Skabelon for Kriseberedskabspolitik i energisektoren

Følgende dokument er en skabelon til udarbejdelse af en kriseberedskabspolitik for virksomheder i energisektoren, jf. bekendtgørelse om modstandsdygtighed og beredskab i energisektoren. Kriseberedskabspolitikken 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 bekendtgørelsen for energisektoren (den danske implementering af NIS2).

Vi har i Lakeside lavet en række skabeloner, som du er velkommen til at bruge. Skabelonerne er generelt tiltænkt SMV’er med produktion, men kan sagtens bruges af organisationer uden produktion (OT). Dog er denne skabelon udarbejdet specifikt ift. energisektoren. Skabelonerne er udarbejdet med udgangspunkt i små og mellemstore forsyningsselskaber på niveau 1 og 2.

* IT-sikkerhedspolitik
* IT-sikkerhedshåndbogen
* OT-leverandørpolitik, og leverandør tjeklister
* Risikostyringspolitik og Risikolog
* Hændelseshåndteringsproces og Hændelseslog
* Nærværende kriseberedskabspolitik, -planer og -skabeloner (til hhv. små og mellemstore virksomheder)

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 markeret med gult bør du ændre eller som minimum forholde dig til. Alle tekster markeret med grønt er først krav til niveau 2 virksomheder.
* Kontaktinformation og organisation skal opdateres i sidehoved og sidefod. OBS! Organisation og logo på forsiden er også i en sidefod.

Versionshistorik for skabelon:

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Dato | Ansvarlig | Ændringer |
| 1.0 | 28.01.2025 | MTH | Oprettet første version, som en tilpasning af den mere generelle IT-beredskabspolitik, med sikring af overholdelse af bekendtgørelse om modstandsdygtighed og beredskab i energisektoren, som den har ligget i udkast på Høringsportalen siden 16.12.2024. |
| 1.1 | 27.02.2025 | MTH | Tilpasset efter feedback. Markering af krav som først er relevante for virksomheder på niveau 2 eller over. |
| 1.2 | 01.05.2025 | MTH | Strammet politik. Udskilt fx reetableringsmål til eget dokument. |
| 1.3 | 22.06.2028 | MTH | Tilføjet Bilag A – Plan for beredskabsarbejdet |

Dato | Version x.x

Kriseberedskabspolitik

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. |
| RPO | 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. |
| RTO | 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. |
| 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. |

versions- 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 BestyrelsesformandTlf.: +45 xxxx xxxxxxx@domæne.dk |

Indholdsfortegnelse

[1 Indledning 4](#_Toc201640704)

[1.1 Antagelser 4](#_Toc201640705)

[1.2 Revision & godkendelse 4](#_Toc201640706)

[2 Målsætning 5](#_Toc201640707)

[3 Ansvarsfordeling 5](#_Toc201640708)

[3.1 <Organisation>s ansvar 6](#_Toc201640709)

[3.2 Leverandørers ansvar i <Organisation>s beredskab 6](#_Toc201640710)

[3.3 SaaS-Leverandører 7](#_Toc201640711)

[3.4 Dokumentation 8](#_Toc201640712)

[4 Beredskabsorganisation 8](#_Toc201640713)

[4.1 Roller i beredskab 9](#_Toc201640714)

[4.2 Driftsvagt, sektorberedskab & IT-sikkerhedstjeneste 10](#_Toc201640715)

[5 Beredskabets faser 11](#_Toc201640716)

[6 Reetableringsstrategier 12](#_Toc201640717)

[7 Implementering af beredskabspolitikken 13](#_Toc201640718)

[8 Beredskabsøvelse 13](#_Toc201640719)

[Bilag A - Plan for Beredskabsplanlægning 15](#_Toc201640720)

# Indledning

[Vejledning: denne skabelon er tiltænkt fjernvarmeværker på niveau 1 og 2. Antagelsen i skabelonen er at værket har udliciteret hele eller dele af deres IT- og OT-drift. Skabelonen er opdateret så den tager højde for de krav der fremgår af bekendtgørelse for modstandsdygtighed og beredskab i energisektoren.]

Formålet med denne kriseberedskabspolitik er at fastlægge de overordnede rammer for s arbejde med og implementering af kriseberedskab. Politikken indeholder en beskrivelse af det ønskede niveau for kriseberedskabet og er udtryk for s forventninger og krav til hertil.

