Lovtidende A

2025

Udgivet den 6. marts 2025

6. marts 2025. Nr. 260.

Bekendtgørelse om modstandsdygtighed og beredskab i energisektoren[1)]

I medfør af § 4, stk. 3, § 5, stk. 3 og 4, § 6, stk. 2, § 7, stk. 2, § 8, stk. 2, § 10, § 12, § 13, § 19, stk. 4 og 5, § 22, stk. 3, § 23, stk. 4, § 26, stk. 2, § 30, § 32, stk. 1, § 34, § 35, stk. 2, § 36 og § 37, stk. 4, i lov nr. 258 af 6. marts 2025 om styrket beredskab i energisektoren og efter forhandling med ministeren for samfundssikkerhed og beredskab fastsættes efter bemyndigelse i henhold til § 4, stk. 1, nr. 34, og stk. 2, samt § 5 i bekendtgørelse nr. 259 af 6. marts 2025 om Energistyrelsens opgaver og beføjelser:

Kapitel 1

Formål, anvendelsesområde og definitioner

§ 1. Denne bekendtgørelse fastsætter regler om organisatorisk beredskab, fysisk sikring og cybersikkerhed for virksomheder, der er væsentlige for energiforsyning og energimarkeder i Danmark og Europa. Bekendtgørelsen fastsætter endvidere regler for Energistyrelsen og Energinets opgavevaretagelse i forbindelse med beredskabet i energisektoren.

§ 2. Bekendtgørelsen finder anvendelse på virksomheder omfattet af § 2 i lov om styrket beredskab i energisektoren, jf. dog § 5.

Stk. 2. Regler om foranstaltninger til at understøtte anlægs modstandsdygtighed efter kapitel 10 finder anvendelse på virksomheder med anlæg klassificeret i henhold til § 6, stk. 2, jf. dog §§ 8, 42 og 43.

Stk. 3. Regler om foranstaltninger til at understøtte sikkerheden i net- og informationssystemer i denne bekendtgørelse finder anvendelse på de net- og informationssystemer, som virksomheder anvender til deres operationer eller til leveringen af deres tjenester jf. § 8 i lov om styrket beredskab i energisektoren.

§ 3. I denne bekendtgørelse forstås ved:

1) Beredskab: Organisering af processer, aktiviteter og foranstaltninger, som aktiveres, når der er behov for at forhindre, begrænse eller håndtere risici for nedbrud i eller forstyrrelse af en tjeneste, i perioden frem til genoprettelse af normal drift.
2) Cybersikkerhed: De aktiviteter, der er nødvendige for at beskytte net- og informationssystemer, brugerne af sådanne systemer og andre personer berørt af cybertrusler.
3) Forsyningskritisk net- og informationssystem: Et net- og informationssystem med mulighed for direkte at afbryde eller påvirke fysiske og logiske processer, som er nødvendige for forsyningen til en eller flere slutbrugere, herunder industrielle kontrolsystemer, operationelle teknologier samt net- og informationssystemer med direkte integration til disse.
4) Hændelse: En begivenhed, der har potentiale til i betydelig grad at forstyrre, eller som forstyrrer, leveringen af en væsentlig tjeneste, herunder når den påvirker de nationale systemer, der sikrer retsstatsprincippet, herunder en begivenhed, der bringer tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare.
5) Håndtering af en hændelse: Enhver handling og procedure, der tager sigte på at forebygge, opdage, analysere og inddæmme eller at reagere på og reetablere sig efter en hændelse.
6) Industrielle kontrolsystemer: Net- og informationssystemer, der anvendes til alle former for digital styring, kontrol og overvågning af fysiske og industrielle processer, eksempelvis styring, kontrol og overvågning af ventiler og pumper eller opsamling og analyse af data fra et fysisk system, herunder sensorer og styringskomponenter forbundet til et industrielt netværksmiljø.
7) Ledelsesorgan: henholdsvis det centrale ledelsesorgan som defineret i selskabsloven og ledelsen som defineret i LEV-loven, afhængigt af virksomhedens selskabsform.
8) Net- og informationssystem:
   a) Et elektronisk kommunikationsnet, hvorved forstås transmissionssystemer, uanset om de bygger

[1)] Bekendtgørelsen indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet), EU-Tidende 2022, nr. L 333, side 80, og dele af Europa-Parlamentets og Rådets direktiv (EU) 2022/2557 af 14. december 2022 om kritiske enheders modstandsdygtighed og om ophævelse af Rådets direktiv 2008/114/EF, EU-Tidende 2022, nr. L 333, side 164.

DB001118

Klima-, Energi- og Forsyningsmin.,
Energistyrelsen, j.nr. 2024-6493

på en permanent infrastruktur eller centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet og mobilnet, elkabelsystemer, i det omfang de anvendes til transmission af signaler, net, som anvendes til radio- og tv-spredning, samt kabel-tv-net, uanset hvilken type information der overføres.

b) Enhver anordning eller gruppe af forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data.

c) Digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a og b med henblik på deres drift, brug, beskyttelse og vedligeholdelse.

9) Operationelle teknologier: Fysiske net- og informationssystemer, der overvåges eller styres af industrielle kontrolsystemer.

10) Risiko: Potentialet for tab eller forstyrrelse som følge af en hændelse, udtrykt som en kombination af størrelsen af et sådant tab eller en sådan forstyrrelse og sandsynligheden for, at hændelsen indtræffer.

11) Risikovurdering: Den samlede proces med henblik på at bestemme arten og omfanget af en risiko ved at identificere og analysere potentielle relevante trusler, sårbarheder og farer, der kunne føre til en hændelse, og ved at evaluere det potentielle tab eller den potentielle forstyrrelse af leveringen af en væsentlig tjeneste forårsaget af denne hændelse.

12) Sikkerhed i net- og informationssystemer: Net- og informationssystemers evne til på et givet sikkerhedsniveau at modstå enhver begivenhed, der kan være til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer.

13) Sårbarhed: En svaghed, modtagelighed eller fejl ved processer, produkter, tjenester, fysiske indretninger og lignende, som kan påvirke sandsynligheden for, at der kan indtræde en hændelse.

Kapitel 2

Niveauinddeling af virksomheder og klassificering af anlæg

§ 4. Virksomheder inddeles i fem niveauer, jf. tærskelværdierne i bilag 1.

Stk. 2. Energistyrelsen træffer afgørelse om en virksomheds niveauinddeling på grundlag af virksomhedens aktiviteter og betydning for den samlede forsyning i den pågældende delsektor på lokalt, regionalt, nationalt eller europæisk plan.

Stk. 3. Virksomheder, der opererer inden for flere delsektorer, tildeles det højeste niveau, jf. tærskelværdierne i bilag 1. Dette vurderes særskilt for hver selskabsretlig enhed med selvstændigt CVR-nummer.

Stk. 4. Virksomheder der i fællesskab varetager beredskabsarbejde i et samordnet beredskab, jf. § 113, tildeles samme niveau. Energistyrelsen inddrager i afgørelsen virksomhedernes indbyrdes forhold i leveringen af tjenester og deres samlede betydning for den samlede forsyning i de relevante delsektorer efter § 113.

Stk. 5. Energistyrelsen kan træffe afgørelse om, at en virksomhed skal tildeles et højere niveau, end hvad der fremgår af tærskelværdierne i bilag 1, hvis særlige omstændigheder gør, at den pågældende virksomhed leverer sin tjeneste til slutbrugere, der udgør kritiske enheder i andre sektorer.

§ 5. Virksomheder, som er inddelt i niveau 1, efter § 4, stk. 1 og 2, skal, uagtet bestemmelserne i denne bekendtgørelse, kun overholde bestemmelserne i kapitel 15-17 og 19-20, samt §§ 4, 5, 9, 19, stk. 1-5 samt § 73, stk. 1, 3 og 4.

§ 6. Virksomheders anlæg inddeles i fem klasser, jf. tærskelværdierne i bilag 2.

Stk. 2. Energistyrelsen træffer afgørelse om klassificering af en virksomheds anlæg på grundlag af anlæggets funktion og betydning for den samlede forsyning i den pågældende delsektor på lokalt, regionalt, nationalt eller europæisk plan.

Stk. 3. Anlæg, som anvendes inden for flere delsektorer, klassificeres i højeste klasse, jf. tærskelværdierne i bilag 2.

Stk. 4. Sammenbyggede anlæg anses som ét anlæg og klassificeres efter det anlæg med den højeste klasse.

Stk. 5. Energistyrelsen kan træffe afgørelse om, at en virksomheds anlæg skal klassificeres i en højere klasse, end hvad der fremgår af tærskelværdierne i bilag 2, hvis særlige omstændigheder gør, at det pågældende anlæg kan påvirke leveringen af en virksomheds tjeneste til slutbrugere, der udgør kritisk infrastruktur i andre sektorer.

Stk. 6. Energistyrelsen kan give forhåndstilsagn om et anlægs forventede klasse ved etablering, sammenlægning og ændring af et anlæg. Energistyrelsens forhåndstilsagn er bindende, forudsat at de faktiske forhold, som tilsagnet er baseret på, ikke ændres.

§ 7. Virksomheders almindelige kontorfaciliteter, som anvendes til leveringen af virksomhedens tjenester, skal overholde kravene i § 36, stk. 1 og 2, § 38, stk. 1, § 38, stk. 2, nr. 1 og 2 og § 38, stk. 3.

§ 8. Virksomheders anlæg, som ikke opfylder tærskelværdierne i bilag 2, klassificeres ikke af Energistyrelsen efter § 6.

Stk. 2. Foranstaltningerne i kapitel 10 finder ikke anvendelse for anlæg i klasse 1.

§ 9. Virksomheder skal hvert tredje år den 1. oktober sende de oplysninger efter bilag 3 til Energistyrelsen, som er nødvendige for niveauinddeling af virksomheder, jf. § 4, og klassificering af anlæg, jf. § 6, dog første gang den 1. april 2025.

Stk. 2. Virksomheder skal uden unødigt ophold sende oplysninger om ændrede forhold af betydning for en virksomheds niveauinddeling og et anlægs klasse.

Stk. 3. Energistyrelsen kan kræve, at en virksomhed inden for en nærmere angivet frist på minimum en uge sender manglende oplysninger til brug for afgørelser efter § 4, stk. 2, og § 6, stk. 2.

Stk. 4. Inden for el- og fjernvarmesektoren videregiver Energistyrelsen oplysninger om virksomheders tildelte niveau samt virksomheders anlægs tildelte klasse til Forsyningstilsynet.

Kapitel 3

Roller og ansvar

§ 10. Virksomheders risikostyring og beredskab fastlægges af virksomhedens ledelsesorgan, som skal godkende følgende:

1) Risiko- og sårbarhedsvurderinger efter § 18.
2) Risikovurderinger i forbindelse med projekter, som skal sendes til Energistyrelsen efter § 28, stk. 1.
3) Beredskabsplaner efter § 19.

§ 11. Virksomheder skal have én beredskabskoordinator til at koordinere beredskabsplanlægningen, herunder bistå ved udarbejdelsen af risiko- og sårbarhedsvurderinger efter § 18 og beredskabsplaner efter § 19.

Stk. 2. Virksomheder skal have én cyberkoordinator til at kordinere foranstaltningerne til at understøtte sikkerheden i net- og informationssystemer, samt bistå beredskabsplanlægningen for virksomhedens net- og informationssystemer.

Stk. 3. Virksomheder med anlæg i klasse 4 og 5 skal have én eller flere sikringskoordinatorer til at koordinere foranstaltninger på virksomhedens anlæg i klasse 4 og 5.

Stk. 4. Beredskabskoordinatoren, cyberkoordinatoren og sikringskoordinatoren skal indbyrdes koordinere de forskellige områder, så virksomhedens beredskab planlægges ud fra et samlet risikobillede.

Stk. 5. Virksomhedens ledelsesorgan skal minimum fire gange årligt mødes med de koordinerende roller i stk. 1-3 med henblik på at tage stilling til virksomhedens organisatoriske beredskab, fysiske sikring og cybersikkerhed. Der skal føres referat af møderne.

Stk. 6. Virksomheder i niveau 4 og 5 må ikke have personsammenfald mellem beredskabskoordinatoren, cyberkoordinatoren og virksomhedens ledelsesorgan, der godkender risikovurderinger og beredskabsplaner efter § 10.

Stk. 7. Virksomheder skal underrette Energistyrelsen om opdaterede kontaktoplysninger på de koordinerende roller i stk. 1-3.

Kapitel 4

Politik for risikostyring

§ 12. Virksomheder skal have politikker for risikostyring eller tilsvarende til at sætte rammerne for virksomhedens risikostyring. Politikkerne skal omfatte følgende:

1) Beskrivelse af ledelsesansvar og rolle.
2) Metoder til at identificere, vurdere og evaluere risici, herunder risici for anlæg og net- og informationssystemer.
3) Metoder til identifikation, vurdering, håndtering og prioritering af passende foranstaltninger til at mitigere og styre risici.
4) Kriterier for evaluering og prioritering af risici.
5) Kriterier for accept af risici.

Kapitel 5

Beredskabsplanlægning

§ 13. Virksomheder skal foretage beredskabsplanlægning, således at virksomhedens beredskabsplaner efter § 19 sikrer driftskontinuitet, og virksomheden kan overholde sine underretningsforpligtigelser i tilfælde af en hændelse.

Stk. 2. Virksomheder skal tage stilling til behovet for redundans, herunder redundans af net- og informationssystemer og anlæg, som anvendes i leveringen af virksomhedens tjenester.

Stk. 3. Virksomheder skal indgå i den nationale krisehåndtering, herunder omsætte udmeldinger om ændringer i sektorberedskabsniveau og sektorberedskabsforanstaltninger til nødvendige tiltag i egen organisation uden unødigt ophold.

Fortegnelser

§ 14. Virksomheder skal føre ajourførte fortegnelser over anlæg, som er nødvendige for at virksomheden kan levere sine tjenester.

