



Energistyrelsen

Vejledning: Udarbejdelse af beredskabsplaner for niveau 2-5-virksomheder

Checkskema

Kontor/afdeling
Beredskab

Dato
06-07-2026



Energistyrelsen

Energistyrelsen

Carsten Niebuhrs Gade 43
1577 København V

T: +45 3392 6700
E: ens@ens.dk

www.ens.dk



Versionshistorik

Versi- ons-nr.	Ændret	Ændret af	Kommentarer
1	15.05.2025	Magnus W. Ege- bjerg	Vejledningen blev oprettet.
1.1	17.11.2025	Stine Buemann	Tydeliggørelse af fortrolighedsgrad i materialet i sidefod og på forsiden. Konsekvensændring af 'BEK' til 'bekendtgørelsen'.
1.2	22.05.2026	Stine Buemann	Henvi sning til vejledningen i an- søgning om samordnet beredskab på side 10.
1.3	06.07.2026	Stine Buemann	Fortrolighedsstempel fjernet.



Indhold

Indledning	4
Generelt	4
Indholdet i beredskabsplanerne	4
Krav i bekendtgørelsen (§ 19).....	5



Indledning

Virksomhederne i el-, gas-, brint-, olie-, fjernvarme- og fjernkølingssektoren skal, jf. bekendtgørelse om modstandsdygtighed og beredskab i energisektoren nr. 260 af 6. marts 2025 (bekendtgørelsen), § 19, have en eller flere beredskabsplaner, procedurer og instrukser for håndtering af hændelser og styring af kriseindsatsen.

Denne vejledning er målrettet niveau 2-5-virksomheder i energisektoren. Vejledningen er udformet som et checkskema, som lister minimumskravene til disse virksomheders beredskabsplaner. De første to kolonner fortæller, hvad bekendtgørelsens krav er, og den tredje hvad Energistyrelsen anbefaler, at I overvejer. Den fjerde kolonne kan virksomheden bruge til at notere, hvor de konkrete krav findes i virksomhedens eget beredskabsmateriale.

Som supplement til denne vejledning har Energistyrelsen udarbejdet en række mere detaljerede vejledninger og værktøjer til konkrete beredskabsemner som fx risiko- og sårbarhedsanalyse, hændelsesindberetning, iværksættelse af sektorberedskabsforanstaltninger mv., som kan findes på Energistyrelsens lukkede beredskabssite.

Generelt

Beredskabsarbejdet handler om:

- At forebygge, at hændelser medfører alvorlige problemer for virksomheden og samfundet.
- At reducere omfanget af skader og konsekvenser, hvis der opstår hændelser.
- At nå en stabiliseret og normal tilstand så hurtigt som muligt.

Beredskabsplanerne er i forlængelse heraf operative vejledninger eller instrukser, som virksomhedens medarbejdere hurtigt skal kunne tage i anvendelse, når en beredskabssituation bliver varslet eller opstår. Formålet er at sikre driftskontinuiteten, og at virksomheden kan overholde sine underretningsforpligtelser i forbindelse med en hændelse.

Indholdet i beredskabsplanerne

Når Energistyrelsen vurderer en beredskabsplan, lægger sagsbehandlerne vægt på, at planen virker overskuelig og operationel. Planen skal kunne forstås og anvendes i praksis af de medarbejdere, der skal kunne håndtere en hændelse. Derfor er det afgørende, at de relevante parter (medarbejdere, centrale leverandører, ledere mv.) har været involveret i udarbejdelsen og kvalitetssikringen af planen.



Det er desuden en god idé, at det fremgår af planen, hvilke love og bekendtgørelser planen skal leve op til, og hvad formålet med planen er. Er det fx et indeks over action cards og detailplaner, et flowdiagram, en manual eller lign.? Det bør også fremgå af planen, hvornår og hvor hyppigt I planlægger at opdatere materialet.

