Lovtidende A

2018

Udgivet den 5. maj 2018

25. april 2018. Nr. 424.

Bekendtgørelse om beredskab for oliesektoren[1)]

I medfør af § 3, § 13, stk. 3, § 16, stk. 3, § 17, stk. 5, § 21, stk. 5 og § 23, stk. 2, i lov nr. 354 af 24. april 2012 om olieberedskab, fastsættes efter bemyndigelse i henhold til § 4, stk. 1, i bekendtgørelse nr. 1512 af 15. december 2017 om Energistyrelsens opgaver og beføjelser:

Generelle bestemmelser

§ 1. Denne bekendtgørelse har til formål at fastsætte regler om beredskab, herunder it-beredskab, for virksomheder, der er kritiske for forsyning af råolie og olieprodukter til slutbrug i Danmark i en beredskabssituation og andre ekstraordinære situationer, således at forsyningen til det danske samfund i videst muligt omfang kan opretholdes og videreføres.

§ 2. Denne bekendtgørelse finder anvendelse på:

1) Lagringspligtige virksomheder efter olieberedskabsloven, som har en lagringspligtig omsætning større end nul.
2) Den centrale lagerenhed efter olieberedskabsloven.

Stk. 2. Virksomheder omfattet af stk. 1, nr. 1, og den centrale lagerenhed skal have det fornødne beredskab. Herved forstås, at virksomheden skal foretage planlægning og træffe foranstaltninger for at sikre forsyningen fra egne beredskabslagre til slutbrug i en beredskabssituation og andre ekstraordinære situationer. I denne planlægning skal indgå alle forsyningskritiske processer og forsyningskritisk infrastruktur, der har betydning for, at virksomhedens produkt når til slutbrug i Danmark.

Stk. 3. Virksomhedernes og den centrale lagerenheds beredskabsarbejde skal indgå i planlægnings- og driftsopgaver vedrørende virksomhedernes olieforsyning med henblik på:

1) at reducere olieforsyningens sårbarheder og risici,
2) at sikre et hensigtsmæssigt beredskab over for disse sårbarheder og risici,
3) at sikre en koordineret og effektiv krisehåndtering og
4) at sikre den nødvendige kommunikation og informationsudveksling i forbindelse hermed.

Definitioner

§ 3. I denne bekendtgørelse forstås ved:

1) Beredskab: Foranstaltninger, processer og det arbejde, der skal forhindre, begrænse eller håndtere forsyningssvigt som resultat af nedbrud eller forstyrrelser, herunder fjendtlige handlinger, i forsyningskritiske processer eller forsyningskritisk infrastruktur, herunder it-systemer.
2) Slutbrug: Råolie eller olieprodukter anvendt til forbrug i Danmark.
3) Forsyningskritisk proces: Proces, der er nødvendige for forsyning til slutbrug.
4) Forsyningskritisk it-system: Et it-system, der styrer eller i væsentligt omfang påvirker forsyningskritiske processer.
5) Hændelse: En hændelse, hvor et nedbrud i eller angreb på et fysisk forsyningskritisk anlæg i væsentligt omfang aktiverer virksomhedens almene beredskab.
6) It-sikkerhedshændelse: En hændelse, hvor et nedbrud i eller angreb på et forsyningskritisk it-system i væsentligt omfang aktiverer virksomhedens it-beredskab.
7) Varsel: Melding om forhold af betydning for lagringspligtige virksomheders forsyning af olieprodukter til slutbrug, uagtet hvem der er afsenderen. Afsenderen af varslet kan være en anden lagringspligtig virksomhed, private sikkerhedsvirksomheder eller en myndighed.
8) Forsyningskritisk infrastruktur: Lagre, rørledninger eller terminaler, som anvendes af de lagringspligtige virksomheder eller den centrale lagerenhed til olieforsyning til slutbrug.
9) Råolie: Mineralolie af naturlig oprindelse, der består af kulbrinter og forskellige urenheder såsom svovl. Råolie forekommer i flydende form ved normal temperatur og normalt tryk. og har varierende fysiske egenskaber. Råolie omfatter også kondensat, der udvindes af associeret og ikkeassocieret gas i tilknytning til indvindingen og blandes med råolie, og halvfabrikata, der har gennemgået en raffineringsproces og skal gennemgå yderligere processer, inden de bliver til endelige olieprodukter.