Stk. 2. Fortegnelser efter stk. 1 skal beskrive et anlægs funktion i leveringen af virksomhedens tjenester, dets kritikalitet for leveringen af virksomhedens tjenester, geografiske placering og eventuelle afhængigheder af reservedele, net- og informationssystemer og leverandører.

Stk. 3. Fortegnelser efter stk. 1 skal indeholde oplysninger om virksomhedens afhængighed af andre virksomheders anlæg i leveringen af virksomhedens tjenester.

§ 15. Virksomheder skal føre ajourførte fortegnelser over net- og informationssystemer, som virksomheden anvender i leveringen af sine tjenester.

Stk. 2. Fortegnelser efter stk. 1 skal indeholde beskrivelser af de processer, et net- og informationssystem understøtter, dets kritikalitet for leveringen af virksomhedens tjenester, intern ansvarsplacering, levetid og eventuelle afhængigheder af andre net- og informationssystemer og leverandører.

Stk. 3. Fortegnelser efter stk. 1 skal indeholde oplysninger om virksomhedens afhængighed af interne og eksterne net- og informationssystemer i leveringen af virksomhedens tjenester.

§ 16. Virksomheder skal føre en fortegnelse over fysiske og digitale informationsstrømme, som indgår i kommunikationen mellem styringskritiske funktioner i leveringen af virksomhedens tjenester, og som virksomheden sender og modtager fra eksterne aktører og eksterne net- og informationssystemer.

Stk. 2. Fortegnelsen efter stk. 1 skal indeholde en vurdering af risici for tab af fortrolighed, integritet og tilgængelighed for nævnte informationsstrømme.

§ 17. Fortegnelser efter §§ 14-16 skal holdes opdateret, så fortegnelserne altid er retvisende.

Risiko- og sårbarhedsvurdering

§ 18. Virksomheder skal gennemføre en risiko- og sårbarhedsvurdering af kendte og mulige risici, der kan forstyrre eller forhindre leveringen af virksomhedens tjenester.

Stk. 2. Risiko- og sårbarhedsvurderingen efter stk. 1 skal indeholde:

1) En identifikation og vurdering af risici og sårbarheder.
2) En vurdering af konsekvenser ved potentielle hændelser, herunder mulige afledte samfundsmæssige konsekvenser.
3) En handlingsplan for risikohåndtering, som angiver:
   a) Foranstaltninger til at mitigere og styre risici og sårbarheder, herunder foranstaltninger jf. kapitel 10 og kapitel 11.
   b) Tidsplan for implementering af foranstaltningerne i litra a.
   c) Intern ansvarsplacering for implementering foranstaltningerne i litra a.

Stk. 3. Virksomheder skal som led i deres identifikation og analyse af risici og sårbarheder:

1) Tage stilling til Energistyrelsens risiko- og sårbarhedsscenarier, jf. § 107, stk. 5.
2) Inkludere relevante informationskilder, herunder virksomhedens egne erfaringer samt trussels- og sårbarhedsvurderinger fra myndigheder og it-sikkerhedstjenesten, jf. § 33, stk. 1.
3) Tage stilling til risici, der vurderes at være tilbage, efter at virksomheden har implementeret foranstaltninger efter stk. 2, nr. 3, litra a.

Stk. 4. Risiko- og sårbarhedsvurderingen efter stk. 1 skal gennemføres med inddragelse af relevante medarbejdere og leverandører med teknisk og organisatorisk kendskab til virksomhedens processer, anlæg, net- og informationssystemer, netværksinfrastruktur og leverandørforhold.

Stk. 5. Risiko- og sårbarhedsvurderingen efter stk. 1 skal opdateres ved væsentlige ændringer og integreres i virksomhedens samlede risikobillede.

Stk. 6. Foranstaltninger efter stk. 2, nr. 3, skal implementeres under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostninger og risicienes alvor.

Beredskabsplaner

§ 19. Virksomheder skal have ledelsesgodkendte, jf. § 10, beredskabsplaner for håndtering af hændelser og styring af kriseindsatsen. Beredskabsplaner kan omfatte en eller flere delberedskabsplaner, procedurer og instrukser.

Stk. 2. Beredskabsplaner efter stk. 1 skal som minimum beskrive:

1) Intern ansvars- og rollefordeling, herunder vagtordninger og etablering af en krisestab eller krisestyringsorganisation af relevans for håndteringen af en hændelse.
2) Muligheder for at aktivere yderligere ressourcer og materiel, herunder ekstra driftsbemanding samt støtte fra andre virksomheder i henhold til kontrakter eller andre aftaler.
3) Operationel ansvarsfordeling mellem virksomheden og dennes samarbejdspartnere eller leverandører i forbindelse med håndteringen af en hændelse.
4) Kontaktoplysninger på relevante personer i forbindelse med håndteringen af en hændelse, herunder beredskabsansvarlige og systemansvarlige medarbejdere samt krisestabens medarbejdere.
5) Kriterier for aktivering af en krisestab til håndteringen af en hændelse.

Stk. 3. Beredskabsplaner efter stk. 1 skal indeholde følgende procedurer:

1) Procedurer for etablering af alternative driftsformer ved nedbrud i processer, anlæg og net- og informationssystemer, herunder beskrivelser af:
   a) Muligheder for at overgå til manuel drift.
   b) Metoder til og betingelser for at aktivere redundante net- og informationssystemer og nødprocedurer.
2) Procedurer for isolering af industrielle kontrolsystemer og operationelle teknologier, herunder en beskrivelse af metoder til at isolere systemerne samt betingelser for at aktivere planerne.
3) Procedurer for genoprettelse af et anlæg, herunder en beskrivelse af hvor hurtigt reservedele, mandskab og øvrige ressourcer kan anskaffes for at genoprette driften ved beskadigelse af de dele af anlægget, der er væsentlige for virksomhedens tjeneste.
4) Procedurer for at fremskaffe kritiske reservedele fra eget lager eller fra leverandører.
5) Procedurer for genoprettelse af net- og informationssystemer, herunder beskrivelser af:
   a) Maksimalt accepteret nedetid og datatab for net- og informationssystemer.
   b) Målsætningen for genetableringstid og metoder til at genoprette net- og informationssystemer fra backup.
   c) Betingelserne for aktivering af procedurer for genoprettelse.
6) Procedurer for iværksættelse af beredskabsforanstaltninger, som kan iværksættes i forbindelse med håndteringen af en hændelse, herunder sektorberedskabsforanstaltninger.
7) Procedurer for udveksling af driftskritisk information ved nedbrud i normale kommunikationslinjer i forbindelse med en hændelse.
8) Procedurer for dokumentation for virksomhedens håndtering af en hændelse.
9) Procedurer for at modtage, indhente, behandle og fordele relevant information internt i virksomheden i forbindelse med håndteringen af en hændelse.
10) Procedurer for ekstern informationsdeling om hændelser og håndteringen af hændelser til relevante myndigheder, samarbejdspartner, forbrugere, pressen, offentligheden og andre aktører.

Stk. 4. Beredskabsplaner efter stk. 1 skal være i overensstemmelse med sektorberedskabsplanen for den delsektor, virksomheden opererer inden for.

Stk. 5. Beredskabsplaner efter stk. 1 skal være versionsstyrede med en kort beskrivelse af ændringerne i forhold til tidligere versioner.

Stk. 6. Beredskabsplaner efter stk. 1 skal tage højde for konklusionerne i risiko- og sårbarhedsvurderingen, jf. § 18, og skal i nødvendigt omfang opdateres i forbindelse med gennemførelsen af en risiko- og sårbarhedsvurdering.

Øvelser og funktionstest

§ 20. Virksomheder skal have en plan over øvelser, som virksomheden planlægger at gennemføre over en femårig periode i henhold til § 21.

Stk. 2. Den femårige øvelsesplan skal dække alle øvelseselementer i bilag 4.

Stk. 3. Virksomheder skal første gang udarbejde en femårig øvelsesplan som dækker perioden fra den 1. oktober 2025 til den 30. september 2030. Derefter udarbejdes en ny øvelsesplan for en ny femårig periode.

Stk. 4. Den femårige øvelsesplan er tentativ og skal opdateres minimum én gang årligt og ved væsentlige ændringer.

§ 21. Virksomheder i niveau 3-5 skal minimum øve deres beredskab én gang om året med udgangspunkt i egne beredskabsplaner, jf. § 19.

Stk. 2. Virksomheder i niveau 2 skal minimum øve deres beredskab hvert andet år.

Stk. 3. Virksomheder i niveau 4 og 5 skal én gang om året øve genopretning af virksomhedens forsyningskritiske net- og informationssystemer, jf. øvelseselement nr. 18 i bilag 4.

Stk. 4. Virksomheders ledelsesorgan skal i relevant omfang deltage i beredskabsøvelser.

Stk. 5. Virksomheder skal efter anmodning fra henholdsvis Energinet eller Energistyrelsen deltage i sektorberedskabsøvelser, jf. § 89 og § 101.

§ 22. Virksomheder skal årligt gennemføre funktionstests af teknisk udstyr, som virksomheden planlægger at anvende i forbindelse med håndteringen af en hændelse, herunder test af alternative kommunikationsmidler og teknisk kontrol af kommunikationsveje.

§ 23. Virksomheder skal evaluere øvelser, som virksomheden gennemfører efter § 21.

Stk. 2. Virksomheder skal udarbejde og sende en øvelsesevaluering, når øvelsen har indeholdt øvelseselementer fra bilag 4 til Energistyrelsens til godkendelse senest tre måneder efter, at en øvelse er afholdt. Øvelsesevalueringen skal som minimum indeholde en beskrivelse af:

1) Trænede øvelseselementer, jf. bilag 4.
2) Øvelsens forløb.
3) Opnåede erfaringer.
4) Relevante læringspunkter.
5) Planlagt opfølgning på læringspunkterne i nr. 4, herunder tidsplan og intern ansvarsplacering for opfølgningen.

Stk. 3. Energistyrelsen kan videresende relevante læringspunkter fra en virksomhed i el-, gas- eller brintsektorens øvelsesevaluering efter stk. 2, nr. 4, til Energinet, hvis Energistyrelsen vurderer det nødvendigt for Energinets evne til at varetage de koordinerende opgaver i sektorberedskabet, jf. § 81.

Stk. 4. Energistyrelsen kan i anonymiseret form dele relevante læringspunkter fra en virksomheds øvelsesevaluering med andre virksomheder og myndigheder, hvis Energistyrelsen vurderer det relevant for sektorberedskabet som helhed.

Stk. 5. Energistyrelsen skal høre den pågældende virksomhed, hvis læringspunkter planlægges videresendt, inden videresendingen må finde sted efter stk. 3 og 4.

Kapitel 6

Undervisning og awareness

§ 24. Medlemmer af en virksomheds ledelsesorgan skal deltage i relevante kurser eller undervisning om organisatoriske beredskab, fysiske sikring og cybersikkerhed.

§ 25. Virksomheder skal sikre, at personer, som udfører opgaver inden for virksomhedens organisatoriske beredskab, fysiske sikring og cybersikkerhed, opbygger og fastholder de nødvendige kompetencer, herunder modtager den fornødne instruktion, undervisning og træning.

§ 26. Virksomheder skal årligt gennemføre awareness-tiltag for at fremme og fastholde kendskab til relevante beredskabsplaner, trusler og sårbarheder i virksomheden.

Stk. 2. Virksomheder skal årligt gennemføre awareness-tiltag for at fremme og fastholde virksomhedens evne til at genkende og håndtere relevante cybertrusler og sårbarheder.

Kapitel 7

Risikovurderinger af projekter

§ 27. Virksomheder skal gennemføre en risikovurdering i henhold til § 18, stk. 1 og 2 og stk. 4, i forbindelse med følgende projekter:

1) Erhvervelse og udvikling af forsyningskritiske net- og informationssystemer.
2) Etablering af nye anlæg eller opkøb af anlæg i klasse 3-5, jf. tærskelværdierne i bilag 2. Ændring af eksisterende anlæg i klasse 3-5, som forventes at medføre en ændring i et anlægs klassificering, jf. tærskelværdierne i bilag 2.
3) Outsourcing af udviklings-, drifts- og vedligeholdelsesopgaver, der kan påvirke leveringen af virksomhedens tjenester.

Stk. 2. Risikovurderinger efter stk. 1, hvor der indgår et leverandørforhold, skal inkludere en vurdering af risici som følger af leverandørforholdet, jf. procedurerne i § 29.

Stk. 3. Risikovurderinger efter stk. 1 skal udarbejdes ved projektets opstart og foreligge skriftligt, inden projektet påbegyndes. Risikovurderingen skal opdateres, når projektets omfang, tidsplan og delleverancer ændres i en sådan grad, at det ændrer forudsætningerne for risikovurderingen.

§ 28. Risikovurderinger efter § 27 skal fremsendes til Energistyrelsen til godkendelse i forbindelse med følgende projekter:

1) Anlægsprojekter efter § 27, stk. 1, nr. 2 og 3, hvor et anlæg ved fuldførelse forventes at opfylde tærskelvær-

dierne for anlæg i klasse 4 og 5, jf. tærskelværdierne i bilag 2.
2) Erhvervelse eller udvikling af forsyningskritiske net- og informationssystemer efter § 27, stk. 1, nr. 1 og 3.

Stk. 2. Risikovurderinger efter stk. 1 skal sendes til Energistyrelsen senest én måned efter ledelsesorganets godkendelse af en risikovurdering jf. § 10, nr. 2.

Stk. 3. Projekter efter § 27 kan gennemføres, indtil Energistyrelsens endelige godkendelse af risikovurderingen, jf. stk. 1, foreligger.