Bekendtgørelsen stiller ikke krav til formen på planerne, men lister en række konkrete krav til indholdet i beredskabsplanerne:

Krav i bekendtgørelsen (§ 19)

Bekendtgørelsens krav til beredskabsplanens indhold	§	Uddybning	Hvor og hvordan er emnet behandlet?
Ledelsesgodkendt Er planerne godkendt af virksomhedens ledelse?	19, stk. 1	Hvem, der udgør <i>ledelsesorganet</i>, skal forstås i overensstemmelse med definitionerne af henholdsvis 'det centrale ledelsesorgan' i selskabsloven¹ og 'ledelsen' i LEV-loven². Ifølge selskabsloven er det centrale ledelsesorgan: • Bestyrelsen i selskaber, der har en direktion og en bestyrelse. • Direktionen i selskaber, der alene har en direktion. • Direktionen i selskaber, der både har en direktion og et tilsynsråd. <i>Ledelsen</i> er i LEV-loven medlemmer af en bestyrelse, direktion eller et tilsvarende ledelsesorgan. Det vil være op til den enkelte virksomhed at vurdere deres virksomhedskonstruktion i forhold til selskabsloven og LEV-loven. Bemærk, at dette kun gælder ved større og væsentlige ændringer i planen samt de opdateringer, som I laver med et eller tre års	

¹ Bekendtgørelse af lov om aktie- og anpartsselskaber (selskabsloven) nr. 331 af 20. marts 2025.

² Bekendtgørelse af lov om visse erhvervsdrivende virksomheder (erhvervsvirksomhedsloven) nr. 330 af 20. marts 2025.



		mellemrum. Små rettelser, som laves undervejs for at holde dokumentet levende og opdateret, fx ændringer i kontaktnumre mv., er ikke nødvendige at få ledelsesgodkendt ³ .	
Intern rolle- og ansvarsfordeling Har I etableret en vagtordning?	19, stk. 2, pkt. 1	I skal sikre, at der altid og uanset hændelsens karakter er en person tilgængelig, som kan modtage varsler og sætte gang i relevante tiltag til håndtering af en hændelse.	
Har I etableret en krisestab eller krisestyringsorganisation?	19, stk. 2, pkt. 1	Har I planer for, hvordan I eskalerer håndteringen af en hændelse? Har I beskrevet, hvem der har mandat til at træffe hvilke beslutninger? Hvem skal have hvilke roller i krisestaben? Hvad gør I, hvis krisen strækker sig over længere tid eller foregår i døgndrift?	
Aktivering af yderligere ressourcer og materiel Har I taget stilling til, hvordan I aktiverer yderligere ressourcer og materiel?	19, stk. 2, pkt. 2	Har I en plan for, hvordan I indkalder ekstra mandskab, hvis der bliver behov for det? Har I overblik over, hvor I kan skaffe nødvendige reservedele, og hvor lang leveringstiden er på dem? Har I evt. aftaler med andre virksomheder eller kontrakter med leverandører, som I kan hente ressourcer fra? Hvordan koordinerer I med andre aktører, hvis I trækker på de samme ressourcer?	
Operationel ansvarsfordeling Har I taget stilling til den operationelle ansvarsfordeling i håndteringen af en hændelse?	19, stk. 2, pkt. 3	Har I aftalt med jeres samarbejdspartner og leverandører, hvem der skal gøre hvad under en hændelse? Det kan fx være ved samordnet beredskab, it-leverandører (inklusive it-sikkerhedstjenesten), eksterne vagtfirmaer mv.	
Kontaktoplysninger Er der en kontaktiliste i beredskabsplanen?	19, stk. 2, pkt. 4	Listen bør inkludere de relevante personer og funktioner både i og uden for organisationen. Ud over krisestaben, det operationelle kontaktpunkt (jf. § 73) og beredskabs-, system- og driftsansvarlige kan det fx være politi, brandvæsen, centrale leverandører mv.	

³ Læs evt. mere om ledelsens rolle og ansvar, samt hvordan ledelsesbegrebet er defineret, i Q & A på www.ens.dk.



