vil betyde udbredt brud på tilgængeligheden til informationsaktiver. |

Revisions- og Godkendelseshistorik

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Dato | Ansvarlig | Godkendt | Ændringer |
| [0.0] | [dd/mm/yy] | [Initialer] | [dd/mm/yy][Intialer] |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Kontaktpersoner

|  |  |
| --- | --- |
| Fornavn Efternavn (initialer)Skriv din titel her, fx direktørTlf.: +45 xxxx xxxxxxx@domæne.dk | Fornavn Efternavn (initialer)Skriv din titel her, fx IT-sikkerhedsfunktionTlf.: +45 xxxx xxxxxxx@domæne.dk |

Indholdsfortegnelse

[1 Indledning 4](#_Toc184933898)

[1.1 Antagelser 4](#_Toc184933899)

[1.2 Revision 4](#_Toc184933900)

[1.3 Afprøvning af IT-beredskabet 5](#_Toc184933901)

[2 Målsætning 5](#_Toc184933902)

[3 Ansvarsfordeling 6](#_Toc184933903)

[3.1 <Organisation>s ansvar 6](#_Toc184933904)

[3.2 Beredskab hos IT/OT-Leverandør 6](#_Toc184933905)

[3.3 IT/OT-Leverandørers ansvar i <Organisation>s beredskab 7](#_Toc184933906)

[4 IT-beredskabsorganisation 8](#_Toc184933907)

[4.1 Strategisk niveau 9](#_Toc184933908)

[4.2 Taktisk niveau 9](#_Toc184933909)

[4.3 Operationelt niveau 9](#_Toc184933910)

[5 Beredskabets faser 10](#_Toc184933911)

[6 Reetableringsstrategier 10](#_Toc184933912)

[7 Krisescenarier 12](#_Toc184933913)

[8 Implementering af IT-beredskabspolitikken 13](#_Toc184933914)

# Indledning

[Vejledning: denne skabelon er tiltænkt SMV’er som har udliciteret hele deres IT- og OT-drift. IT-beredskab kaldes også IT-kriseledelse. Begge udtryk vil være afspejlet i skabelonerne som understøtter IT-beredskabet.]

Formålet med denne IT-beredskabspolitik er at fastlægge de overordnede rammer for s arbejde med og implementering af IT-beredskab. Politikken indeholder en beskrivelse af det ønskede niveau for IT-beredskabet og er udtryk for s forventninger og krav til hertil.

Den operationelle udmøntning af politikken beskrives særskilt i IT-beredskabs planen.

IT-beredskabsplanen baserer sig på aftaler med IT- og OT-leverandører.

IT-beredskabsplanen indgår i s samlede beredskab, sammen med beredskabsplaner for brand og evakuering etc.

## Antagelser

IT-beredskabet forventes at fungere effektivt under forudsætning af følgende antagelser:

* Det antages, at en katastrofe ikke samtidigt ødelægger s og driftsleverandørens fysiske lokationer.

## Revision

IT-beredskabspolitikken gennemgår årligt review og ledelsesgodkendelse hos den øverste ledelse. sIT-sikkerhedsfunktion er ansvarlig for det årlige review.

IT-beredskabsplanen og tilhørende skabeloner gennemgår review og opdatering efter aktivering, og som minimum årligt i overensstemmelse med IT-beredskabspolitikken.

For at lette vedligeholdelsen af den skrevne politik og plan er opgaver og aktiviteter primært placeret i funktionelle enheder eller hos rolleindehavere frem for hos navngivne personer. I Bilag A fremgår den navngivne liste over personer, som kan varetage forskellige roller i en krisesituation.

## Afprøvning af IT-beredskabet

 vil løbende afprøve IT-beredskabet i forhold til at sikre forretnings- og informationssikkerhedskontinuiteten. Fx ved via IT-beredskabsøvelser at afprøve IT-beredskabet, IT-beredskabsorganisationen og eventuelle nødprocedurer. Regelmæssig afprøvning af IT-beredskabet sikrer et kontinuerligt fokus på optimering af procedurer og roller, og forbereder de enkelte aktører på den dag, hvor det bliver virkelighed.