Kapitel 8

Leverandørstyring og forsyningskædesikkerhed

§ 29. Virksomheder skal have procedurer for forsyningskædesikkerhed i leverandørforhold, så virksomheden træffer passende og forholdsmæssige foranstaltninger i forhold til produkter og tjenester, som virksomheden anvender i leveringen af sine tjenester. Procedurerne skal indeholde:
1) Metoder til at identificere, vurdere og håndtere risici, der er specifikke for hver direkte leverandør og tjenesteudbyder i forsyningskæden, herunder risici forbundet med afhængigheder af underleverandører og internationale forhold i en aftale med en direkte leverandør og tjenesteudbyder.
2) Metoder til at vurdere modstandsdygtigheden af leverede produkter og tjenester, herunder den generelle kvalitet af eventuelt integrerede foranstaltninger til at styre risici i net- og informationssystemer.

§ 30. Virksomheder skal ved indgåelse af aftaler med direkte leverandører og tjenesteudbydere af produkter og tjenester, som kan påvirke forsyningssikkerheden eller påvirke sikkerheden i virksomhedens net- og informationssystemer, sikre:
1) At der stilles krav til passende foranstaltninger til at styre risici og håndtere hændelser, for så vidt angår de leverede produkter og tjenester.
2) At virksomheden underrettes om væsentlige hændelser, jf. § 77, stk. 2, for så vidt angår de leverede produkter og tjenester, hos den direkte leverandør eller tjenesteudbyder.
3) At den direkte leverandør eller tjenesteudbyder bistår virksomheden med at overholde sine rapporteringsforpligtelser i tilfælde af væsentlige hændelser, jf. §§ 77-80.
4) At direkte leverandører og tjenesteudbydere kan inddrages i forbindelse med Energistyrelsens tilsyn med virksomheden angående overholdelse af bestemmelser i lov om styrket beredskab i energisektoren og denne bekendtgørelse.
5) At direkte leverandører forpligter sig til i passende omfang at indgå i virksomhedens øvelser, jf. bilag 4, nr. 13 og 14.
6) At direkte leverandører og tjenesteudbydere kan inddrages i virksomhedens beredskabsarbejde i det omfang, det er relevant.
7) At der opstilles kriterier for direkte leverandørers udlicitering af væsentlige dele af en leverandøraftale til en eller flere underleverandører.
8) At virksomheden i relation til direkte leverandører og tjenesteudbydere bevarer ejerskab af data, som er nødvendig for leveringen af virksomhedens tjeneste eller som er fortrolige, jf. § 26 i lov om styrket beredskab i energisektoren.

§ 31. Virksomheder skal have procedurer for styring af fjernadgange for direkte leverandører og tjenesteudbydere, som kan tilgå virksomhedens forsyningskritiske net- og informationssystemer.

Stk. 2. Hvis en direkte leverandør eller tjenesteudbydere har behov for fjernadgang til virksomhedens forsyningskritiske net- og informationssystemer, skal procedurerne fremgå af leverandøraftalen.

§ 32. Virksomheder skal sikre, at krav om organisatorisk beredskab, fysisk sikring og cybersikkerhed rettet mod direkte leverandører eller tjenesteudbydere i henhold til § 30 og § 31 fremgår af en leverandøraftale.

Stk. 2. Virksomheder skal sikre, at direkte leverandører og tjenesteudbydere over for virksomheden kan dokumentere overholdelse af krav, som stilles i en leverandøraftale, jf. § 30 og § 31.

Kapitel 9

It-sikkerhedstjeneste

§ 33. Virksomheder skal være tilmeldt en it-sikkerhedstjeneste, som skal varsle virksomheden om relevante sårbarheder og cybertrusler uden ugrundet ophold og vejlede virksomheden om mitigerende tiltag.

Stk. 2. Det skal fremgå af leverandøraftalen med en it-sikkerhedstjeneste, hvor hurtigt it-sikkerhedstjenesten skal varsle virksomheden efter opdagelse af sårbarheder og cybertrusler.

Stk. 3. Virksomheder skal sikre, at it-sikkerhedstjenesten har det nødvendige kendskab til virksomhedens net- og informationssystemer, så it-sikkerhedstjenesten kan identificere og varsle virksomheden om relevante sårbarheder og cybertrusler.

Stk. 4. Virksomheder skal sikre, at varsler modtages af personer med de nødvendige kompetencer til at omsætte varsler til mitigerende handling i virksomheden under hensyntagen til et varsels alvor.

Stk. 5. Virksomheder, som indgår en fælles kontrakt med en it-sikkerhedstjeneste, skal alle fremgå af kontrakten med it-sikkerhedstjenesten. Kontrakten skal opbevares hos alle tilmeldte virksomheder.

§ 34. Virksomheder i niveau 3-5 skal sikre, at en it-sikkerhedstjeneste bistår virksomheden i forbindelse med håndteringen af en hændelse, herunder at it-sikkerhedstjenesten kan yde assistance til skadesbegrænsning, bevisindsamling og teknisk bistand til genoprettelse af net- og informationssystemer.

§ 35. Virksomheder skal sikre, at oplysninger om sårbarheder og hændelser, som tilvejebringes gennem virksomhedens it-sikkerhedstjeneste, kan videreformidles til andre virksomheder uden ugrundet ophold.

Kapitel 10

Anlægs modstandsdygtighed

§ 36. Virksomheder skal have passende og forholdsmæssige foranstaltninger til at sikre, at virksomhedens anlæg er modstandsdygtige over for skader og funktionstab.

Stk. 2. Virksomheder skal gennemføre passende og forholdsmæssig klimatilpasning af virksomhedens anlæg, så anlæg er modstandsdygtige over for skader eller funktionstab som følge af klimarelaterede hændelser.

Stk. 3. Virksomheder skal for virksomhedens anlæg i klasse 3-5 som minimum have foranstaltninger, der kan understøtte følgende, jf. dog stk. 4:

1) At skader eller fejl på anlægget opdages, verificeres og alarmeres.
2) At anlægget er modstandsdygtig over for funktionssvigt af net- og informationssystemer.
3) At anlægget er modstandsdygtig over for funktionssvigt af offentligt udbudte elektroniske kommunikationsnet eller -tjenester.

Stk. 4. Transmisionssystemoperatører og distributionssystemoperatører inden for elsektoren skal have foranstaltninger efter stk. 3, for anlæg i klasse 2-5.

Stk. 5. Virksomheder skal for anlæg i klasse 3-5 skal have nødstrømsforsyning, som i tilfælde af strømafbrydelse sikrer, at anlægget ikke tager skade under nedlukning og er funktionsdygtig, når strømforsyningen genoprettes, jf. dog stk. 6.

Stk. 6. Transmisionssystemoperatører og distributionssystemoperatører inden for elsektoren skal for anlæg i:

1) Klasse 4 og 5 have nødstrømsforsyning, som i tilfælde af strømafbrydelse sikrer anlæggets funktionalitet i en periode frem til strømforsynings genopretning.
2) Klasse 3 have nødstrømsforsyning, som i tilfælde af strømafbrydelse sikrer anlæggets funktionalitet i minimum 24 timer.
3) Klasse 2 have nødstrømsforsyning, som i tilfælde af strømafbrydelse sikrer anlæggets funktionalitet i minimum 4 timer.

Stk. 7. Virksomheder skal sikre, at funktionstab og skader på anlæg udbedres, så virksomheden kan genoprette evnen til at levere sine tjenester uden unødigt ophold.

Stk. 8. Virksomheder skal som minimum hvert halve år foretage kontrol med, at foranstaltninger efter stk. 2-4, stk. 7 og stk. 10 gennemføres, er intakte og fungerer efter hensigten.

Stk. 9. Virksomheder skal som minimum hvert år foretage afprøvning af et anlægs nødstrøm, jf. stk. 5 og 6.

Stk. 10. Virksomheder skal i forbindelse med anlægsprojekter på baggrund af en risikovurdering have passende og nødvendige foranstaltninger til at sikre anlæggets modstandsdygtighed i anlægsprojektfasen.

§ 37. Virksomheder skal have et system for styret adgangskontrol, så kun godkendte og verificerede personer kan få adgang til virksomhedens anlæg.

Stk. 2. Virksomheder skal tage stilling til, hvilke medarbejdere og leverandører der må og kan få adgang til forskellige dele af virksomhedens anlæg, herunder mulighed for at færdes uledsaget på anlægget eller dele heraf.

Stk. 3. Virksomheder skal sikre, at gæster og andre personer, som ikke har fast arbejdsgang på et anlæg, eller på dele af anlægget, indgår i den styrede adgangskontrol.

Stk. 4. Virksomheder skal sikre, at adgange logges, så der kan dokumenteres personhenførbare logs på adgange til virksomhedens anlæg. Dokumentationen skal beskyttes som beskrevet i § 67.

Stk. 5. Virksomheder skal som minimum hvert halve år foretage kontrol med, at den styrede adgangskontrol efter stk. 1-4 gennemføres, er intakt og fungerer efter hensigten, herunder at kun godkendte personer kan få adgang til virksomhedens anlæg.

§ 38. Virksomheder skal have foranstaltninger til at sikre, at forsøg på uautoriseret adgang på virksomhedens anlæg forebygges, opdages og reageres på.

Stk. 2. Foranstaltninger efter stk. 1 skal som minimum omfatte:

1) Styret adgangskontrol, jf. § 37.
2) Sikring til at forsinke og besværliggøre fysisk indtrængen på anlægget.
3) Elektronisk overvågning til at opdage forsøg på indtrængen, herunder forsøg på sabotage, indbrud eller tyveri.
4) Elektronisk overvågning til at verificere forsøg på indtrængen på anlæg i klasse 4 og 5.

Stk. 3. Sikring efter stk. 2 skal også omfatte en generel perimetersikring, så uautoriserede personer, køretøjer eller fartøjer på vandet ikke kan få adgang til at bevæge sig ind på et anlægs perimeter uden at blive opdaget. For anlæg, der indgår som en del af en kontorbygning og almindelige kontorfaciliteter, som anvendes i leveringen af virksomhedens tjenester, kan der i stedet for perimetersikring alene anvendes skalsikring, jf. stk. 1 og 2.

Stk. 4. Virksomheder skal for anlæg i klasse 4 og 5 foretage celle- eller objektsikring af områder med adgang til forsyningskritiske net- og informationssystemer, arbejdsstationer, kritiske anlægskomponenter og netværksudstyr, der kan tilgå forsyningskritiske net- og informationssystemer, herunder kontrolrum, serverrum og datacentre.

Stk. 5. Virksomheder i niveau 4 og 5 skal på baggrund af en risikovurdering foretage visuel afskærmning af områder og udstyr, der kan give indsigt i forsyningskritisk energiinfrastruktur, herunder visuel afskærmning af kontrolrum.

Stk. 6. Virksomheder skal foretage kontrol med, at foranstaltninger efter stk. 2-5 gennemføres, er intakte og fungerer efter hensigten, herunder besigtige og afprøve anlægs fysiske sikring. Kontrollen for anlæg i klasse 2 og 3 skal foretages hvert kvartal. Kontrollen for anlæg i klasse 4 og 5 skal foretages hver måned.

§ 39. Virksomheder skal have procedurer for håndtering af alarmer om ulovlig indtrængen på virksomhedens anlæg, så alarmer håndteres på en hurtig og kvalificeret måde.

Stk. 2. Forsøg på indtrængen på anlæg skal uden unødigt ophold alarmeres til et døgnbemandet kontrolrum eller en af Rigspolitiet godkendt kontrolcentral.

Stk. 3. Virksomheder skal hvert kvartal foretage kontrol med, at procedurer for håndtering af alarmer efter stk. 1 og 2 gennemføres på effektiv vis.

§ 40. Virksomheder skal have en plan for, hvornår virksomheden i løbet af et år planlægger at gennemføre kontrol med et anlægs sikringsforanstaltninger, jf. § 36, stk. 8 og 9, § 37, stk. 5, § 38, stk. 6, § 39, stk. 3, § 42, stk. 2 og § 43, stk. 2.

Stk. 2. Fejl og mangler ved foranstaltningerne skal rettes hurtigt og årsagerne hertil undersøges.

Stk. 3. Virksomheder skal føre kontroljournaler over gennemførte kontroller. Kontroljournalerne skal som minimum indeholde følgende oplysninger:

1) Hvor kontrollen er foretaget.
2) Hvornår kontrollen er foretaget.
3) Hvordan kontrollen er foretaget.
4) Fejl og afvigelser der måtte konstateres.
5) Hvordan og hvornår fejl og afvigelser er afhjulpet.

Stk. 4. Virksomheder skal når fejl og afvigelser ikke kan afhjælpes inden for kort tid, udarbejde en plan for hvordan og hvornår fejlen eller afvigelsen vil være endelig afhjulpet.

Stk. 5. Virksomheder skal ved næstfølgende kontrol sikre, at fejl og afvigelser fra den forrige kontrol på ny kontrolleres så det kan konstateres, at de afhjælpende foranstaltninger virker efter hensigten.

§ 41. Virksomheder skal implementere foranstaltninger efter §§ 36-39 på anlæg, som er sammenbygget med andre anlæg, uanset sammenbygningen, i henhold til anlægget med højeste klasse.

§ 42. Virksomheder skal for rørledninger og kabler, som er nedgravet, hænger i luften, ligger på eller er nedgravet i havbunden, kun implementere foranstaltninger efter § 36, stk. 1 og 2, samt sikre, at anlægget overvåges, så funktionssvigt opdages og reageres på uden unødigt ophold.

Stk. 2. Virksomheder skal som minimum hvert halve år foretage kontrol med, at foranstaltninger efter stk. 1 gennemføres, er intakte og fungerer efter hensigten.

§ 43. Virksomheder skal have passende og forholdsmæssige foranstaltninger til at sikre, at forsøg på indtrængen og uautoriseret adgang på virksomhedens anlæg, lokationer, faciliteter, som ikke er klassificeret, men hvor der opbevares kritiske anlægskomponenter eller netværksudstyr, der kan tilgå net- og informationssystemer, opdages og uden unødigt ophold alarmeres til et døgnbemandet kontrolrum eller en af Rigspolitiet godkendt kontrolcentral.

Stk. 2. Virksomheder skal foretage stikprøvevis kontrol med, at foranstaltninger efter stk. 1 gennemføres, er intakte og fungerer efter hensigten, jf. § 40, stk. 2 og 3.