Den operationelle udmøntning af politikken beskrives særskilt i beredskabsplanen.

Kriseberedskabsplanen baserer sig på aftaler med leverandører.

Kriseberedskabsplanen indgår i s samlede beredskab, sammen med beredskabsplaner for brand og evakuering etc.

## Antagelser

Kriseberedskabet forventes at fungere effektivt under forudsætning af følgende antagelser:

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

## Revision & godkendelse

Kriseberedskabspolitikken gennemgår årligt review og efterfølgende godkendelse i bestyrelsen. <Organisation>sIT-sikkerhedsfunktion er ansvarlig for det årlige review.

Kriseberedskabsplanen og tilhørende skabeloner gennemgår review og opdatering efter aktivering, og som minimum årligt i overensstemmelse med kriseberedskabspolitikken.

[Vejledning: virksomheder på niveau 2 eller over skal foretage risiko- og sårbarhedsvurdering jf. §18 i bekendtgørelse om modstandsdygtighed og beredskab i energisektoren. Der er ikke krav om risiko- og sårbarhedsvurdering for virksomheder på niveau 1.]

Alle dokumenter i kriseberedskabet kan blive opdateret på baggrund af konklusioner fra risiko- og sårbarhedsvurdering foretaget af <Organisation>, sektorberedskabet eller <Organisation>s leverandører.

For at lette vedligeholdelsen af den skrevne politik og plan er opgaver og aktiviteter placeret i funktionelle enheder eller hos rolleindehavere frem for hos navngivne personer.

# Målsætning

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

Følgende målsætninger skal opfyldes i kriseberedskabet:

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

# Ansvarsfordeling

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

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

## s ansvar

[Vejledning: Man kan ikke som sådan uddelegere ansvaret for sit beredskab, men man kan uddelegere opgaverne. I sidste ende er det dog jeres eget ansvar, at I har valgt nogle gode leverandører, at aftaler er dækkende og jeres medarbejdere er uddannet og trænet i at udføre opgaverne i beredskabet.]

s ledelse har det overordnede ansvar for kriseberedskabet.

 har ansvaret for at sikre forretningskontinuitetsprocedurer for de enkelte afdelinger.

 har ansvaret for at indgå dækkende aftaler med leverandørerne ift. afsnit 3.2.

 har ansvaret for at vedligeholde beredskabsplaner, -skabeloner og -værktøjer, inkl. kontaktlister.

## Leverandørers ansvar i s beredskab

[Vejledning: I det omfang jeres beredskab er afhængigt af eksterne leverandører, skal det sikres at der er indgået aftaler om, hvad deres opgave er, hvor hurtigt de kan reagere, hvor længe det tager at skaffe ressourcer i form af mandskab, reservedele og genetablering, så disse aftaler dækker jeres behov i en krisesituation jf. jeres organisering og evt. risikovurdering. Dvs. at det skal 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.

Herunder er indsat nogle eksempler på ansvarsplacering hos leverandører.]

Vedligehold og support af OT-netværk er outsourcet til leverandør X. Ved en hændelse på netværk er der indgået aftale med leverandør X om 24/7 tilkaldeberedskab med igangsættelses responstid på max 2 timer.

Vedligehold og support af IT-netværk, og enheder på IT-netværket, er outsourcet til leverandør Y. Ved en hændelse på netværk er der indgået aftale med leverandør Y om 24/7 tilkaldeberedskab med igangsættelses responstid på max 2 timer.

For resterende leverandører af komponenter i OT-miljøet er der indgået aftale om service og support i arbejdstimer, og med mulighed for at tilkalde ekstra ressourcer udenfor almindelig arbejdstid mod merbetaling, men uden garanti for opgaveløsning udenfor almindelig arbejdstid.

Alle leverandører er ansvarlige for at orientere <Organisation> om ændringer til kontaktoplysninger ift. henvendelse ved en hændelsessituation.

Alle leverandører er ansvarlige for at orientere <Organisation> om hændelser og aktivering af eget beredskab, i det omfang disse har en effekt på <Organisation>s levering af tjenester, sikkerhed eller overholdelse af indberetningspligt, og at dette foretages uden unødigt ophold og på en måde som understøtter <Organisation>s forpligtigelser.

Det er vigtigt at pointere, at aktivering af s kriseberedskab ikke nødvendigvis aktiverer leverandørens beredskab og vice versa.