Afprøvningen kan foregå som en skrivebordsøvelse, fx baseret på Beredskabsspillet fra [www.sikkerdigital.dk](https://www.sikkerdigital.dk/myndighed/iso-27001-implementering/beredskabsstyring/beredskabsspillet), eller ved aktivering af IT-beredskabet for en mindre hændelse, der normalt ikke vil afstedkomme en aktivering af IT-beredskabet.

Afprøvningen vil blive foretaget halvårligt. En afprøvning kan aflyses, hvis IT-beredskabet har været aktiveret og afprøvet på en virkelig hændelse.

# Målsætning

Med udgangspunkt i de forretningsmæssige behov i er en række elementer afgørende for, at IT-beredskabet lever op til ledelsens målsætning for IT-beredskab. Elementerne er desuden grundlag for valg af reetableringsstrategi.

Følgende målsætninger skal opfyldes i IT-beredskabet:

* IT-beredskabet skal begrænse skadevirkningerne af en katastrofe på IT- og OT-understøttede forretningsprocesser.
* IT-beredskabet skal understøtte smidig retablering af data og systemer efter en krisehændelse.
* IT-beredskabet skal understøtte at medarbejdere uddannes i håndtering af en krisehændelse, der berører IT- og OT-anvendelsen.
* IT-beredskabet skal understøtte, at der kan etableres et smidigt samarbejde med leverandører i tilfælde af en krisehændelse, der berører organisationens IT- og OT-anvendelse.
* IT-beredskabet skal understøtte, at efterfølgende vurdering og evt. kontrol af retableringsforløbet kan redegøres gennem fyldestgørende udfyldelse af hændelseslog.

# Ansvarsfordeling

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

Dette afsnit beskriver ansvarsfordelingen i relation til udarbejdelsen og vedligeholdelsen af de enkelte operationelle delelementer i IT-beredskabsplanlægningen og de væsentligste planlægningsområder.

## s ansvar

s ledelse har det overordnede ansvar for IT-beredskabet.

 har ansvaret for at sikre forretningskontinuitetsprocedurer for de enkelte afdelinger.

 har ansvaret for at indgå dækkende aftaler med leverandørerne ift. afsnit 3.2. s krav til sikkerhed og tilgængelighed skal opfyldes, også selvom er afhængig af eksterne leverandører. Derfor skal det som en del af IT-beredskabsplanlægningen sikres, at leverandørerne kan leve op til de sikkerhedskrav til beskyttelse af data, og det serviceniveau i forhold til tilgængelighed, som forventer.

 har ansvaret for at vedligeholde kontaktoplysningerne i Bilag A.

## Beredskab hos IT/OT-Leverandør

For de leverandører som leverer services som understøtter s IT/OT, skal det sikres at det fremgår enten af en specifik aftale, en standardaftale eller på anden vis skriftlig fastholdelse at:

* det er aftalt hvorledes leverandøren skal informere i tilfælde af aktivering af eget IT-beredskab.

Det er vigtigt at pointere, at aktivering af s IT-beredskab ikke nødvendigvis aktiverer leverandørens IT-beredskab og vice versa. Der skal derfor være aftaler om kommunikationsniveauet fra leverandøren, som sikrer at s forpligtigelser er dækket i forbindelse med IT-beredskabet.

## IT/OT-Leverandørers ansvar i <Organisation>s beredskab

For de leverandører som kan have opgaver i forbindelse med et aktiveret IT-beredskab hos , skal det sikres at det fremgår enten af en specifik aftale, en standardaftale eller på anden vis skriftlig fastholdelse:

* at det er aftalt hvorledes leverandøren skal inddrages i håndtering af en krisehændelse (kontaktpunkt, ressourcer, svartider, kommunikation).
* at leverandørens opgaver og SLA er aftalt ift. genetablering af nøddrift og normal drift
* at det er aftalt at leverandøren skal orientere om ændringer til kontaktoplysningerne i Bilag A, og hvorledes denne orientering skal foretages.

Samtidig skal det sikres at det aftalte svarer til s behov ift. s risikovurdering og organisering.

### SaaS-Leverandører

Ansvaret for hardware, software, genskabelse etc. ligger alene hos den pågældende SaaS IT-leverandør. For disse leverandører, skal det sikres at det fremgår enten af en specifik aftale, en standardaftale eller på anden vis skriftlig fastholdelse:

* at det er aftalt hvilke informationer leverandøren skal rapportere til i forbindelse med en krisehændelse (kontaktpunkt, ressourcer, svartider, kommunikation).
* at leverandøren varetager sit ansvar for IT-sikkerhed inkl. backup og genetablering, og at der er defineret faste aftaler herom.