[1)] Bekendtgørelsen indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net-og informationssystemer i hele Unionen, EU-Tidende 2009, nr. L 194, s. 1.

CI000448

Energi-, Forsynings- og Klimamin.,
Energistyrelsen, j.nr. 2017-1546

10) Olieprodukter: Produkter, der er fremstillet ved raffinering af råolie, og additiver eller biobrændstoffer, der tilsættes eller iblandes disse produkter.
11) Virksomheder: Virksomheder omfattet af § 2, stk. 1, nr. 1.

Koordinerende og operative forhold omkring beredskabet

§ 4. Virksomhederne og den centrale lagerenhed, er ansvarlige for eget beredskab, herunder at planlægge og administrere tiltag i egen organisation, samt indgå aftaler med andre virksomheder, der har indflydelse på virksomhedens beredskab efter § 2 stk. 2.

Stk. 2. Virksomheder og den centrale lagerenhed, der af geografiske eller tekniske årsager er afhængige af forsyningskritisk infrastruktur, der opereres eller ejes af andre virksomheder eller tredjeparter, i varetagelsen af sin egen tjeneste skal sikre, at denne afhængighed ikke medfører komplikationer for virksomhedens operative og planlægningsmæssige opgaver, der skal sikre den fortsatte drift af forsyningskritiske processer og forsyningskritiske it-systemer.

Stk. 3. Virksomheder, der alene er afhængige af forsyningskritisk infrastruktur, som ejes eller opereres af andre virksomheder, den centrale lagerenhed eller tredjeparter, kan ved ansøgning til Energistyrelsen fritages for beredskabsplanlægning efter denne bekendtgørelse, såfremt det kontraktmæssigt kan godtgøres, at den pågældende virksomhed varetager denne opgave i overensstemmelse med reglerne i denne bekendtgørelse og underkaster sig Energistyrelsens tilsyn.

Stk. 4. Ansøgningen sendes skriftligt til Energistyrelsen og skal som minimum indeholde:
1) En beskrivelse af de praktiske forhold, der tilsiger, at en anden virksomhed skal varetage beredskabsplanlægningen.
2) De relevante kontrakter, der dokumenterer, at virksomheden, den centrale lagerenhed eller tredjeparten påtager sig at overholde og varetage forpligtigelserne i denne bekendtgørelse og samtidig underkaster sig Energistyrelsens tilsyn med overholdelsen heraf.

Stk. 5. Energistyrelsen har 6 uger fra modtagelsen af ansøgningen til at træffe afgørelse herom. Afgørelsen skal meddeles skriftligt til ansøgeren.

Organisatoriske forhold

§ 5. Virksomhederne og den centrale lagerenhed skal sikre, at beredskabsarbejdet baseres på alle risici, således at virksomhedens ledelse har et samlet risikobillede, der repræsenterer kendte og mulige risici, og som kan forhindre, at virksomhedens produkt når til slutbrug.

§ 6. Virksomhederne og den centrale lagerenhed skal organisere beredskabet, således at det sikres, at virksomheden kan modtage varsler af teknisk karakter fra andre virksomheder og myndighederne. Virksomhederne skal på baggrund af egne risiko- og sårbarhedsvurderinger etablere den fornødne organisering, der kan iværksætte relevante tiltag ved modtagelse af et varsel.

Stk. 2. Virksomhederne og den centrale lagerenhed skal sikre, at beredskabsarbejdet organiseres, således at de i akutte situationer er i stand til at kommunikere med relevante samarbejdsparter for at genoprette forsyningen af eget produkt til slutbrug.

Stk. 3. Såfremt virksomheden eller den centrale lagerenhed er afhængig af anden virksomheds eller tredjeparts ydelser eller bistand for at organisere beredskabet eller sikre forsyningen, skal virksomheden eller den centrale lagerenhed tilsikre at have etableret de fornødne procedurer og aftaler med denne virksomhed eller tredjepart til fortsat at kunne sikre beredskabet og forsyningen.