## SaaS-Leverandører

[Vejledning: Jeres krav til sikkerhed og tilgængelighed skal opfyldes, også selvom I benytter jer af SaaS leverandører. Det er jeres ansvar at I kun indgår de standardaftaler som stemmer overens med jeres sikkerhedskrav ift. til beskyttelse, placering og genetablering af data, tilgængelighed i det omfang I har behov for, brug af underleverandører, kommunikation i en krisesituation etc. Hvordan får I besked om en hændelse eller krise som påvirker jer, jeres tjenester og jeres brugere? Hvordan får I information om hændelsens omfang således at I kan overholde jeres underretningsforpligtigelser?]

<Organisation> har indgået aftale med en række SaaS-leverandører om brug af forskellige løsninger. Ansvaret for hardware, software, genskabelse, kommunikation etc. ligger alene hos den pågældende SaaS-leverandør i overensstemmelse med den indgåede aftale.

En hændelse hos SaaS leverandøren vil sjældent aktivere <Organisation>s fulde kriseberedskab, 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.

## Dokumentation

[Vejledning: De fleste større organisationer har et system til indrapportering af fejl og planlægning af opgaver. For mindre organisationer kan dette håndteres i en hændelseslog i fx et dokument eller et regneark.]

Dokumentation for hændelser opsamles i <Organisation>s sagsbehandlingssystem/hændelseslog som en del af <Organisation>s procedure for hændelseshåndtering.

Dokumentation for hændelser der aktiverer beredskabet (kriser) opsamles jf. beredskabsplanen.

# Beredskabsorganisation

Den klassiske beredskabsorganisation er delt i tre niveauer: strategisk-, taktisk- og operationelt niveau. For små organisationer som <Organisation>, hvor der er meget personsammenfald mellem det operationelle og det strategiske niveau, giver det ikke mening at se det taktiske niveau, som særskilt niveau, men det er vigtigt at have udpeget en rolle til varetagelsen af kommunikation og koordinering med det operationelle niveau.



Figur : Beredskabsorganisationens niveauer.

Strategisk niveau
Styrer og sætter retning for det aktiverede beredskab med mandat af s ledelse. Det strategiske niveau er ansvarlig for kommunikation ud af beredskabsorganisationen.

Ved aktivering af beredskab udpeges en taktisk kriseleder, somleder og styrer de konkrete opgaver og kommer med forslag og status; dvs. er ansvarlig for kommunikation mellem det operationelle- og det strategiske niveau af beredskabsorganisationen. Taktisk kriseleder er udpeget baseret på det fagområde, der er primært involveret i krisehændelsen.

Rollerne i det strategiske niveau af beredskabet tildeles primært udpegede personer i IT-sikkerhedsorganiseringen angivet i IT-sikkerhedspolitikken. For alle udpegede roller er der dog tillige udpeget en backup, hvis den primære person ikke er tilgængelig. Tildeling af roller fremgår af beredskabsplanen.

Operationelt niveau
Udfører de konkrete opgaver ift. afklaring, nødprocedurer og genetablering. Det operationelle niveau består af medarbejdere (service, support og/eller drift) hos:

* leverandør(er) og/eller
* egne medarbejdere

## Roller i beredskab

[Vejledning: Nedenstående roller dækker alle opgaver i beredskabsorganisationen. I små organisationer kan det være nødvendigt at sammenlægge roller, da opgaverne skal fordeles på færre hænder. Det er vigtigt at opgaverne er entydigt fordelt, så der ikke opstår tvivl om hvem der gør hvad i en krisesituation. Det er også derfor vi anbefaler at man øver sit beredskab, selvom hvis man ikke er underlagt krav om dette for virksomheder under niveau 2.]

Beredskabsorganisationen varetager en række opgaver af meget forskellig karakter, og der er flere forskellige roller, 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. |
| Kommunikationsansvarlig | Ansvarlig for planlægning af kommunikation til interessenter udenfor beredskabsorganisationen: kunder, ansatte, andre samarbejdspartnere, medier og myndigheder. OBS! Ikke nødvendigvis udførende af kommunikationsopgaverne. |
| Taktisk kriseleder | Der er en taktisk kriseleder for hvert fagområde / team. Ansvarlig for at samle op og indrapportere fra berørte områder. Input til konsekvensvurdering, samt indmelding af ressourcer til operationelt niveau.Taktisk kriseleder er ansvarlig for at holde overblikket over igangsatte handlinger og sikre fremdrift (via specialister på operationelt niveau), samt rapportere tilbage til Kriseledelsen for det pågældende fagområde / team.  |
| Specialister | Det operationelle niveau af kriseberedskabet (specialisterne) ligger dels hos 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. De deltager som udgangspunkt ikke i krisemøder, men kan inddrages i det omfang der er behov for faglige input. |

Medarbejdere udpeges og trænes i at varetage ovenstående aktørroller. Alle roller skal være tildelt mindst to (2) navngivne personer i beredskabsplanen for at sikre dækning ved ferier, kurser etc.