Kapitel 11

Sikkerhed i net- og informationssystemer

§ 44. Virksomheder skal have en politik for informationssystemsikkerhed til at fastlægge en overordnet ramme for sikkerhed i virksomhedens net- og informationssystemer.

§ 45. Virksomheder skal have procedurer for sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer. Procedurerne skal indeholde:

1) Krav til opretholdelse af et passende sikkerhedsniveau i net- og informationssystemer, som en virksomhed erhverver, udvikler og vedligeholder, herunder krav til sikkerheden i udviklings- og testmiljøer.
2) Metoder til at kontrollere, om de erhvervede eller udviklede net- og informationssystemer lever op til virksomhedens krav efter nr. 1.

§ 46. Virksomheder skal sikre, at virksomhedens net- og informationssystemer samt software- og hardwareaktiver, som anvendes i leveringen af virksomhedens tjenester, så vidt muligt hærdes, herunder gennem sikre konfigurationer, jf. § 49, samt med antimalware og nyeste system- og sikkerhedsopdateringer i hele deres livscyklus.

Stk. 2. System- og sikkerhedsopdateringer af forsyningskritiske net- og informationssystemer efter stk. 1, skal gennemføres på baggrund af en risikovurdering, hvor risici mod sikkerheden i systemerne evalueres i forhold til risici for opretholdelsen af virksomhedens evne til at levere sine tjenester.

§ 47. Virksomheder skal være i stand til at identificere, reagere på og mitigere sårbarheder, som kan påvirke sikkerheden i virksomhedens net- og informationssystemer.

Stk. 2. Virksomheder skal være i stand til at modtage varsler om sårbarheder på elektronisk vis.

Stk. 3. Virksomheder skal ved modtagelse af et varsel om en sårbarhed foretage en risikovurdering af virksomhedens eksponering og mitigere sårbarheder, som kan påvirke sikkerheden i virksomhedens net- og informationssystemer.

Stk. 4. Virksomheder i niveau 4 og 5 skal være i stand til at reagere på varsler efter stk. 2 og 3 uden unødigt ophold.

Stk. 5. Virksomheder skal tage stilling til, om sårbarheder, som virksomheden identificerer i virksomhedens net- og informationssystemer, bør offentliggøres, herunder i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, jf. § 45.

Stk. 6. Virksomheder skal sikre, at oplysninger om sårbarheder, som kan have sikkerhedsmæssig betydning for energisektoren, videreformidles til Energistyrelsen. Virksomheder i el-, gas- og brintsektoren skal ligeledes videreformidle oplysning om sårbarheder, til Energinet.

Forvaltning af software- og hardwareaktiver

§ 48. Virksomheder skal have ajourførte fortegnelser over følgende software- og hardwareaktiver:

1) Servere, databaser og netværksudstyr, som anvendes i forbindelse med leveringen af virksomhedens tjenester.

2) Endpoints og virtuelle maskiner, der kan tilgå virksomhedens net- og informationssystemer.
3) Software- og hardwareaktiver i virksomhedens forsyningskritiske net- og informationssystemer.

Stk. 2. Fortegnelserne skal være tilstrækkeligt detaljerede til at sikre hurtig identifikation af et aktiv, så eventuelle sårbarheder kan identificeres, vurderes og mitigeres, jf. § 47.

Stk. 3. Virksomhederne skal regelmæssigt og som minimum årligt kontrollere, at fortegnelser efter stk. 1 er ajourførte. Fejl og mangler skal rettes hurtigt og årsagerne hertil undersøges.

Stk. 4. Virksomhederne skal mitigere risici for software- og hardwareaktiver, jf. stk. 1, nr. 1-3, der anvendes i leveringen af virksomhedens tjenester, som ikke længere kan supporteres med system- og sikkerhedsopdateringer, jf. § 46, stk. 1.

§ 49. Virksomheder skal have procedurer til at sikre, at virksomhedens net- og informationssystemer samt software- og hardwareaktiver efter § 48 konfigureres på sikker vis, herunder at funktioner, services, applikationer, netværksprotokoller og porte, som ikke er nødvendige for at levere virksomhedens tjenester, lukkes eller deaktiveres.

Stk. 2. Procedurer efter stk. 1 skal omfatte sikker tilslutning af nye hardwareaktiver i de netværk, som virksomheden er afhængige af i leveringen af virksomhedens tjenester.

Stk. 3. Virksomheder skal logge væsentlige konfigurationsændringer i virksomhedens forsyningskritiske net- og informationssystemer.

Stk. 4. Virksomheder skal logge ændringer på netværksudstyr, der anvendes i segmenteringen af netværk efter § 62.

Stk. 5. Virksomheder skal regelmæssigt og som minimum årligt kontrollere, at virksomhedens net- og informationssystemer samt software- og hardwareaktiver efter § 48 er konfigureret efter stk. 1-4. Fejl og mangler skal rettes hurtigt og årsagerne hertil undersøges.

§ 50. Virksomheder i niveau 4 og 5 skal placere servere og datacentre, der understøtter virksomhedens forsyningskritiske net- og informationssystemer, inden for EU/EØS-lande.

Adgangsstyring

§ 51. Virksomheder skal have en politik for adgangskontrol til at sikre, at virksomhedens net- og informationssystemer beskyttes mod uautoriseret fysisk og logisk adgang.

§ 52. Virksomheder skal foretage adgangskontrol af adgange, identiteter og rettigheder til virksomhedens net- og informationssystemer. Adgangskontrollen skal understøtte følgende:

1) At adgange og rettigheder er personhenførbare og kun tildeles ved et arbejdsbetinget behov.
2) At inaktive identiteter, bruger- og servicekonti deaktiveres og fjernes.
3) At tildeling, ændring og fjernelse af adgange, identiteter, rettigheder og konti systematisk logges.

Stk. 2. Virksomheder skal som minimum gennemføre en kvartalvis sanering af adgange, identiteter og rettigheder til forsyningskritiske net- og informationssystemer.

§ 53. Virksomheder skal så vidt muligt og hvor relevant anvende multifaktorautentificering (MFA) eller kontinuerlig autentificering ved adgang til virksomhedens net- og informationssystemer jf. dog § 55, stk. 1.

§ 54. Virksomheder skal foretage styring af adgangselementer, herunder passwords til virksomhedens net- og informationssystemer samt til netværksudstyr, der kan påvirke leveringen af virksomhedens tjenester. Adgangsstyringen skal understøtte:

1) At anvendte adgangselementer modsvarer kritikaliteten af det pågældende net- og informationssystem eller netværksudstyr.
2) At der så vidt muligt sker tvungen udskiftning af passwords, så styrken af passwords modsvarer kritikaliteten af det pågældende net- og informationssystem eller netværksudstyr.

Stk. 2. Virksomheder skal foretage tvungen udskiftning af standardpasswords til net- og informationssystemer og netværksudstyr, inden at de tilsluttes virksomhedens netværk, jf. § 49, stk. 2.

§ 55. Virksomheder skal sikre, at fjernadgange til virksomhedens net- og informationssystemer beskyttes efter bestemmelserne i §§ 52-54.

Stk. 2. Fjernadgange til virksomhedens forsyningskritiske net- og informationssystemer skal tildeles i en tidsbegrænset periode, så fjernadgange kun er åbne i tidsrum med et godkendt arbejdsbetinget behov for at tilgå et system.

Stk. 3. Virksomheder skal udarbejde procedurer til at kunne opdage og håndtere cyberangreb mod fjernadgange til forsyningskritiske net- og informationssystemer.

§ 56. Virksomheder skal sikre, at mobile og stationære enheder, der kan tilgå virksomhedens industrielle kontrolsystemer og operationelle teknologier, ikke anvendes til privat brug og konfigureres på sikker vis, jf. § 49, så der kun kan installeres programmer, der skal anvendes i leveringen af tjenesten, på enheden.

§ 57. Virksomheder skal regelmæssigt kontrollere, at foranstaltninger efter §§ 52-56 gennemføres og fungerer efter hensigten. Fejl og mangler skal rettes hurtigt og årsagerne hertil undersøges.

Backup-styring

§ 58. Virksomheder skal have en politik og procedurer for backup-styring for virksomhedens net- og informationssystemer. Politikken skal som minimum indeholde minimumsfrekvens for at tage backup samt passende opbevaringstider for backup, jf. § 19, stk. 3, nr. 5, litra a.

§ 59. Virksomheder skal tage backup af virksomhedens forsyningskritiske net- og informationssystemer og netværkskonfigurationer, så virksomheden kan genoprette systemerne og netværksinfrastrukturen for forsyningskritiske net- og informationssystemer.

Stk. 2. Backups efter stk. 1 skal beskyttes og opbevares på sikker vis i henhold til kritikaliteten af det forsyningskritiske net- og informationssystem eller netværkskonfiguration, der tages backup af.

Stk. 3. Virksomheder i niveau 4 og 5 skal tage backup efter stk. 1 i flere kopier, så virksomheden kan tilgå backups, uagtet om det forsyningskritiske net- og informationssystem eller netværkskonfiguration, som der tages backup af, er utilgængelig eller kompromitteret. Backups skal opbevares særskilt, eksempelvis som offline kopier.

Kryptografi og sikret tale

§ 60. Virksomheder skal have politikker og procedurer for brug af kryptografi, og, hvor det er relevant, skal kryptering anvendes med henblik på at beskytte data, når data lagres, og når data overføres mellem netværk.

§ 61. Virksomheder skal anvende sikret tale-, video- og tekstkommunikation i virksomheden, hvor det er relevant, for at beskytte mod hændelser.

Netværkssegmentering og netværksdokumentation

§ 62. Virksomheder skal foretage netværkssegmentering, så virksomhedens forsyningskritiske net- og informationssystemer isoleres fra andre net- og informationssystemer og udstyr.

Stk. 2. Netværkssegmentering efter stk. 1, stk. 3 og stk. 5, skal ske ved brug af en demilitariseret zone eller tilsvarende, som skal placeres mellem det isolerede netværk med forsyningskritiske net- og informationssystemer og øvrige netværk.

Stk. 3. Virksomheder i niveau 4 og 5 skal fysisk adskille netværk med forsyningskritiske net- og informationssystemer fra andre netværk, jf. dog stk. 5.

Stk. 4. Multiforsyningsvirksomheder i niveau 4 og 5 skal sikre, at netværk med forsyningskritiske net- og informationssystemer er adskilt på tværs af forsyningsarter i henhold til stk. 3, medmindre det er forsyningskritisk net- og informationssystem til styring af et anlæg der leverer flere energiforsyningstjenester.

Stk. 5. Virksomheder i niveau 4 og 5 skal foretage netværkssegmentering for net- og informationssystemer, som anvendes i adgangskontrollen for anlæg, jf. § 37 og § 38, stk. 2, nr. 3 og 4. Net- og informationssystemerne kan placeres i samme fysiske netværk som forsyningskritiske net- og informationssystemer.

§ 63. Virksomheder skal have ajourført netværksdokumentation, der beskriver opbygningen af virksomhedens netværksinfrastruktur, herunder netværkssegmenteringen i § 62.

Stk. 2. Virksomheder skal have ajourført dokumentation over kommunikationsprotokoller, der anvendes i netværkssegmenter med forsyningskritiske net- og informationssystemer jf. § 62, herunder kommunikationsprotokoller med adgang til forsyningskritiske net- og informationssystemer.

Stk. 3. Virksomheder skal regelmæssigt og som minimum årligt kontrollere, at dokumentationen efter stk. 1 og 2 er opdateret.

Logning og monitorering

§ 64. Virksomheder skal have en logpolitik til at fastlægge en overordnet ramme for logning og monitorering i virksomhedens net- og informationssystemer. Logpolitikken skal som minimum indeholde følgende:

1) Metoder for systematisk opsamling af logs, som er nødvendige for at identificere og efterforske hændelser.
2) Metoder for monitorering af logs.
3) Ansvar for monitorering af logs.
4) Opbevaringstid for opbevaring af logs.

§ 65. Virksomheder i niveau 2 og 3 skal i fornødent omfang implementere logning og monitorering i virksomhedens net- og informationssystemer og netværksinfrastruktur med henblik på at kunne identificere hændelser og nærvedhændelser samt understøtte myndighedernes efterforskning.

§ 66. Virksomheder i niveau 4 og 5 skal implementere logning og monitorering i virksomhedens net- og informationssystemer og netværksinfrastruktur med henblik på at kunne identificere hændelser og nærvedhændelser i realtid samt understøtte myndighedernes efterforskning.

Stk. 2. Virksomheder i niveau 4 og 5 skal som minimum logge følgende:

1) Steder, hvorfra der går datatrafik ind og ud af virksomhedens netværk, herunder firewalls og internetvendte tjenester.
2) På hardware og software der understøtter leveringen af tjenesten, herunder netværkskomponenter og udstyr til fjernadgang, hvor det er muligt og de genererede logs viser forbindelser og brugerhandlinger.
3) På hardware og software der understøtter et anlægs adgangskontrol, jf. 38. stk. 2.

§ 67. Logs efter § 65 og § 66 skal være tidssynkroniserede og skal beskyttes med foranstaltninger, der garanterer, at logs opbevares på sikker vis i henhold til kritikaliteten af det net- og informationssystem eller netværksudstyr, hvorfra der opsamles logs.

Stk. 2. Logs skal opbevares særskilt fra det net- og informationssystemer og netværksudstyr, hvorfra der opsamles logs, og skal sikres mod manipulation og beskyttes mod uautoriseret adgang.

Stk. 3. Virksomheder i niveau i 4 og 5 skal opbevare logs efter § 66 i 13 måneder.

§ 68. Virksomheder i niveau 4 og 5 skal være i stand til at reagere på uregelmæssigheder i net- og informationssystemer og netværksinfrastruktur i realtid med henblik på at sikre, at hændelser håndteres uden unødigt ophold.