§ 7. Energistyrelsen kan vejlede virksomhederne i forbindelse med etablering af procedurer for modtagelse af varsler og etablering af tiltag.

Risiko- og sårbarhedsvurderinger

§ 8. Virksomheder og den centrale lagerenhed skal udarbejde en vurdering af alle de risici og sårbarheder, der kan påvirke virksomhedens forsyning fra egne beredskabslagre i en beredskabssituation eller anden ekstraordinær situation, første gang senest 1. oktober 2018.

Stk. 2. Risiko- og sårbarhedsvurderinger skal indeholde alle relevante forhold, herunder egne erfaringer fra øvelser og hændelser, jf. §§, 13 og 15, samt varsler og det aktuelle trusselsniveau vurderet af myndighederne inden for såvel it-trusler, terrortrusler og andre trusler.

Stk. 3. Risiko- og sårbarhedsvurderinger skal som minimum indeholde:
1) Identifikation af alle risici af betydning for virksomhedens forsyning.
2) Identifikation af virksomhedens sårbarheder.
3) Vurdering af konsekvenserne for virksomheden og for forsyningen ved en hændelse, hvor sårbarheden udsættes for risikoen.
4) Identificerede tiltag, der har til hensigt at nedbringe sandsynligheden eller konsekvensen af identificerede risici.

Stk. 4. Risiko- og sårbarhedsvurderinger skal udarbejdes med inddragelse af relevante personer i organisationen.

Stk. 5. Risiko- og sårbarhedsvurderingen skal opdateres senest 3 måneder efter, at nye trusler erkendes samt ved væsentlige ændringer af forsyningskritiske anlæg, processer eller it-systemer. Virksomhederne skal på forlangende kunne dokumentere, hvordan og hvornår risiko- og sårbarhedsvurderingen er opdateret.

Stk. 6. Energistyrelsen kan skriftligt meddele virksomhederne, at der skal foretages risiko- og sårbarhedsvurderinger efter konkrete scenarier eller trusler, der vurderes relevante på baggrund af erfaringer eller meddelelser fra andre virksomheder, myndigheder eller sektorer.

§ 9. Virksomheder og den centrale lagerenhed skal underrette Energistyrelsen, såfremt de under risiko- og sårbarhedsvurderingen efter § 8 har konstateret:
1) at være afhængige af et forsyningskritisk it-system, og
2) en hændelse i dette forsyningskritiske it-system vil få væsentlige forstyrrende virkninger for leveringen af rå-

olie eller olieprodukter i en beredskabssituation eller anden ekstraordinær situation.

Stk. 2. Underretningen skal ske skriftligt senest 2 måneder efter gennemførelse af risiko- og sårbarhedsvurderingen, dog første gang inden 1. oktober 2018.

Planmateriale for forsyningskritiske it-systemer

§ 10. Virksomheder og den centrale lagerenhed, der opfylder kriterierne beskrevet i § 9 stk. 1, skal udarbejde planmateriale over egne forsyningskritiske it-systemer. Planmaterialet skal indeholde:

1) Beskrivelse af afhængighed af andre virksomheder, den centrale lagerenhed og tredjeparter.
2) Identificering af den driftskritiske kommunikation eller informationsudveksling, med andre virksomheder, den centrale lagerenhed, andre tredjeparter eller slutbrug.
3) Beskrivelse af forsyningskritiske it-systemer, herunder hvilke systemer de forsyningskritiske it-systemer er afhængige af.
4) Mulighed for redundans af systemerne, enten ved back-up-systemer eller ved anvendelse af andre systemer eller metoder.

Stk. 2. Planmaterialet skal opdateres ved ændringer i eller tilføjelse af nye forsyningskritiske it-systemer eller forsyningskritiske processer.

Beredskabsplanlægning

§ 11. Virksomhederne og den centrale lagerenhed skal udarbejde beredskabsplaner baseret på risiko- og sårbarhedsvurderingerne, jf. § 8, seneste 3 måneder efter gennemførelse af disse.