Samtidig skal det sikres at det aftalte svarer til <Organisation>s behov ift. <Organisation>s risikovurdering og organisering.

Aktivering af SaaS leverandørens beredskab vil sjældent aktivere <Organisation>s IT-beredskab, men vil aktivere <Organisation>s nødprocedurer til sikring af forretningskontinuitet, samt muligvis pålægge <Organisation> et indberetningsansvar til myndigheder. Dvs. at Kriseledelsen vil i dette tilfælde primært have ansvaret for:

1. at samle op på information fra leverandøren og kommunikere til egne interessenter og myndigheder.
2. aktivere interne alternative forretningsprocesser, til sikring af forretningskontinuitet.

Til understøttelse af dette kan evt. benyttes kommunikationsplanen til IT-beredskabet.

# IT-beredskabsorganisation



Figur : De tre niveauer i kriseberedskabsorganiseringen.

De tre niveauer af kriseberedskabet er:

* Strategisk niveau
Styrer og sætter retning med mandat af s ledelse. Er ansvarlig for kommunikation ud af IT-beredskabsorganisationen.
* Taktisk niveau
Leder og styrer de konkrete opgaver og kommer med forslag og status. Er ansvarlig for kommunikation mellem det operationelle- og det strategiske niveau af IT-beredskabsorganisationen. Taktisk kriseleder er udpeget baseret på det fagområde, der er primært berørt af krisehændelsen.
* Operationelt niveau
Udfører de konkrete opgaver. Vil bestå af medarbejdere (service, support og/eller drift) hos:
	+ IT leverandør(er),
	+ OT leverandør(er) og/eller
	+ egne medarbejdere

## Strategisk niveau

Det strategiske niveau af IT-beredskabsorganisationen omfatter en række opgaver af meget forskellig karakter, og der er flere forskellige aktører, som bidrager i en krisesituation:

* Kriseleder
Leder af det strategiske niveau og ansvarlig for at sætte retningen og rapportering til direktionen og bestyrelsen.
* Krisekoordinator
Ansvarlig for at indkalde til møder, tage referater og sikre forplejning.
* Taktisk kriseleder
Ansvarlig for koordinering med og styring af det operationelle niveau og kommunikation mellem IT-beredskabsniveauerne. Udpeget blandt Fagchef/Teamleads.
* Fagchef(er)/Teamlead
Ansvarlig for at samle op og indrapportere fra berørte områder. Input til konsekvensvurdering, samt indmelding af ressourcer til operationelt niveau.
* Kommunikationsansvarlig
Ansvarlig for kommunikation til interessenter udenfor IT-beredskabs-organisationen: kunder, ansatte, andre samarbejdspartnere, medier og myndigheder.

Medarbejdere udpeges og trænes i at varetage ovenstående aktørroller. Alle roller på det strategiske niveau skal være tildelt mindst to (2) navngivne personer i Bilag A for at sikre dækning selv ved ferier, kurser etc.

## Taktisk niveau

Det taktiske niveau består kun af Taktisk kriseleder, som fungerer som en buffer og kommunikationslag mellem det strategiske og det operationelle niveau. Taktisk kriseleder er ansvarlig for at holde overblikket over igangsatte handlinger og sikre fremdrift, samt rapportere til Kriseledelsen.

## Operationelt niveau

Det operationelle niveau af IT-beredskabet ligger dels hos IT/OT-leverandør(er), i tilfælde af outsourcing af specifikke driftsopgaver, og dels hos egne medarbejdere (Driftsvagt). Det operationelle niveau består af de personer der undersøger mulige årsager til hændelsen og får normal drift genetableret.

# Beredskabets faser



Figur : Beredskabets forskellige faser.

En krisehændelse sker og det registreres lidt efter. Nu aktiveres beredskabet og opgaver uddelegeres (responstid). Det operationelle beredskab går i gang med at re-etablere normal drift evt. med en mellemliggende periode i nøddrift. Når normal drift er genetableret, afsluttes beredskabet og der foretages en opsamling ift. læringspunkter og evt. en endelig afrapportering til relevante myndigheder.