## Driftsvagt, sektorberedskab & IT-sikkerhedstjeneste

[Vejledning: for virksomheder på niveau 2 og over er der krav om brug af en IT-sikkerhedstjeneste. For energisektoren kan SektorCERT opfylde de fleste af opgaverne og kravene som stilles til en IT-sikkerhedstjeneste. Virksomhederne er dog ansvarlige for at sikre, at der stilles de nødvendige krav til deres IT-sikkerhedstjenesteleverandør, og at virksomheden løbende følger op på og kontrollerer, at IT-sikkerhedstjenesten opfylder de krav, der er blevet stillet til dem.]

 har en etableret driftsvagt som er bemandet 24/7. Driftsvagten modtager information om alle hændelser, store og små. Driftsvagten udbedrer de hændelser der kan udbedres med det samme, eller tager beslutning om uddelegering af opgaver til leverandører, henlæggelse til almindelig arbejdstid eller aktivering af beredskab.

Sektorberedskab og IT-sikkerhedstjeneste kontakter via driftsvagten. Driftsvagten iværksætter hændelseshåndtering og aktiverer evt. kriseberedskabet.

Sektorberedskabsforanstaltninger kan aktiveres gennem kriseledelsen jf. beredskabsplanen.

# 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.

Der afrapporteres til relevante myndigheder løbende, samt via en opsamling efter afslutning af beredskabet.

# 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).

For de IT- og OT-systemer (inkl. netværk og anlæg) i , der er identificeret som forretningskritiske, er der defineret retableringsmål og -strategier jf. dokumentet ”Reetabeleringsmål\_<organisation>”. Reetablering sker som udgangspunkt i normal arbejdstid, medmindre andet er aftalt.

For systemer og anlæg hvor der er en aftale om vedligehold (serviceaftale) med leverandører, eller hvor der er tale om leverandørens egne systemer og enheder installeret på s netværk, fremgår s konkrete krav til reetableringsmål (RTO, RPO mv.) af leverandøraftalerne.

Løbende kontrol af om leverandøren kan efterleve disse krav udføres jf. de konkrete aftaler og består af en eller flere af følgende kontroller:

* Opfølgning på overholdelsen af SLA-aftaler og aftaleforhold, der forpligter leverandører til et højt kvalitets- og sikkerhedsniveau (fx efterlevelse af ISO-standarder)
* Gennemgang af periodevise revisionserklæringer udarbejdet af tredjepart
* Periodiske test og målinger udført af på egne netværk, eller af leverandøren selv på sine netværk
* Opfølgning på og rapportering af hændelser

Reetableringsmålene er blevet sat ud fra arbejde med Energistyrelsens udmeldte risiko- og sårbarhedsscenarier i Scenariekatalog til ROS 2025. For niveau 2 fjernvarmeselskaber er der 10 obligatoriske scenarier, samt krav om af fjernvarmeselskabet selv udvælger minimum 3 scenarier fra det resterende katalog. ROS-scenarierne dækker både klassiske beredskabssituationer og cybersikkerhed.

# Implementering af 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 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 kriseberedskabsplan, hvad den indeholder, og hvordan den vil kunne påvirke medarbejderen i en krisesituation
* informere beredskabsorganisationen om opdateringer til kriseberedskabsplanen, når det er relevant
* skabe en distributionskanal for den opdaterede kriseberedskabsplan og sikre og forbedre krisehåndteringen.

En god implementering af kriseberedskabsplanen 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.
* sikrer overensstemmelse med sektorberedskabsplanen for delsektor(er) som <Organisation> opererer indenfor.