Stk. 2. Beredskabsplanerne skal indeholde følgende:

1) En identificering af forsyningskritiske anlæg og processer, samt afhængighed af andre systemer uden for virksomheden.
2) Beskrivelse af forebyggende foranstaltninger til mulig iværksættelse under en beredskabssituation, herunder muligheder for alternative driftsformer.
3) Beskrivelse af intern ansvars- og rollefordeling under krisestyring.
4) Overordnet beskrivelse af intern beredskabsorganisering, der kan iværksættes for at håndtere en beredskabssituation, som f. eks. en krisestab eller skærpet driftsbemanding.
5) Beskrivelse af kommunikation med andre virksomheder, den centrale lagerenhed, Energistyrelsen og andre myndigheder i en akut krisesituation.
6) Beskrivelse af procedurer for etablering af alternativ drift ved nedbrud på forsyningskritiske anlæg og processer.
7) Plan for genoprettelse af forsyningskritisk infrastruktur og processer.
8) Plan for dokumentation og opfølgning på hændelser.
9) Beskrivelse af den operative ansvarsfordeling mellem virksomheden og dennes samarbejdsparter.

Stk. 3. Virksomheder og den centrale lagerenhed skal, såfremt de opfylder kriterierne beskrevet i § 9 stk. 1 tilsikre, at it-forhold integreres i beredskabsplanlægningen, således at følgende elementer indarbejdes i deres beredskabsplaner efter stk. 1:

1) Beskrivelse af forsyningskritiske it-systemer, samt afhængighed af andre it-systemer uden for virksomheden på baggrund af planmateriel efter § 10.
2) Beskrivelse af forbyggende foranstaltninger til mulig iværksættelse i it-systemerne identificeret i punkt 1, herunder muligheder for segmentering af it-systemer og alternative driftsformer. Anvendes fjernadgang til forsyningskritiske it-systemer, skal beredskabsplanen indeholde en plan for, hvordan angreb på disse systemer opdages og håndteres.
3) Beskrivelse af procedurer for etablering af alternativ drift ved nedbrud på forsyningskritiske it-systemer.
4) Plan for genoprettelse af forsyningskritiske it-systemer.
5) Benyttes ekstern opkobling til virksomhedens forsyningskritiske it-systemer, skal beredskabsplanen beskrive procedurer for, hvordan it-sikkerhed sikres i disse forbindelser.
6) Relevante forhold der i medfør af afhængigheden af it-systemer påvirker elementer beskrevet i stk. 2, nr. 3, 4, 5, 8 og 9.

Stk. 4. Beredskabsplaner skal opdateres senest 3 måneder efter gennemførelse af en risiko- og sårbarhedsvurdering, jf. § 8, stk. 4.

Stk. 5. Beredskabsplaner skal være versionsstyret med en kort beskrivelse af ændringer i forhold til tidligere versioner.

Stk. 6. Energistyrelsen skal vejlede virksomhederne i udarbejdelse af beredskabsplaner.

Øvelser, rapportering mv.

§ 12. Virksomheder og den centrale lagerenhed skal sikre, at de medarbejdere, der indgår i håndteringen af beredskabet, løbende modtager den fornødne instruktion, uddannelse og træning i håndtering af en beredskabssituation og andre ekstraordinære situationer som planlagt efter § 11.

§ 13. Virksomheder og den centrale lagerenhed skal afholde beredskabsøvelser med udgangspunkt i egne beredskabsplaner, jf. § 11 stk. 1.

Stk. 2. Virksomhederne og den centrale lagerenhed skal udarbejde og vedligeholde en øvelsesplan, der beskriver, hvilke øvelser virksomheden påregner at gennemføre de næste tre år. Denne øvelsesplan skal sikre, at alle væsentlige elementer i virksomhedens øvelsesplan øves jævnligt.

Stk. 3. Virksomheder og den centrale lagerenhed skal minimum afholde én årlig beredskabsøvelse.