§ 69. Virksomheder skal planlægge logning og monitoreringen jf. §§ 65-68 i koordination med virksomhedens it-sikkerhedstjeneste, så der opsamles og monitoreres logs af relevans for it-sikkerhedstjenestens hændelseshåndtering.

Stk. 2. Virksomheder i niveau 4 og 5 skal være i stand til at afgive logs til it-sikkerhedstjenesten inden for 24 timer.

§ 70. Virksomheder skal regelmæssigt og som minimum årligt kontrollere, at der opsamles korrekte logs fra virk-

somhedens net- og informationssystemer, og at logs kan anvendes til at identificere og efterforske hændelser. Fejl og mangler skal rettes hurtigt, og årsagerne hertil undersøges.

Evaluering af sikkerheden i net- og informationssystemer

§ 71. Virksomheder skal udarbejde en politik og procedurer for vurdering af effektiviteten af foranstaltninger, som virksomheden implementerer til at understøtte sikkerheden i net- og informationssystemer efter denne bekendtgørelse, og for vurdering af behov for tekniske sikkerhedsscanninger, eksempelvis i form af sårbarhedsscanninger og penetrationstests.

Kapitel 12

Håndtering af hændelser

§ 72. Hændelser skal håndteres af den enkelte virksomhed med udgangspunkt i virksomhedens beredskabsplaner med de nødvendige tilpasninger til situationen.

Stk. 2. Virksomheder i niveau 3-5 skal i forbindelse med håndteringen af en hændelse være i stand at indsætte tilstrækkeligt personale og teknisk assistance på alle tider af døgnet, så virksomheden kan opretholde eller genoprette virksomhedens tjenester.

§ 73. Virksomheder skal have et operationelt kontaktpunkt inden for egen organisation, som myndigheder og virksomheder, der forestår sektorberedskabet, kan kontakte.

Stk. 2. Det operationelle kontaktpunkt skal være i stand til at modtage udmeldinger om ændringer i sektorberedskabsniveau på alle tider af døgnet, så virksomheden kan iværksætte sektorberedskabsforanstaltninger i henhold til § 13, stk. 3, og videreformidle information og udmeldinger internt i virksomheden.

Stk. 3. Virksomheder skal holde Energistyrelsen underrettet om opdaterede kontaktoplysninger på virksomhedens operationelle kontaktpunkt, jf. dog stk. 4.

Stk. 4. Virksomheder i henholdsvis el-, gas- og brintsektoren skal holde Energinet underrettet om opdaterede kontaktoplysninger på virksomhedens operationelle kontaktpunkt.

§ 74. Virksomheder skal være i stand til at opretholde kommunikationslinjer eller anvende alternative kommunikationsformer i forbindelse med håndteringen af en hændelse.

Underretningsforpligtelser

§ 75. Virksomheder skal uden unødigt ophold underrette modtagerne af deres tjenester om væsentlige hændelser jf. § 77, der sandsynligvis vil påvirke leveringen af virksomhedens tjenester negativt.

Stk. 2. Virksomhederne skal sammen ved underretningen efter stk. 1, så vidt muligt angive:

1) De forventede konsekvenser, faktiske konsekvenser samt den forventede varighed af hændelsen.
2) Eventuelle foranstaltninger eller modforholdsregler, som modtagerne af virksomhedens tjeneste kan træffe for at afbøde risici eller konsekvenser som følge af den pågældende hændelse.
3) Tidspunkter for yderligere information.

§ 76. Virksomheder skal uden unødigt ophold oplyse modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, om eventuelle foranstaltninger eller modforholdsregler, som modtagerne kan træffe som reaktion herpå. Enhederne skal også informere de pågældende modtagere om den væsentlige cybertrussel, hvor det er relevant.

Stk. 2. Oplysninger om væsentlige cybertrusler skal stilles til rådighed for modtagerne i et let forståeligt sprog.

Stk. 3. Virksomheder må ikke tage betaling fra modtagerne af deres tjenester for at give underretninger efter stk. 1.

Stk. 4. Virksomheder er ved oplysning efter stk. 1, ikke fritaget fra at træffe passende og øjeblikkelige foranstaltninger til at forebygge eller afhjælpe enhver trussel eller hændelses negative eller potentielle negative indvirkning på modtagerne af virksomhedens tjenester.

§ 77. Virksomheder skal uden unødigt ophold og under alle omstændigheder underrette Energistyrelsen om enhver hændelse, der har en væsentlig indvirkning på leveringen af virksomhedens tjenester, jf. dog stk. 4 og 5.

Stk. 2. Væsentlige hændelser efter stk. 1 omfatter:

1) Hændelser, som har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser i leveringen af virksomhedens tjenester, herunder som følge af havari af anlæg, arbejdsmarkedskonflikter og manglende leverancer af væsentlig betydning for samfundets energiforsyning.
2) Hændelser, som har forårsaget eller er i stand til at forårsage økonomisk tab for den berørte virksomhed.
3) Hændelser, som har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig fysisk eller ikke-fysisk skade.
4) Hændelser, som har aktiveret eller burde have aktiveret virksomhedens beredskabsplaner, herunder:
   a) Hændelser, hvor et net- og informationssystems fortrolighed, integritet, tilgængelighed og autenticiteten er blevet kompromitteret.
   b) Hændelser, hvor der er begrundet mistanke om eller kendskab til indbrud, tyveri, sabotage og spionage.
   c) Hændelser, der har krævet bistand til situationsudredning, udbedring og genopretning af virksomhedens net- og informationssystemer, herunder fra en it-sikkerhedstjeneste, CSIRT og Energinet.

Stk. 3. Virksomheder skal uden unødigt ophold og senest inden for 24 timer efter at have fået kendskab til en væsentlig hændelse underrette Energistyrelsen. Virksomheden skal ved indberetning i videst muligt omfang angive følgende oplysning om hændelsen:

1) Hændelsens kendetegn, art eller type.
2) Hændelsens årsag og hændelsesforløb.
3) Hændelsens konsekvenser.
4) Om hændelsen mistænkes for at være forårsaget af ulovlige eller ondsindede handlinger.
5) Om hændelsen kunne have haft en grænseoverskridende virkning.

Stk. 4. Virksomheder skal inden for 72 timer efter at have fået kendskab til en væsentlig hændelse underrette Energi-

styrelsen, om status på hændelsen, herunder give en indledende vurdering af hændelsens alvor, indvirkning og hvis muligt kompromitteringsindikatorerne.

Stk. 5. Virksomheder skal underrette CSIRT'en ved væsentlige hændelser, hvor hændelsen har kompromitteret sikkerheden i virksomhedens net- og informationssystemer, på samme måde som underretninger til Energistyrelsen efter stk. 2, nr. 1-3, stk. 3-4, og § 78, stk. 1 og 2.

Stk. 6. Virksomheder i henholdsvis el-, gas- og brintsektoren skal uden unødigt ophold varsle Energinet om væsentlige hændelser efter stk. 2 i henhold til stk. 3-5.

Stk. 7. Virksomheder skal efter anmodning fra Energistyrelsen eller sikkerhedsmyndighederne herunder CSIRT'en fremsende en foreløbig rapport om relevante statusopdateringer.

§ 78. Virksomheder skal senest én måned efter hændelsesunderretningen i § 77, stk. 4, sende en hændelsesrapport til Energistyrelsen. Hændelsesrapporten skal indeholde en detaljeret beskrivelse af hændelsen og virksomhedens håndtering af hændelsen, herunder:

1) Hændelsens alvor og indvirkning.
2) Antallet og andelen af brugere berørt af en eventuel forstyrrelse i leveringen af tjenesten samt forstyrrelsens varighed.
3) Geografisk område berørt at en eventuel forstyrrelse i leveringen af tjenesten.
4) Den type trussel eller grundlæggende årsag, der sandsynligvis har udløst hændelsen.
5) Anvendte og igangværende afbødende foranstaltninger.
6) Eventuelle grænseoverskridende virkninger af hændelsen.
7) En beskrivelse af samarbejdet med eksterne parter i håndteringen af hændelsen.
8) Opnåede erfaringer og læringspunkter fra virksomhedens håndtering af hændelsen.
9) Planlagt opfølgning på erfaringer og læringspunkter efter nr. 8, herunder tidsplan for opfølgning.

Stk. 2. Hvis en hændelse pågår for tidspunktet for hændelsesrapporten i stk. 1, kan virksomheden sende en foreløbig rapport med relevante statusopdateringer på det pågældende tidspunkt og en endelig hændelsesrapport senest en måned efter virksomhedens håndtering af hændelsen.

Stk. 3. Virksomheder kan i forbindelse med stk. 2 ansøge Energistyrelsen om, at hændelsesevalueringen i stk. 1 godkendes som en øvelsesevaluering, jf. § 23, hvis virksomheden har afprøvet konkrete øvelseselementer i bilag 4 i håndteringen af hændelsen. Ansøgninger om godkendelse af hændelse som en øvelse skal vedlægges en opdateret øvelsesplan, jf. § 20.

§ 79. Underretning om væsentlige hændelser, hvor hændelsen har kompromitteret sikkerheden i virksomhedens net- og informationssystemer, efter § 77, stk. 1-5, og § 78, stk. 1 og 2, skal indberettes til CSIRT'en og Energistyrelsen via den af CSIRT'en anviste løsning for underretning, jf. dog stk. 2.

Stk. 2. Underretning om alle andre væsentlige hændelser efter § 78 skal ske gennem den af Energistyrelsen anviste løsning for underretning.

Stk. 3. Ansøgninger om godkendelse af en hændelse som en øvelse efter § 78, stk. 3, skal sendes til Energistyrelsen gennem den af Energistyrelsen anviste løsning for ansøgning.

§ 80. Virksomheder skal anmelde hændelser på land, hvor der er begrundet mistanke om eller kendskab til indbrud, tyveri, sabotage og spionage til politiet.

Stk. 2. Virksomheder skal anmelde hændelser på havet, hvor der er begrundet mistanke om eller kendskab til indbrud, tyveri, sabotage og spionage til politiet og Forsvaret.

Kapitel 13

Energinets opgavevaretagelse i forbindelse med sektorberedskabet

§ 81. Energinet skal varetage de koordinerende, planlægningsmæssige og operative opgaver i sektorberedskabet før, under og efter en hændelse for henholdsvis el-, gas- og brintsektoren, herunder:

1) Indhente og videreformidle data og information, der er nødvendig for sektorberedskabet, mellem myndigheder og virksomheder i henholdsvis el-, gas- og brintsektoren, herunder data og information af betydning for forsyningssikkerheden.
2) Udmelde ændringer i sektorberedskabsniveau og iværksættelse af sektorberedskabsforanstaltninger for henholdsvis el-, gas- og brintsektoren.
3) Forestå krisehåndteringen ved aktivering af sektorberedskabsplaner for henholdsvis el-, gas- og brintsektoren.

Stk. 2. Energinet skal i forbindelse med krisehåndteringen efter stk. 1, nr. 3, indhente relevant og opdateret information om henholdsvis:

1) Situationen i nabolandes el-, gas- og brintforsyningssystemer af relevans for krisehåndteringen i henholdsvis el-, gas- og brintsektoren.
2) Situationen i væsentlige dele af det indenlandske elnet, også på spændingsniveauer under 100 kV.
3) Situationen i væsentlige dele af de indenlandske gas- og brintforsyningssystemer, herunder også distribution, produktion og lager.

Stk. 3. Energinet skal ved forsyningsafbrydelser, som berører flere virksomheder i henholdsvis el-, gas- og brintsektoren, koordinere krisehåndteringen på tværs af relevante virksomheder og Energistyrelsen, herunder bistå med kontaktoplysninger til virksomheder og myndigheder i en akut situation samt oplysninger om aktuelle driftstilstande til brug for virksomheders håndtering af hændelser.

Stk. 4. Energinet skal til enhver tid og uden unødigt ophold kunne modtage og videreformidle information af betydning for beredskabet fra myndigheder og andre aktører, til relevante virksomheder i henholdsvis el-, gas- og brintsektoren og Energistyrelsen.

§ 82. Energinet skal etablere et formaliseret samarbejde om beredskabsforhold i henholdsvis el-, gas- og brintsektoren, herunder gennem vidensdeling og møder om beredskab, fysisk sikring og cybersikkerhed.

§ 83. Energinet skal varetage arbejdet for henholdsvis el-, gas- og brintsektoren i de lokale beredskabsstabe, som er etableret af politikredsene, og kan inddrage relevante virksomheder heri. Energinet skal sammen med Energistyrelsen kunne indgå i den nationale krisestyring.

§ 84. Energinet kan udsende beredskabsmeddelelser om el-, gas- og brintforsyningen i henhold til aftale mellem DR, TV 2/DANMARK A/S, Rigspolitiet og Beredskabsstyrelsen om fremgangsmåden ved udsendelse af beredskabsmeddelelser (varslingsaftalen).

§ 85. Energinet skal føre en fortegnelse over informationsstrømme i digital og fysisk form, som indgår i styringskritiske funktioner og beslutningsprocesser i sektorberedskabet for henholdsvis el-, gas-, og brintsektoren. Fortegnelsen skal indeholde et samlet overblik over de indbyrdes relationer for aktørerne i forsyningssystemerne for henholdsvis el-, gas-, og brintsektoren samt en vurdering af risici for tab af fortrolighed, integritet og tilgængelighed for informationsstrømmene.

Stk. 2. Fortegnelsen skal holdes opdateret, så fortegnelsen altid er retvisende.

§ 86. Energinet skal årligt den 1. marts udarbejde en sektorrisiko- og sårbarhedsvurdering for henholdsvis el-, gas- og brintforsyningssystemerne i Danmark, første gang i 2026.

Stk. 2. Sektorrisiko- og sårbarhedsvurderinger efter stk. 1 skal baseres på konklusioner fra virksomheders risiko- og sårbarhedsvurderinger, jf. § 107, i henholdsvis el-, gas- og brintsektoren. Energistyrelsen sender senest den. 1. november hvert år konklusionerne til Energinet

Stk. 3. Sektorrisiko- og sårbarhedsvurderinger skal inkludere risici forbundet med forsyningssystemernes sammenhænge med relevante forsyningssystemer i udlandet og gensidige afhængigheder.