		Det kan også være til medier eller andre interessenter, som vil have nytte af information om uregelmæssigheder i driften. Overvej også, om kontaktlisten skal inkludere både primære og sekundære kontakter.	
Kriterier for aktivering af krisestaben Har I beskrevet, hvornår krisestaben skal aktiveres?	19, stk. 2, pkt. 5	Beskriv, hvornår en hændelse er alvorlig eller omfattende nok til, at I ikke kan håndtere den inden for almindelig drift. Hvilke kriterier skal være opfyldt, før I eskalerer jeres håndtering af en hændelse? Det kan fx være hændelsens forventede varighed, påvirkning på forsyningen eller forsyningskritiske systemer, involverede aktører, medieinteresse eller personskaade. Er der eventuelt forskellige trin i eskaleringen? Beskriv også, hvad der skal til for at deeskalere krisehåndteringen.	
Procedurer Beredskabsplanerne skal indeholde en række relevante procedurer.	19, stk. 3	Forhold jer til, om de procedurer, der nævnes nedenfor, er relevante for jeres virksomhed. Hvis de er det, skal de indgå i jeres beredskabsplan, være konkrete, operationelle og letforståelige. Det skal være tydeligt, hvem der har ansvar for hvad.	
Etablering af alternative driftsformer Hvordan overgår I til manuel drift?	19, stk. 3, pkt. 1	Fortæl, om I har mulighed for at overgå til manuel drift. Hvad gør I fx ved nedbrud i SCADA? I skal beskrive, hvad kriterierne er for, at I overgår til nødprocedurer og fx skifter til et redundant net- og informationssystem. Beskriv også, hvordan I gør det.	
Isolering af systemer Har I procedurer for, hvordan I isolerer industrielle kontrolsystemer og operationelle teknologier fra virksomhedens øvrige net- og informationssystemer?	19, stk. 3, pkt. 2	Beskriv kriterierne for, hvornår I overgår til it-teknisk ø-drift, og hvordan I gør det. Har I på forhånd defineret, hvilke systemer der fysisk og logisk skal adskilles fra hinanden under en isolation? Hvem har lov til at aktivere planen, og hvem skal informeres?	



		Har I fx markeret, hvilke kabler i jeres rack-skabe, der skal hives ud for at isolere specifikke IT-miljøer? Resultater isoleringen i, at visse arbejds-gange bliver manuelle, eller at nogle stationer skal bemandes, fx hvis det ikke længere er muligt at fjernstyre? Hvordan sikrer I, at isolationen ikke kompromitterer andre sikkerhedskritiske funktioner som fx alarmer og nødstopssystemer?	
Genoprettelse af anlæg Hvordan genetablerer I til normal drift efter et nedbrud på et anlæg?	19, stk. 3, pkt. 3	Beskriv, hvordan I genopretter driften efter et nedbrud i eller en hændelse på jeres anlæg. Hvordan sikrer I, at det sker sikkert og kontrolleret? Hvordan og hvor hurtigt forventer I at kunne hente ressourcer, mandskab og reservedele? Det gælder både på anlægget som helhed, eller hvis der er nedbrud på de dele af anlægget, som I er afhængige af for at kunne levere tjenesten. Har I fx en "midlertidig driftstilstand", som I kan anvende, indtil de normale systemer eller anlæg er genetableret?	
Fremskaffelse af kritiske reservedele Har I en procedure for at fremskaffe kritiske reservedele?	19, stk. 3, pkt. 4	Fortæl, om I fx har et reservedelslager, eller om I har leverandører, som I forventer at kunne købe reservedele hos i en nødsituation. Det kan også være, at I har en aftale med andre, lignende virksomheder om, at I låner materiel af hinanden.	
Net- og informationssystemer Hvordan genopretter I jeres net- og informationssystemer?	19, stk. 3, pkt. 5	I skal redegøre for, hvor lang tid I kan leve med, at jeres systemer er ude af drift eller ikke kan tilgås. I skal vide, hvilke net- og informationssystemer der er kritiske for jeres drift. Dernæst skal I lave en prioriteret liste over, hvilke systemer der skal genetableres først. Hvor meget data kan I tåle at tabe, før det går ud over jeres evne til at drifte? Hvilke	



		backup-løsninger har I, og hvor ofte opdateres de? Hvor hurtigt kan data gendannes? Hvad er jeres målsætning for nedetid, og hvordan vil I genetablere systemerne? Forklar, hvem der har ansvaret for at sætte gang i genetableringen, og hvilke samarbejdsparter eller leverandører I eventuelt har brug for at involvere. Hvilke betingelser skal være opfyldt, før I genetablerer systemerne? Hvordan sikrer I jer, at I genetablerer systemerne sikkert? Scanner I fx for malware, inden I genetablerer?	
Iværksættelse af beredskabsforanstaltninger Har I beskrevet de beredskabsforanstaltninger, I kan iværksætte i forbindelse med en hændelse?	19, stk. 3, pkt. 6	Her menes der både jeres egne, interne foranstaltninger, fx til beskyttelse af anlæg og systemer, og de sektorberedskabsforanstaltninger, som Energistyrelsen melder ud. Bemærk, at I skal beskrive, hvad I gør rent lavpraktisk ved hver foranstaltning. Hvordan oversætter I sektorberedskabsforanstaltningerne til de lokale forhold? Hvad gør I hos jer? Og hvem gør hvad?	
Alternative kommunikationslinjer Hvad er jeres alternativ til de normale kommunikationsformer?	19, stk. 3, pkt. 7	I skal sikre jer, at I kan udveksle driftskritisk information såvel internt som med eksterne parter, selv når der er nedbrud i de kommunikationskanaler, I anvender til dagligt. Har I fx SINE? Er der redundans på jeres telefon- og internetforbindelser? Har I aftalt med jeres samarbejdsparter, hvordan I kommer i kontakt med hinanden? Hvordan får I fat i jeres kollegaer, hvis telefonnettet er nede?	
Dokumentation af håndtering af hændelse Hvordan dokumenterer I jeres håndtering af hændelser?	19, stk. 3, pkt. 8	Hvordan dokumenterer I jeres håndtering af hændelser undervejs? Har I systemer til logføring? Gør I det manuelt eller digitalt? Hvor ofte opdaterer I jeres logs?	