Stk. 4. Virksomhederne og den centrale lagerenhed skal udarbejde en evaluering af hver afholdt beredskabsøvelse. Øvelsesevalueringen skal angive øvelsens forløb, opnåede erfaringer samt planlagt opfølgning og tidsplan herfor. Evalueringen skal indeholde en vurdering af, hvilke læringspunkter der er relevante at dele med andre virksomheder eller myndigheder.

Hændelser

§ 14. Hændelser, der i væsentlig grad reducerer virksomhedens eller den centrale lagerenheds funktionalitet eller

funktionaliteten af andre dele af oliesektoren, skal uden ugrundet ophold meddeles Energistyrelsen.

Stk. 2. Virksomhederne og den centrale lagerenhed skal uden ugrundet ophold underrette Energistyrelsen og Center for Cybersikkerhed om it-sikkerhedshændelser, der påvirker forsyningskritiske it-systemer, gennem en af Erhvervsstyrelsen dertil indrettet internetbasseret portal, såfremt de opfylder kriterierne beskrevet i § 9 stk. 1. Underretningen skal som minimum indeholde en beskrivelse af:

1) Hændelsen.
2) Hændelsens konsekvenser.
3) Hvorvidt hændelsen vurderes at have væsentlige konsekvenser for tjenester i andre sektorer eller andre EU- eller EØS-lande.

Stk. 3. Energistyrelsen kan efter høring af den meddelende virksomhed i stk. 1 oplyse offentligheden om konkrete itberedskabshændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

§ 15. Virksomheder og den centrale lagerenhed skal udarbejde evaluering af hændelser meddelt i medfør af § 14 stk. 1. Der skal minimum udarbejdes en evaluering på baggrund af følgende situationer:

1) Hændelser, der har aktiveret beredskabsorganiseringen om beskrevet i § 11 stk. 2.
2) Hændelser, hvor nedbrud i it-systemer har afstedkommet behov for manuel drift af forsyningskritiske systemer, eller situationer, hvor en reduktion i it-styring har haft negative konsekvenser for driften af forsyningssystemer.
3) Hændelser, der har krævet ekstern bistand til situationsudredning, udbedring eller reetablering af systemer eller funktionalitet i virksomhedens it-systemer.
4) Hændelser, der vurderes at aflede væsentlig læring internt i egen organisation eller ved andre virksomheder.

Stk. 2. Hændelsesevalueringen skal angive hændelsens forløb, opnåede erfaringer samt planlagt opfølgning og tidsplan herfor samt en vurdering af, hvilke læringspunkter der er relevante at dele med andre virksomheder eller myndigheder.

Stk. 3. Hændelsesevalueringen skal fremsendes senest tre måneder efter hændelsen til Energistyrelsen.

Sikringsforanstaltninger

§ 16. Virksomheder og den centrale lagerenhed skal sikre, at forsyningskritiske anlæg og it-systemer beskyttes i forhold til deres kritikalitet.

Stk. 2. Virksomhederne skal sikre forsyningskritiske anlæg og forsyningskritiske it-systemer mod uautoriseret adgang.

Leverandørstyring

§ 17. Virksomheder og den centrale lagerenhed har ansvar for sikkerheden i egen forsyningskritisk infrastruktur og egne forsyningskritiske it-systemer, ved anvendelse af eksterne leverandører til foretagelse af installation, vedligehold og opdatering.

Stk. 2. Virksomhederne og den centrale lagerenhed skal etablere procedurer for leverandørers adgang til forsyningskritisk infrastruktur og forsyningskritiske it-systemer eller dele heraf. Såfremt der er behov for fjernadgang til forsyningskritiske it-systemer, skal procedurer for denne fjernadgang beskrives i kontrakter, der på anmodning skal forevises ved tilsyn.

Stk. 3. Virksomhederne og den centrale lagerenhed sikrer, at data, der er følsomme af hensyn til forsyningen, håndteres med den fornødne sikkerhed. Den fornødne sikkerhed omfatter minimum:

1) at virksomhederne og den centrale lagerenhed i relation til leverandører bevarer ejerskab af forsyningskritisk data,
2) at adgangen til disse data logges, med mulighed for henføring til specifikke medarbejdere ved leverandører og
3) at disse data opbevares i lokaler, der er fysisk sikret mod uvedkommendes adgang.