Stk. 4. Energistyrelsen kan påbyde Energinet at opdatere og sende en opdateret sektorrisiko- og sårbarhedsvurdering til Energistyrelsen ved ændringer i trusselsbilledet eller forsyningssituationen i øvrigt indenfor en nærmere fastsat frist.

§ 87. Energinet skal udarbejde sektorberedskabsplaner for henholdsvis el-, gas- og brintforsyningssystemerne i Danmark. Sektorberedskabsplanerne skal angive, hvordan Energinet planlægger at styre kriseindsatsen på en koordineret måde. Sektorberedskabsplaner skal indeholde:

1) Ansvarsfordelingen mellem virksomheder i henholdsvis el-, gas- og brintsektoren og Energinet.
2) Beskrivelse af hvordan Energinet planlægger at informere virksomheder i henholdsvis el-, gas- og brintsektoren om ændringer i sektorberedskabet, således at der opnås en fælles situationsforståelse hos virksomheder.
3) Krav til form på og indhold i situationsrapporter, som virksomheder i henholdsvis el-, gas- og brintsektoren skal sende til Energinet i forbindelse med håndteringen af en hændelse, som har aktiveret sektorberedskabsplanerne.
4) Beskrivelse af kommunikationsveje, herunder alternative kommunikationsveje og forholdsregler i forbindelse med kompromittering af normale kommunikationsveje.
5) Instruktion om kryptering af information og driftsordrer.

Stk. 2. Sektorberedskabsplanerne skal være koordineret på tværs af henholdsvis el-, gas- og brintsektoren.

Stk. 3. Sektorberedskabsplanerne skal forholde sig til relevante forsyningssystemer i udlandet og være koordineret med de relevante systemansvarlige virksomheder i udlandet.

§ 88. Sektorberedskabsplaner efter § 87 skal opdateres senest tre måneder efter gennemførelse eller opdatering af en sektorrisiko- og sårbarhedsvurdering, jf. § 86.

Stk. 2. Sektorberedskabsplanerne skal være versionsstyret med en kort beskrivelse af ændringer i forhold til tidligere versioner.

Stk. 3. Energinet skal årligt den 1. april sende opdaterede sektorberedskabsplaner for henholdsvis el-, gas- og brintsektoren til Energistyrelsen, første gang i 2026.

Stk. 4. Energistyrelsen skal godkende sektorberedskabsplanerne for henholdsvis el-, gas- og brintsektoren. Sektorberedskabsplanerne må tages i brug under godkendelsesprocessen.

§ 89. Energinet skal mindst én gang hvert andet år afholde sektorberedskabsøvelser for henholdsvis el-, gas- og brintsektoren med udgangspunkt i sektorberedskabsplanerne i § 87.

§ 90. Energinet skal have en plan over sektorøvelser, som Energinet planlægger at gennemføre for henholdsvis el-, gas- og brintsektoren over en femårig periode. Planen skal deles med berørte virksomheder.

Stk. 2. Den femårige øvelsesplan for sektorberedskabet skal som minimum dække øvelseselementerne nr. 1-11, 13-14, 16-17 og 19 i bilag 4.

Stk. 3. Energinet skal første gang udarbejde en femårig øvelsesplan for sektorberedskabet, som dækker perioden fra den 1. april 2025 til den 31. marts 2030. Derefter udarbejdes en ny øvelsesplan for en ny femårig periode.

Stk. 4. Den femårige øvelsesplan for sektorberedskabet er tentativ og skal opdateres én gang årligt og ved væsentlige ændringer.

§ 91. Energinet skal evaluere sektorberedskabsøvelser som gennemføres i henhold til § 89. Energinet skal involvere relevante virksomheder i evalueringsprocessen.

Stk. 2. Energinet skal udarbejde og sende en øvelsesevaluering til godkendelse i Energistyrelsen senest tre måneder efter, at en sektorberedskabsøvelse er afholdt. Øvelsesevalueringen skal indeholde elementerne beskrevet i § 23, stk. 2.

Stk. 3. Energinet skal videreformidle konklusioner fra øvelsesrapporten til virksomheder omfattet af sektorberedskabet i henholdsvis el-, gas- og brintsektoren.

§ 92. Energistyrelsen kan godkende, at en evaluering af en hændelse, som har aktiveret henholdsvis sektorberedskabsplaner for el-, gas- og brintsektoren, kan indgå som en sektorberedskabsøvelse i sektorberedskabets øvelsesplan. Energinet skal i forbindelse med ansøgningen sende en opdateret øvelsesplan for sektorberedskabet sammen med en hændelsesevaluering efter § 78.

§ 93. Energinet skal årligt gennemføre funktionstests af teknisk udstyr, som Energinet planlægger at anvende i forbindelse med aktiveringen af sektorberedskabsplaner for henholdsvis el-, gas- og brintsektoren, herunder test af alternative kommunikationsmidler og teknisk kontrol af kommunikationsveje.

§ 94. Energinet skal senest 1. maj hvert år fremsende en årlig redegørelse til Energistyrelsen om status på henholdsvis el-, gas- og brintsektorens beredskab, herunder om virksomhedens beredskabsarbejde for henholdsvis el-, gas- og brintsektoren i det forløbne år.

Kapitel 14

Energistyrelsens opgavevaretagelse i forbindelse med sektorberedskabet

§ 95. Energistyrelsen varetager de koordinerende, planlægningsmæssige og operative opgaver i sektorberedskabet før, under og efter en krise for henholdsvis olie-, fjernvarme- og fjernkølingssektoren, herunder:

1) Indhentning og videreformidling af data og information, der er nødvendig for sektorberedskabet, mellem myndigheder og virksomheder i henholdsvis olie-, fjernvarme- og fjernkølingssektoren.
2) Udmelding om ændringer i sektorberedskabsniveau og iværksættelse af sektorberedskabsforanstaltninger for virksomheder i henholdsvis olie-, fjernvarme- og fjernkølingssektoren.
3) Krisehåndteringen ved aktivering sektorberedskabsplaner for henholdsvis olie-, fjernvarme- og fjernkølingssektoren.

Stk. 2. I tilfælde af større forsyningsafbrydelser, som berører flere virksomheder i henholdsvis olie-, fjernvarme- og fjernkølingssektoren, koordinerer Energistyrelsen krisehåndteringen med de relevante virksomheder.

Stk. 3. Energistyrelsen sender uden unødigt ophold relevant information om beredskabsmæssige forhold til relevante virksomheder i henholdsvis olie-, fjernvarme- og fjernkølingssektoren samt Energinet.

§ 96. Energistyrelsen etablerer et formaliseret samarbejde om beredskabsforhold i henholdsvis olie-, fjernvarme- og fjernkølingssektoren, herunder gennem vidensdeling og møder om beredskabsforhold, fysisk sikring og cybersikkerhed.

§ 97. Energistyrelsen varetager arbejdet for henholdsvis olie-, fjernvarme- og fjernkølingssektoren i de lokale beredskabsstabe, som er etableret af politikredsene, og kan inddrage relevante virksomheder heri.

§ 98. Energistyrelsen kan udsende beredskabsmeddelelser om henholdsvis olie-, fjernvarme- og fjernkølingsforsyningen i henhold til aftale mellem DR, TV 2/DANMARK A/S, Rigspolitiet og Beredskabsstyrelsen om fremgangsmåden ved udsendelse af beredskabsmeddelelser (varslingsaftalen).

§ 99. Energistyrelsen udarbejder årligt den 1. marts en sektorrisiko- og sårbarhedsvurdering for henholdsvis olie-, fjernvarme- og fjernkølingsforsyningssystemerne i Danmark, første gang i 2026. Sektorrisiko- og sårbarhedsvurdering udarbejdes på baggrund af konklusioner fra virksomheders risiko- og sårbarhedsvurderinger, jf. § 107.

§ 100. Energistyrelsen udarbejder sektorberedskabsplaner for henholdsvis olie-, fjernvarme- og fjernkølingssektoren i Danmark. Sektorberedskabsplanerne angiver, hvordan Energistyrelsen planlægger at styre kriseindsatsen på en koordineret måde, så der opnås en fælles situationsforståelse ved ændringer i sektorberedskabet for henholdsvis olie-, fjernvarme- og fjernkølingssektoren.

Stk. 2. Energistyrelsen koordinerer i fornødent omfang sektorberedskabsplanerne efter stk. 1 på tværs af olie-, fjernvarme- og fjernkølingssektoren såvel som med Energinets sektorberedskabsplaner efter § 87.

Stk. 3. Sektorberedskabsplaner efter stk. 1 skal opdateres senest tre måneder efter gennemførelse af en sektorrisiko- og sårbarhedsvurdering, jf. § 99.

§ 101. Energistyrelsen afholder mindst hvert andet år sektorberedskabsøvelser for henholdsvis olie-, fjernvarme- og fjernkølingssektoren med udgangspunkt i sektorberedskabsplanerne efter § 100.

§ 102. Energistyrelsen udarbejder en plan over sektorøvelser, som Energistyrelsen planlægger at gennemføre for henholdsvis olie-, fjernvarme- og fjernkølingssektoren over en femårig periode. Planen deles med berørte virksomheder.

Stk. 2. Den femårige øvelsesplan for sektorberedskabet dækker øvelseselementer i bilag 4, som Energistyrelsen vurderer er relevante for henholdsvis olie-, fjernvarme- og fjernkølingssektoren.

Stk. 3. Den femårige øvelsesplan for sektorberedskabet udarbejdes første gang, så den dækker perioden fra 1. april 2025 til 31. marts 2030. Derefter udarbejdes en ny øvelsesplan for en ny femårig periode.

§ 103. Energistyrelsen udarbejder en evaluering af afholdte sektorberedskabsøvelser senest tre måneder efter, at en sektorberedskabsøvelse er afholdt.

Stk. 2. Energistyrelsen videreformidler konklusioner fra en sektorberedskabsøvelses evaluering til virksomhederne i olie-, fjernvarme- og fjernkølingssektoren.

Kapitel 15

Fortrolighed, udveksling af oplysninger og digital kommunikation

§ 104. Fortrolig information jf. § 26 i lov om styrket beredskab i energisektoren, skal opbevares, håndteres og behandles på en måde, der sikrer fortrolighed, integritet og tilgængelighed.

Stk. 2. Indsigt i fortrolig information må kun gives til personer, for hvem en sådan indsigt er tjenestelig nødvendig, eller som kan gøre lovkrav herpå.

Stk. 3. Fortrolig information i fysisk og digital dokumentform skal bære tydelig mærkning af materialets fortrolighed.

Stk. 4. Dokumenter efter stk. 3 og bærbare digitale lagringsmedier, der har været anvendt til at lagre fortrolig information, som ikke længere benyttes, skal destrueres eller bortskaffes på sikker vis i overensstemmelse med materialets fortrolighed, medmindre andet følger af lov eller bestemmelser fastsat i medfør af lov.

Stk. 5. Hvis der konstateres eller er mistanke om kompromittering af fortroligheden og integriteten af fortrolig information, skal der foretages en vurdering af, hvorvidt kompromitteringen kan udgøre en trussel for driften af virksomheden eller energiforsyningen lokalt, regionalt, nationalt eller på europæisk niveau. For fortrolig information hos virksomheder foretages denne vurdering af virksomheden, som uden unødigt ophold skal underrette Energistyrelsen herom. For anden fortrolig information foretages vurderingen af Energistyrelsen.

Stk. 6. Energistyrelsen kan pålægge virksomheder at iværksætte mitigerende tiltag i tilfælde af hændelser, jf. stk. 5.

§ 105. Skriftlig kommunikation fra virksomheder til Energistyrelsen om forhold, der er omfattet af lov om styrket beredskab i energisektoren og denne bekendtgørelse, skal ske digitalt gennem den af Energistyrelsen anviste selvbetjeningsløsning.

Stk. 2. Ved skriftlig kommunikation efter stk. 1, forstås afsendelse og modtagelse af alle relevante meddelelser, dokumenter og anden kommunikation, som påkrævet efter bestemmelser i lov om styrket beredskab i energisektoren eller denne bekendtgørelse.

Stk. 3. Stk. 1. finder ikke anvendelse for virksomheder, som er fritaget fra obligatorisk tilslutning til Digital Post efter bekendtgørelse om fritagelse af juridiske enheder med CVR-nummer, samt fysiske personer med erhvervsaktiviteter for tilslutning til Digital Post.

Stk. 4. Den digitale kommunikation skal være forsynet med den offentlige digitale signatur MitID Erhverv.

§ 106. Den digitale kommunikation, som er forsynet med den digitale signatur efter § 105, stk. 4, anses for at være kommet frem på det tidspunkt, hvor den er tilgængelig for Energistyrelsen.

Stk. 2. Den digitale kommunikation, som er forsynet med den digitale signatur efter § 105, stk. 4, anses for at være afsendt af den angivne afsender.

Stk. 3. Skriftlig kommunikation fra virksomheder til Energistyrelsen om forhold omfattet af § 105, stk. 1, anses ikke for modtaget i Energistyrelsen, hvis virksomheden har indsendt den skriftlige kommunikation på anden måde end beskrevet i § 105.

Stk. 4. Energistyrelsen kan i særlige tilfælde behandle en skriftlig kommunikation modtaget på anden måde end beskrevet i § 105.

Stk. 5. Energistyrelsen kan i særlige tilfælde behandle en skriftlig kommunikation, der er modtaget digitalt i henhold til § 105, selv om den ikke er forsynet med digital signatur, som beskrevet i § 105, stk. 4.

Kapitel 16

Tilsyn og Energistyrelsens godkendelse af virksomheders beredskabsplangrundlag

§ 107. Energistyrelsen skal godkende virksomheders konklusioner på risiko- og sårbarhedsvurdering, jf. § 18, og beredskabsplaner, jf. § 19. Beredskabsplaner må tages i brug under godkendelsesprocessen.