Intern kommunikation Hvordan deler I viden i forbindelse med en hændelse?	19, stk. 3, pkt. 9	Hvordan sikrer I jer, at jeres medarbejdere ved (tilstrækkeligt) om en given hændelse? Ved medarbejderne hvor og til hvem, de skal afgive relevant information? Ved medarbejderne, hvad de skal gøre, hvis de får ny viden om hændelsen udefra?	
Ekstern kommunikation Hvordan deler I viden i forbindelse med en hændelse?	19, stk. 3, pkt. 10	Har I en plan for, hvordan I informerer myndighederne (Energistyrelsen, politi, brandvæsen, kommuner mv.), forbrugere, samarbejdspartner medier mv. om en hændelse? Har I fx en skabelon til, hvad I kommunikerer og til hvem? Ved I på forhånd, hvilken rækkefølge I skal kontakte interessenterne i? Hvordan gør I brug af fx hjemmesider og telefonsvarer? Har I fx et action card til, hvordan man lægger information på jeres hjemmeside eller indtaler en besked på virksomhedens telefonsvarer?	
Sektorberedskabsplanen Har I indarbejdet den eller de relevante delsektorplaner i jeres planmateriale?	19, stk. 4	I skal sikre jer, at jeres beredskabsplaner stemmer overens med den eller de relevante sektorberedskabsplaner ⁴ . Har I fx indarbejdet beskrivelserne af de forhold, der vedrører modtagelse af varsler om trusler generelt? Og om iværksættelse af sektorberedskabsniveauer og –foranstaltninger? Fremgår det, hvordan I skal indberette hændelser? Der kan også være detailinstrukser i den eller de delsektorplaner, der omfatter jer, som I bør indarbejde i jeres egne planer.	

⁴ Læs mere om hvilke sektorberedskabsplaner, der er relevante ved samordnet beredskab, i vejledningen 'Ansøgning om samordnet beredskab', som kan findes på www.ens.dk samt Energistyrelsens lukkede beredskabssite.



		Det kan i den forbindelse også være relevant, at I redegør for virksomhedens operationelle kontaktpunkt (jf. § 73), herunder for kontaktinformation og bemanding.	
Versionsstyring Er beredskabsplanen versionsstyret?	19, stk. 5	Beredskabsplanen skal indeholde en beskrivelse af versionshistorikken. Det skal fremgå, hvornår planen sidst er ændret, og hvad der er ændret. Det bør også være tydeligt, hvem der har revideret planen.	
Risiko- og sårbarhedsvurdering Er resultaterne indarbejdet i planerne?	19, stk. 6	Beredskabsplanen skal tage højde for konklusionerne på jeres risiko- og sårbarhedsvurdering (§ 18). Husk, at det både gælder konklusionerne på Energistyrelsens ROS-scenarier⁵ og virksomhedens øvrige overvejelser om og processer for identifikation af risici, som kan forstyrre eller forhindre jeres mulighed for at levere tjenesten. Det kan fx også være i forlængelse af jeres evaluering af øvelser og hændelser. Har I indarbejdet de tiltag og foranstaltninger, I har vedtaget efter seneste risiko- og sårbarhedsvurdering? Efter hver revurdering af risici og sårbarheder skal I forholde jer til, om fundene giver anledning til ændringer i jeres beredskabsplaner.	

⁵ Bemærk, at niveau 2-virksomheder kun skal analysere ti obligatoriske scenarier plus tre valgfrie scenarier, jf. Energistyrelsens *Vejledning i risiko- og sårbarhedsanalyse*. Alt ROS-materialet kan findes på Energistyrelsens lukkede beredskabs-site.