Tilsyn

§ 18. Energistyrelsen fører tilsyn over for virksomhederne og den centrale lagerenhed om overholdelsen af §§ 2 stk. 2, 4, 6, 8, 10, 11, 13, 15, 17. Energistyrelsens tilsyn kan foretages fysisk. Ved fysisk tilsyn skal Energistyrelsen skriftligt varsle virksomheden herom senest 14 dage inden gennemførelsen af tilsynet.

Stk. 2. Virksomhederne og den centrale lagerenhed skal til en hver tid kunne udlevere følgende materiale til Energistyrelsens tilsyn:

1) Risiko- og sårbarhedsvurderinger udarbejdet efter § 8, stk. 1 - 3 og opdateret efter § 8 stk. 4.
2) Planmateriale efter § 10, stk. 1 og opdateret efter § 10 stk. 2.
3) Beredskabsplaner efter § 11, stk. 1 og § 11 stk. 2, opdateret efter § 10 stk. 3 og § 10 stk. 4.
4) Øvelsesplaner og øvelsesrapporter efter § 13.

Stk. 3. Energistyrelsen udarbejder indenfor 6 uger en rapport på baggrund af det gennemførte tilsyn. Rapporten skal forelægges virksomheden til kommentering i 4 uger inden færdiggørelse.

Andre bestemmelser

§ 19. Virksomheder, den centrale lagerenhed og Energistyrelsen skal sikre, at følsomme oplysninger behandles med fortrolighed.

Stk. 2. Ved følsomme oplysninger forstås:

1) Oplysninger om konkrete risici- og sårbarheder, jf. § 8.
2) Planmateriale, jf. § 10.
3) Kritiske dele af beredskabsplaner, jf. §§ 11, indeholdende beskrivelse af, hvordan virksomheden eller sektoren vil agere i givne beredskabssituationer.
4) Materiale af tilsvarende karakter, der af virksomheden vurderes at være følsomt.

Stk. 3. Forsendelse og håndtering af følsomt materiale skal ske på en måde, der sikrer fortrolighed og integritet af materialet. Udstederen har pligt til at gøre modtageren op-

mærksom på eventuelle krav til håndteringen af følsomt materiale.

Stk. 4. Følsomt materiale, som ikke længere benyttes, skal destrueres.

§ 20. Energistyrelsen kan efter ansøgning dispensere fra bestemmelser i denne bekendtgørelse, hvor ansøgeren har godtgjort, at en dispensation fra den konkrete bestemmelse i væsentligt omfang har mindre betydning eller reduceret effekt for beredskabet.

Håndhævelse og klageadgang

§ 21. Afgørelser truffet af Energistyrelsen, jf. §§ 4, 18 og 20 kan ikke påklages til anden administrativ myndighed.

Stk. 2. Afgørelser efter stk. 1 kan dog påklages til Energiklagenævnet, for så vidt angår retlige spørgsmål.

Stk. 3. Klagen skal være indgivet skriftligt inden 4 uger efter, at afgørelsen er meddelt til pågældende.

Straf

§ 22. Medmindre højere straf er forskyldt efter anden lovgivning, straffes med bøde den der:

1) Undlader at meddele Energistyrelsen efter § 9, stk. 1.
2) Undlader at underrette Energistyrelsen efter § 14, stk. 1.
3) Undlader at underrette Energistyrelsen eller Center for Cybersikkerhed efter § 14, stk. 2.
4) Undlader at udarbejde evalueringer efter hændelser efter § 15, stk. 1 og 2 eller fremsende disse til Energistyrelsen efter § 15, stk. 3.
5) Undlader at udlevere materiale til grundlag for Energistyrelsens tilsyn efter § 18, stk. 2.

Stk. 2. Der kan pålægges juridiske personer strafansvar efter reglerne i straffelovens 5. kapitel for overtrædelse af reglerne i bekendtgørelsen.

Ikrafttrædelse

§ 23. Bekendtgørelsen træder i kraft den 9. maj 2018.

Energistyrelsen , den 25. april 2018

MARTIN HANSEN

/ Lykke Mulvad Jeppesen