Stk. 2. Virksomheder i niveau 4 og 5 skal hvert år den 1. oktober sende konklusioner på en opdateret risiko- og sårbarhedsvurdering, jf. § 18, og opdaterede beredskabsplaner, jf. § 19, til Energistyrelsen, dog for 2025 den 7. september.

Stk. 3. Virksomheder i niveau 2 og 3 skal hvert tredje år den 1. oktober sende konklusioner på en opdateret risiko- og sårbarhedsvurdering, jf. § 18, og opdaterede beredskabsplaner, jf. § 19, til Energistyrelsen. Virksomheder i fjernvarme- og fjernkølingssektoren skal sende første gang den 1. oktober 2025. Virksomheder i henholdsvis gas-, brint- og oliesektoren skal sende første gang den 1. oktober 2026. Virksomheder i elsektoren skal sende første gang den 1. oktober 2027.

Stk. 4. Virksomheder i niveau 1 skal fremsende deres beredskabsplaner, jf. § 19, stk. 1-5, til Energistyrelsen efter anmodning herom fra Energistyrelsen.

Stk. 5. Energistyrelsen udarbejder risiko- og sårbarhedsscenarier, som skal indgå i virksomheders risiko- og sårbarhedsvurdering, jf. § 18. Risiko- og sårbarhedsscenarier skal deles med virksomhederne senest seks måneder inden, at virksomheder skal sende konklusioner på en opdateret risiko- og sårbarhedsvurdering til Energistyrelsen i henhold til stk. 2-4.

Stk. 6. Energistyrelsen kan påbyde virksomheder at opdatere deres risiko- og sårbarhedsvurdering ved ændringer i trusselsbilledet. Virksomheder skal uden unødigt ophold sende en opdateret risiko- og sårbarhedsvurdering til Energistyrelsen.

§ 108. Energistyrelsens tilsyn med virksomheder gennemføres frekvensbaseret som specificeret i stk. 2-4.

Stk. 2. For virksomheder i niveau 4 og 5, føres der tilsyn hvert år.

Stk. 3. For virksomheder i niveau 3, føres der tilsyn hvert tredje år.

Stk. 4. For virksomheder i niveau 2, føres der tilsyn hvert sjette år.

§ 109. Energistyrelsens tilsyn gennemføres ved brug af stikprøver, der vurderes at afspejle en virksomheds samlede overholdelse af reglerne i rimeligt omfang.

Stk. 2. Energistyrelsens tilsyn kan gennemføres på anden vis, hvis Energistyrelsen vurderer, at situationen nødvendiggør et dybdegående tilsyn.

Stk. 3. Energistyrelsen kan basere dele af tilsynet på en virksomheds auditering i det omfang, at Energistyrelsen vurderer, at auditering dækker de forhold, der føres tilsyn med.

§ 110. Energistyrelsen varsler skriftligt virksomheder om gennemførelse af et fysisk tilsyn senest 21 dage før tilsynet skal finde sted.

§ 111. Energistyrelsen kan kræve, at virksomheder oversætter materiale til dansk, når dette materiale skal bruges til Energistyrelsens tilsyn. Omkostningen med sådan oversættelse afholdes af virksomheden selv.

§ 112. Energistyrelsen udarbejder en rapport på baggrund af gennemførte tilsyn. Rapporten forelægges virksomheder til kommentering inden færdiggørelse.

Stk. 2. Virksomheder kan sende et eventuelt høringssvar senest to uger efter rapporten er blevet den forelagt efter stk. 1.

Stk. 3. Virksomheder skal snarest muligt efter endt tilsyn forelægge Energistyrelsens tilsynsrapport for virksomhedens ledelsesorgan, med henblik på ledelsens håndtering af Energistyrelsens afgørelser.

Kapitel 17

Samordnet beredskab

§ 113. Virksomheder kan skriftligt ansøge om at etablere samordnet beredskab, der medfører, at beredskabsarbejdet efter lov om styrket beredskab i energisektoren, bekendtgørelse om sikkerhedsgodkendelser i energisektoren og denne bekendtgørelse varetages i fællesskab eller af den ene part.

Stk. 2. Ansøgninger om samordnet beredskab skal sendes til Energistyrelsen til godkendelse og skal som minimum indeholde følgende:

1) En begrundelse for ansøgningen.
2) En beskrivelse af de geografiske forhold mellem virksomhederne.
3) En beskrivelse af organisatoriske forhold hos virksomhederne og forskellene herved.
4) En beskrivelse af fordele og ulemper ved de praktiske og tekniske konsekvenser ved et samordnet beredskab.
5) Hvordan den operative indsats af virksomhederne skal håndteres, herunder angivelse af virksomhedernes indbyrdes ansvars- og kompetenceforhold, samt kommunikations- og informationsforhold.

Stk. 3. Energinet skal høres ved ansøgninger om samordnet beredskab for virksomheder i henholdsvis el-, gas- og brintsektoren.

Stk. 4. Energistyrelsen lægger i sin afgørelse vægt på, om en samordning af beredskabet for virksomhederne må anses at styrke modstandsdygtigheden og beredskabet hos hver enkelt virksomhed, virksomhederne som gruppe og energisektoren som helhed.

Kapitel 18

Identificering af særlige virksomheder

§ 114. Energistyrelsen identificerer og udarbejder en liste over væsentlige og vigtige enheder.

Stk. 2. Energistyrelsen udfører de stk. 1, nævnte opgaver første gang senest den 17. april, 2025 og derefter når det er relevant, dog mindst hvert andet år.

Stk. 3. Energistyrelsen identificerer efter stk. 1, virksomheder som væsentlige virksomheder, hvis de opfylder en af følgende betingelser:

1) Virksomheder der overskrider en af følgende tærskler:
   a) Beskæftiger mere end 250 personer.
   b) Har en årlig omsætning på over 50 mio. EUR og en årlig samlet balance på over 43 mio. EUR.
2) Virksomheden er en kritisk virksomhed i henhold til § 115.
3) Virksomheden er den eneste udbyder i en medlemsstat af en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter.
4) En forstyrrelse af den tjeneste, virksomheden leverer, vil kunne have væsentlig indvirkning på den offentlige sikkerhed eller folkesundheden.
5) En forstyrrelse af den tjeneste, virksomheden leverer, vil kunne medføre en væsentlig systemisk risiko, navnlig for sektorer, hvor en sådan forstyrrelse kan have en grænseoverskridende virkning.
6) Virksomheden er kritisk på grund af sin specifikke betydning på nationalt eller regionalt plan for den pågældende sektor eller type af tjeneste eller for andre indbyrdes afhængige sektorer i medlemsstaten.

Stk. 4. Energistyrelsen identificerer efter stk. 1, virksomheder som vigtige enheder, hvis de ikke opfylder kriterierne for at være væsentlige enheder i medfør af stk. 3, og enheden opfylder mindst én af følgende betingelser

1) enheden beskæftiger mere end 50 personer eller
2) enheden har en årlig omsætning på over 10 mio. EUR og en årlig samlet balance på over 10 mio. EUR.

§ 115. Energistyrelsen identificerer kritiske enheder og udarbejder en liste over disse.

Stk. 2. Energistyrelsen foretager de stk. 1, nævnte opgaver første gang senest den 17. juli 2026 og derefter når det er relevant, dog mindst hvert fjerde år.

Stk. 3. Virksomheder inddelt på niveau 2-5 efter § 4, er kritiske enheder.

Stk. 4. Virksomheder underrettes om, at de er blevet identificeret som en kritisk enhed senest en måned efter Energistyrelsen har udarbejdet listen i stk. 1.

Stk. 5. Energistyrelsen tager ved identifikationen efter stk. 1 behørigt hensyn til resultaterne af Danmarks nationale risikovurdering og nationale strategi for kritiske enheders modstandsdygtighed som udarbejdes i henhold til CER-direktivet, og ligger samtidig vægt på om:

1) Virksomheden leverer en eller flere væsentlige tjenester.
2) Virksomheden opererer i og har sin kritiske infrastruktur beliggende på dansk territorium.
3) En hændelse hos virksomheden vil have betydelig forstyrrende virkning, jf. stk. 6, på virksomhedens levering af en eller flere væsentlige tjenester eller på leveringen af andre væsentlige tjenester i sektorerne anført i

bilag 5, som er afhængige af denne eller disse væsentlige tjenester.

Stk. 6. Ved fastlæggelse af, om en hændelse vil have betydelig forstyrrende virkning, jf. stk. 5, nr. 3, lægges der vægt på følgende:

1) Antal brugere, der er afhængige af den væsentlige tjeneste, som udbydes af den berørte enhed.
2) Omfanget af andre sektorers og delsektorers afhængighed af den pågældende væsentlige tjeneste.
3) Den indvirkning, som hændelser kan have med hensyn til omfang og varighed på økonomiske og samfundsmæssige aktiviteter, miljøet, den offentlige sikkerhed eller befolkningens sundhed.
4) Enhedens markedsandel på markedet for den eller de berørte væsentlige tjenester.
5) Det geografiske område, der kan blive berørt af en hændelse, herunder eventuel grænseoverskridende indvirkning.
6) Enhedens betydning med hensyn til at opretholde et tilstrækkeligt niveau for den væsentlige tjeneste under hensyntagen til tilgængelighed af alternative måder at levere denne væsentlige tjeneste på.

§ 116. Energistyrelsen identificerer kritiske enheder af særlig europæisk betydning.

Stk. 2. Virksomheder der har modtaget underretning efter § 115, stk. 4, skal såfremt de leverer de samme eller lignende væsentlige tjenester til eller i seks eller flere EU-medlemslande oplyse Energistyrelsen om

1) hvilke væsentlige tjenester der leveres, og
2) i hvilke EU-medlemslande disse væsentlige tjenester leveres.

Stk. 3. Der skal ske underretning til Energistyrelsen efter stk. 2 snarest muligt og senest en måned efter underretningen efter § 115, stk. 4.

Stk. 4. Energistyrelsen underretter snarest muligt EU-Kommissionen om underretninger der modtages efter stk. 2.

Stk. 5. Såfremt Energistyrelsen modtager underretning fra EU-Kommissionen om, at EU-Kommissionen har konstateret, at virksomheden er en kritisk enhed af særlig europæisk betydning, oplyser Energistyrelsen virksomheden herom jf. § 5, stk. 2, i lov om styrket beredskab i energisektoren.

Stk. 6. Virksomheder, der er identificeret som en kritisk enhed af særlig europæisk betydning, skal efter en afsluttet rådgivende mission, jf. § 20, stk. 1, i lov om styrket beredskab for energisektoren, skriftligt redegøre for Energistyrelsen, hvilke af de foranstaltninger den rådgivende mission har foreslået at virksomheden gennemfører, som virksomheden har gennemført.

Stk. 7. Energistyrelsen skal modtage redegørelsen efter stk. 6, senest seks måneder efter, at den rådgivende mission har fremsendt sin udtalelse med foreslåede foranstaltninger til virksomheden, der er identificeret som en kritisk enhed af særlig europæisk betydning.

Kapitel 19

Dispensation

§ 117. Energistyrelsen kan efter ansøgning dispensere fra bestemmelser i denne bekendtgørelse, hvor ansøgeren har godtgjort, at en dispensation fra den konkrete bestemmelse har mindre betydning for eller reduceret effekt på organisatorisk beredskab, fysisk sikring og cybersikkerhed hos virksomheden eller i energisektoren.

Kapitel 20

Håndhævelse og klageadgang

§ 118. Afgørelser truffet efter lov om styrket beredskab i energisektoren og denne bekendtgørelse kan ikke påklages til anden administrativ myndighed.

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

§ 119. Energistyrelsen skal ved påbud om revision af en virksomhed efter § 22, stk. 1, i lov om styrket beredskab i energisektoren specificere de områder, hvor der skal foretages revision, og angive fristen for revisionens afslutning.

§ 120. Revision efter § 119 skal foretages af en af virksomheden uafhængig revisor. Revisoren vælges af virksomheden selv og skal som minimum opfylde følgende krav:

1) Revisoren må ikke have udført nogen opgaver for virksomheden eller koncernforbundne virksomheder inden for de sidste fem fulde kalenderår.
2) Faglige kvalifikationer som knytter sig til det område, der skal føres revision af.

Stk. 2. Energistyrelsen skal godkende den valgte revisionsvirksomhed og de konkrete revisorer, der skal udføre revisionen, inden revisionen kan påbegyndes.

Stk. 3. Virksomheden skal, senest to uger efter modtagelsen af påbuddet efter § 22, stk. 1, i lov om styrket beredskab i energisektoren, sende oplysninger om valg af revisor, pris på løsning af opgaven og dokumentation for, at kriterierne i stk. 1 er overholdt, til Energistyrelsen. Såfremt virksomheden ikke overholder fristen, vælger Energistyrelsen en revisor.

Stk. 4. Energistyrelsen har to uger fra modtagelsen af ansøgningen efter stk. 3 til at godkende eller afvise virksomhedens valg af revisor. Såfremt Energistyrelsen ikke overholder fristen, kan revisionen påbegyndes uden godkendelse.

§ 121. Efter gennemført revision skal revisorens rapport snarest muligt forlægges for Energistyrelsen og virksomheden, således at Energistyrelsen snarest muligt kan træffe afgørelse om påbud efter § 22, stk. 2, i lov om styrket beredskab i energisektoren.

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

1) overtræder § 7, § 10, § 11, stk. 1-6, og stk. 7, §§ 12-22, § 23, stk. 1 og 2, §§ 24-76, § 77, stk. 1 og 2, § 77, stk. 4-7, § 78, stk. 1, § 79, stk. 1 og 2, § 80, § 104, § 107, stk. 2-4, § 112, stk. 3, § 116, stk. 3, 6 og 7 og § 120, stk. 1 og 3,

2) meddeler urigtige, vildledende oplysninger eller undlader at meddele oplysninger i medfør af § 9, stk. 1, 2 og 3, § 11, stk. 7, §§ 75-76, § 77, stk. 3, og § 78, stk. 1.