# Reetableringsstrategier

Formålet med en retableringsstrategi er at planlægge, hvordan et system overordnet set retableres i en krisesituation 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).

Recovery Time Objective (RTO) angiver, hvor meget tid der er tolerabel til gendannelse af dine systemer og genetablering af normal funktion efter en krisehændelse. Det svarer på spørgsmålet: “Hvor længe har vi råd til at være nede?” RTO kan evt. forlænges, hvis det er muligt at etablere nøddrift, hvor systemerne fungerer på et operationelt men ikke optimalt niveau.

Recovery Point Objective (RPO) angiver det værste scenario med datatab udtrykt i tid. Det udgør spørgsmål: “Hvor meget data har vi råd til at miste?” RPO er med til at sætte vores back-up strategi.

For de IT- og OT-systemer i , der i risikovurderingen er identificeret som forretningskritiske, er der defineret retableringsstrategier jf. nedenstående tabel.

|  |  |  |  |
| --- | --- | --- | --- |
| System | RTO | RPO | Reetableringsstrategi |
| *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.* |

s konkrete krav til reetableringsmål (RTO, RPO mv.) fremgår af aftalerne med IT- og OT-leverandørerne. 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

# Krisescenarier

I dette afsnit er der en oversigt over de krisescenarier, som anser som mulige konsekvenser ud fra trusselsbilledet, og som IT-beredskabet skal kunne håndtere.

[Det anbefales at præcisere nedenstående 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-2) eller udpege fysiske lokationer, der er særligt kritiske.]

|  |  |
| --- | --- |
| Scenarie | Primære trusler |
| *Forsyningssvigt, hvorved kritiske systemer bliver utilgængelige, og væsentlige opgaver ikke kan løses.* | *Fejlende hardware, fejlende software, naturfænomener, terrorisme, sabotage, menneskelige fejl, malware, hackerangreb* |
| *Brud på fortrolighed af følsomme personoplysninger, hvorved [medarbejdere/forbrugere/kunder] udsættes for risiko for identitetstyveri eller andre væsentlige indskrænkninger i deres handlefrihed.* | *Hackerangreb, konfigurationsfejl, menneskelige fejl, malware* |
| *Svigt af en enkelt komponent i OT-infrastrukturen, som udgør ”single point of failure” (SPOF), hvorved der udløses et krisehændelsesforløb, fx SCADA-anlægget, LDAP.* | *Fejlende hardware, menneskelige fejl, hackerangreb* |
| *Svigt af netværksinfrastruktur, hvorved en hel produktionsmatrikel afskæres fra OT-understøttelse.* | *Fejlende hardware, hackerangreb* |
| *Forsyningssvigt [fx el, gas, flis], 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, sabotage* |

# Implementering af IT-beredskabspolitikken

Kommunikation og implementering i sker efter "top-down" princippet, hvor ledelsen og IT-sikkerhedsfunktionen har ansvaret for at kommunikere videre til de medarbejdere, som indgår i IT-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 krisesituation
* informere IT-beredskabsorganisationen om opdateringer til IT-bereskabsplanen, når det er relevant
* skabe en distributionskanal for den opdaterede IT-beredskabsplan og sikre og forbedre krisehåndteringen.

En god implementering af IT-beredskabsplanen viser sig i en krisesituation, hvor kommunikationen og håndteringen af krisehændelsen:

* 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 reetableringstidsrammen mv.

Bilag A

[Her skriver I navnene på de personer, der kan have de forskellige roller. Det er også disse personer der skal trænes i at have de respektive roller. Det anbefales at der er er mindst to personer, som kan varetage hver rolle, så der er dækning i ferier, ved kurser og andet.]

|  |  |
| --- | --- |
| Rolle | Mulige personer |
| Kriseleder | 1. [*navn*]
2. [*navn*]
 |
| Krisekoordinator | 1. [*navn*]
2. [*navn*]
 |
| Kommunikationsansvarlig | 1. [*navn*]
2. [*navn*]
 |
| Team A | 1. [*navn*]
2. [*navn*]
 |
| Team B | 1. [*navn*]
2. [*navn*]
 |
| … | 1. [*navn*]
2. [*navn*]
 |

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-2)