# Beredskabsøvelse

[Vejledning: virksomheder på niveau 2 eller over skal foretage øvelser og funktionstest af beredskabet jf. §20-23 i bekendtgørelse om modstandsdygtighed og beredskab i energisektoren. Der er ikke krav om beredskabsøvelser for virksomheder på niveau 1 – men vi anbefaler at I gør det alligevel, da det både sikrer at alle involverede parter ved hvad de skal gøre i en krisesituation, samt at I finder evt. mangler og uhensigtsmæssigheder i jeres beredskabsplan før i står i krisen. I Bekendtgørelsen er der krav til at virksomheder på niveau 2 skal øve deres beredskab hvert 2. år, og niveau 3-5 skal øve hvert år.]

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

<Organisation> har udarbejdet en øvelsesplan, som hen over en femårig periode tester alle de øvelseselementer som er påkrævet fra Energistyrelsen. Øvelsesplanen er tentativ og opdateres mindst én gang årligt, og ved væsentlige ændringer i <Organisation>s organisation, fysisk sikkerhed, anlæg, leverandører, IT- eller OT.

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 kriseberedskabet for en mindre hændelse, der normalt ikke vil afstedkomme en aktivering af beredskabet.

Øvelsesplanen sikrer at der afholdes beredskabsøvelse, som minimum hvert andet år, dog skal der årligt gennemføres funktionstest af teknisk udstyr, som indgår i beredskabet.

Øvelseselementer kan ses som gennemført, efter godkendelse fra Energistyrelsen, hvis kriseberedskabet har været aktiveret, og de pågældende øvelseselementer har været aktiveret og dermed afprøvet på en virkelig hændelse.

Øvelserne foretages, dokumenteres og evalueres i en øvelsesevalueringsrapport, som indsendes til Energistyrelsen, senest tre måneder efter, at øvelsen er afholdt.

Konklusioner fra øvelser og test indgår i risiko- og sårbarhedsvurderings arbejdet, og kan føre til ændringer i alle politikker og procedurer, inkl. kriseberedskabsdokumentationen.

# Bilag A - Plan for Beredskabsplanlægning

Dette bilag indeholder planen for beredskabsplanlægning i . Rollen der står understreget, er ansvarlig for gennemførelsen af aktiviteten.

[Vejledning: tilpas tabellen efter jeres behov. Forslag er indsat med gul tekst, men de er blot forslag. Sæt en realistisk kadence som både giver tid til at opgaverne udføres, og samtidig sikrer fremdrift.]

| Aktivitet | Kadence | Deltagere | Indhold |
| --- | --- | --- | --- |
| Status for beredskab | Minimum fire gange årligt som et punkt på bestyrelsesmøde | * Beredskabskoordinator
* Bestyrelsen
 | Orientering om status beredskabsarbejdet siden sidste møde. |
| Gennemgang af beredskabsmateriale* Beredskabspolitik
* Beredskabsplan
* Understøttende materiale
* Øvelsesplan
 | Hvert år fx efter en årlig risikostyringsworkshop.1. Koordineringsmøde
2. Indmelding
 | * Beredskabskoordinator
* Nødprocedure- og værktøjsansvarlige repræsentanter
 | Beredskabskoordinator sikrer at der bliver indkaldt til et koordineringsmøde med alle der er ansvarlige for dele af beredskabet. Koordineringsmødet igangsætter arbejdet og forventningsafstemmer opgaven (deadlines, scope etc.).Beredskabsmaterialet opdateres desuden ad hoc ved opdagelsen af forbedringspunkter.  |
| Review og godkendelse af beredskabspolitik | Hvert år efter gennemgang og evt. opdatering | * Beredskabskoordinator
* Bestyrelsen
 | Beredskabskoordinatoren sikrer at bestyrelsen er klædt på til at kunne lave review og godkende beredskabspolitikken. Godkendelse noteres i referat fra bestyrelsesmøde og versionshistorikken i beredskabspolitikken opdateres. |
| Godkendelse af beredskabsplan ved Energistyrelsen | Hvert 3. år, deadline for indsendelse 1. oktober | * Beredskabskoordinator
* Energistyrelsen
 | Bestyrelsesgodkendt beredskabspolitik og beredskabsplan sendes ind til Energistyrelsen til godkendelse. |
| Godkendelse af øvelsesevaluering ved Energistyrelsen | Hvert 2. år, senest 3 mdr. efter afholdt beredskabsøvelse | * Beredskabskoordinator
* Energistyrelsen
 | Bestyrelsesgodkendt beredskabsøvelsesevaluering sendes ind til Energistyrelsen til godkendelse. |