Stk. 2. Bøder udstedt i medfør af stk. 1, skal overholde de rammer, der er for fastsættelsen af bødens størrelse i § 37, stk. 1, i lov om styrket beredskab for energisektoren.

Stk. 3. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Kapitel 21

Ikrafttrædelses- og overgangsbestemmelser

§ 123. Bekendtgørelsen træder i kraft den 7. marts 2025.

Stk. 2. Følgende bekendtgørelser ophæves:

1) Bekendtgørelse nr. 11 af 7. januar 2011 om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse (EPCIP-direktivet).
2) Bekendtgørelse nr. 424 af 25. april 2018 om beredskab for oliesektoren.
3) Bekendtgørelse nr. 821 af 14. august 2019 om beredskab for naturgassektoren.
4) Bekendtgørelsen nr. 2646 af 28. december 2021 om beredskab for elsektoren.
5) Bekendtgørelse nr. 2647 af 28. december 2021 om it-beredskab for el- og naturgassektorerne.

Stk. 3. Foranstaltninger efter § 36 og § 37 skal senest være gennemført den 1. marts 2026, jf. dog stk. 5.

Stk. 4. Foranstaltninger efter §§ 38, 43, 48, 50 og 62 skal senest være gennemført den 1. marts 2027, jf. dog stk. 5.

Stk. 5. Stk. 3 og 4, finder ikke anvendelse på virksomheder der har været omfattet af bestemmelserne i bekendtgørelse nr. 424 af 25. april 2018 om beredskab for oliesektoren, bekendtgørelse nr. 821 af 14. august 2019 om beredskab for naturgassektoren, bekendtgørelsen nr. 2646 af 28. december 2021 om beredskab for elsektoren og bekendtgørelse nr. 2647 nr. 28. december 2021 om it-beredskab for el- og naturgassektorerne, når foranstaltningerne nævnt i stk. 3 og 4, indholdsmæssigt svarer til foranstaltninger i de førnævnte bekendtgørelser.

Energistyrelsen, den 6. marts 2025

Kristoffer Böttzauw

/ Jesper Rode Tholstrup

Bilag 1

Skemaer med tærskelværdier for niveauinddeling af virksomheder, jf. § 4.

1. Tærskelværdier for virksomheder i elsektoren

1.1. Tærskelværdier for niveau 5

a) Elproducenter, udpegede elektricitetsmarkedsoperatører og markedsdeltagere, der leverer tjenester, som vedrører aggregering, fleksibelt elforbrug eller energilagring, og som producerer eller håndterer en kapacitet på minimum 1.650 MW elproduktion eller elforbrug. Markedsdeltagere, der leverer tjenester, som vedrører aggregering, fleksibelt elforbrug eller energilagring, omfattes såfremt disse har mulighed for styring med elproduktion, elforbrug eller udveksling af el med det kollektive net.

b) Operatører af ladepunkter, der er ansvarlige for forvaltningen og driften af en ladepunkter, som leverer en ladetjeneste til slutbrugere, herunder i en mobilitetstjenesteudbyders navn og på dennes vegne, og som har en samlet kapacitet på minimum 1.650 MW elforbrug fra det kollektive elnet.

c) Operatører inden for brintproduktion, der har en kapacitet på minimum 1.650 MW elforbrug fra det kollektive elnet.

d) Distributionssystemoperatører, der forvalter et forsyningsområde med minimum 750.000 slutbrugere, eller som i det seneste fulde kalenderår har distribueret minimum 3.500 GWh el.

e) Transmissionssystemoperatører.

f) Virksomheder, der har delegerede myndighedsopgaver med betydning for elforsyningen på nationalt plan.

1.2. Tærskelværdier for niveau 4

a) Elproducenter, udpegede elektricitetsmarkedsoperatører og markedsdeltagere, der leverer tjenester, som vedrører aggregering, fleksibelt elforbrug eller energilagring, og som producerer eller håndterer en kapacitet på minimum 600 MW elproduktion eller elforbrug. Markedsdeltagere, der leverer tjenester, som vedrører aggregering, fleksibelt elforbrug eller energilagring, omfattes såfremt disse har mulighed for styring med elproduktion, elforbrug eller udveksling af el med det kollektive net.

b) Operatører af ladepunkter, der er ansvarlige for forvaltningen og driften af et ladepunkt, som leverer en ladetjeneste til slutbrugere, herunder i en mobilitetstjenesteudbyders navn og på dennes vegne, og som har en samlet kapacitet på minimum 600 MW elforbrug fra det kollektive elnet.

c) Operatører inden for brintproduktion, der har en kapacitet på minimum 600 MW elforbrug fra det kollektive elnet.

d) Distributionssystemoperatører, der forvalter et forsyningsområde med minimum 250.000 slutbrugere, eller som i det seneste fulde kalenderår har distribueret minimum 1.200 GWh el.

e) Regionale koordinationscentre.

1.3. Tærskelværdier for niveau 3

a) Elproducenter, udpegede elektricitetsmarkedsoperatører og markedsdeltagere, der leverer tjenester, som vedrører aggregering, fleksibelt elforbrug eller energilagring, og som producerer eller håndterer en kapacitet på minimum 100 MW elproduktion eller elforbrug. Markedsdeltagere, der leverer tjenester, som vedrører aggregering, fleksibelt elforbrug eller energilagring, omfattes såfremt disse har mulighed for styring med elproduktion, elforbrug eller udveksling af el med det kollektive net.

b) Operatører af ladepunkter, der er ansvarlige for forvaltningen og driften af et ladepunkt, som leverer en ladetjeneste til slutbrugere, herunder i en mobilitetstjenesteudbyders navn og på dennes vegne, og som har en samlet kapacitet på minimum 100 MW elforbrug fra det kollektive elnet.

c) Operatører inden for brintproduktion, der har en kapacitet på minimum 100 MW elforbrug fra det kollektive elnet.

d) Distributionssystemoperatører, der forvalter et forsyningsområde med minimum 30.000 slutbrugere, eller som i det seneste fulde kalenderår har distribueret minimum 150 GWh el.

1.4. Tærskelværdier for niveau 2

a) Elproducenter, udpegede elektricitetsmarkedsoperatører og markedsdeltagere, der leverer tjenester, som vedrører aggregering, fleksibelt elforbrug eller energilagring, og som producerer eller håndterer en kapacitet på minimum 25 MW elproduktion eller elforbrug, såfremt disse har mulighed for styring med elproduktion, elforbrug eller udveksling af el med det kollektive net, jf. pkt. f.

b) Operatører af ladepunkter, der er ansvarlige for forvaltningen og driften af et ladepunkt, som leverer en ladetjeneste til slutbrugere, herunder i en mobilitetstjenesteudbyders navn og på dennes vegne, og som har en samlet kapacitet på minimum 25 MW elforbrug fra det kollektive elnet.

c) Operatører inden for brintproduktion, der har en kapacitet på minimum 25 MW elforbrug fra det kollektive elnet.

d) Øvrige distributionssystemoperatører, der forvalter et forsyningsområde, og som falder under tærskelværdierne for niveau 3-5.

e) Elektricitetsvirksomheder, der varetager levering af elektricitet, og som beskæftiger minimum 50 ansatte eller har en årlig omsætning på minimum 10 mio. EUR og en årlig samlet balance på minimum 10 mio. EUR.

f)	Markedsdeltagere, der leverer tjenester, som vedrører aggregering, fleksibelt elforbrug eller energilagring, men som udelukkende foretager handler og ikke har mulighed for styring med elproduktion, elforbrug eller udveksling af el med det kollektive net, omfattes såfremt disse beskæftiger minimum 50 ansatte eller har en årlig omsætning på minimum 10 mio. EUR og en årlig balance på minimum 10 mio. EUR.
g)	Virksomhedstyper som nævnt i pkt. a, b, c, d, e og f, som beskæftiger minimum 50 ansatte eller har en årlig omsætning på minimum 10 mio. EUR og en årlig balance på minimum 10 mio. EUR.
1.5.	Tærskelværdier for niveau 1
	Ikke relevant.
2.	**Tærskelværdier for virksomheder i gassektoren**
2.1.	Tærskelværdier for niveau 5
a)	Gasforsyningsvirksomheder, LNG-systemoperatører, naturgasvirksomheder, operatører af naturgasraffinaderier og –behandlingsanlæg og operatører inden for brintlagring, der årligt opgraderer til eller injicerer minimum 1.000 mio. Nm^3 gas i et gasnet, eller som årligt producerer eller behandler minimum 1.000 mio. Nm^3 gas.
b)	Lagersystemoperatører, der har en samlet udtrækskapacitet på minimum 5 mio. Nm^3 gas pr. dag eller en injektionskapacitet på minimum 2 mio. Nm^3 gas pr. dag.
c)	Virksomheder, der har delegerede myndighedsopgaver med betydning for gasforsyningen på nationalt plan.
d)	Transmissionssystemoperatører.
e)	Operatører af opstrømsrørledningsnet.
2.2.	Tærskelværdier for niveau 4
a)	Gasforsyningsvirksomheder, LNG-systemoperatører, naturgasvirksomheder, operatører af naturgasraffinaderier og –behandlingsanlæg og operatører inden for brintlagring, der årligt opgraderer til eller injicerer minimum 375 mio. Nm^3 gas i et gasnet, eller som årligt producerer eller behandler minimum 375 mio. Nm^3 gas.
b)	Lagersystemoperatører, der har en samlet udtrækskapacitet på minimum 3 mio. Nm^3 gas pr. dag eller en injektionskapacitet på minimum 1 mio. Nm^3 gas pr. dag.
c)	Distributionssystemoperatører og operatører inden for brinttransmission, der håndterer minimum 100.000 Nm^3 gas/time, eller som forvalter et forsyningsområde med minimum 250.000 slutbrugere
d)	Operatører af bygas, som forvalter et forsyningsområde med minimum 250.000 slutbrugere

2.3.	Tærskelværdier for niveau 3
a)	Gasforsyningsvirksomheder, LNG-systemoperatører, naturgasvirksomheder, operatører af naturgasraffinaderier og –behandlingsanlæg og operatører inden for brintlagring, der årligt opgraderer til eller injicerer minimum 100 mio. Nm^3 gas i et gasnet, eller som årligt producerer eller behandler minimum 100 mio. Nm^3 gas.
b)	Lagersystemoperatører, der har en samlet udtrækskapacitet på minimum 1 mio. Nm^3 gas pr. dag eller en injektionskapacitet på minimum 0,5 mio. Nm^3
c)	Distributionssystemoperatører og operatører inden for brinttransmission,, der håndterer minimum 10.000 Nm^3 gas/time, eller som forvalter et forsyningsområde med minimum 30.000 slutbrugere
d)	Operatører af bygas, som forvalter et forsyningsområde med minimum 30.000 slutbrugere.
2.4.	Tærskelværdier for niveau 2
a)	Gasforsyningsvirksomheder, LNG-systemoperatører, naturgasvirksomheder, operatører af naturgasraffinaderier og –behandlingsanlæg og operatører inden for brintlagring, der årligt opgraderer til eller injicerer minimum26 mio. Nm^3 gas i et gasnet, eller som årligt producerer eller behandler minimum 26 mio. Nm^3 gas.
b)	Lagersystemoperatører, der har en samlet udtrækskapacitet på minimum 0,5 mio. Nm^3 gas pr. dag eller en injektionskapacitet på minimum 200.000 Nm^3 gas pr. dag.
c)	Øvrige distributionssystemoperatører og operatører inden for brinttransmission.
d)	Øvrige operatører af bygas.
e)	Virksomhedstyper som nævnt i pkt. a, b, c og d, som beskæftiger minimum 50 ansatte eller har en årlig omsætning på minimum 10 mio. EUR og en årlig balance på minimum 10 mio. EUR.
2.5.	Tærskelværdier for niveau 1
	Ikke relevant.

3.	**Tærskelværdier for virksomheder i oliesektoren**
3.1.	Tærskelværdier for niveau 5
a)	Virksomheder, der har delegerede myndighedsopgaver.
b)	Den centrale lagerenhed.

c) Operatører af olieproduktionsanlæg, herunder offshore olieanlæg med en årlig produktion af olie på minimum 1 mio. m^3 i tre ud af fem år, eller som har en forventet produktion af olie på minimum 1 mio. m^3 i et kalenderår.

d) Operatører af olieraffinaderier eller oliebehandlingsanlæg, og som har en årlig forarbejdning på minimum 1 mio. m^3 råolie i tre ud af fem år, eller som har en forventet forarbejdning af råolie minimum på 1 mio. m^3 i et kalenderår.

3.2. Tærskelværdier for niveau 4

a) Operatører af olietransmission.

b) Operatører af olieproduktionsanlæg, herunder offshore olieanlæg, med en årlig produktion af olie på minimum 375.000 m^3 i tre ud af fem år, eller som har en forventet produktion af olie på minimum 375.000 m^3 i et kalenderår.

c) Operatører af olieraffinaderier eller oliebehandlingsanlæg, som har en årlig forarbejdning på minimum 375.000 m^3 råolie i tre ud af fem år, eller som har en forventet forarbejdning af råolie på minimum 375.000 m^3 i et kalenderår.

3.3. Tærskelværdier for niveau 3

a) Operatører af olielagre, herunder olieterminaler med en samlet kapacitet på minimum 300.000 m^3.

b) Operatører af olieproduktionsanlæg, herunder offshore olieanlæg, med en årlig produktion af olie på minimum 100.000 m^3 i tre ud af fem år, eller som har en forventet produktion af olie på minimum 100.000 m^3 i et kalenderår.

c) Operatører af olieraffinaderier eller oliebehandlingsanlæg, som har en årlig forarbejdning på minimum 100.000 m^3 råolie i tre ud af fem år, eller som har en forventet forarbejdning af råolie på minimum 100.000 m3 i et kalenderår.

3.4. Tærskelværdier for niveau 2

a) Operatører af olielagre, herunder olieterminaler med en samlet kapacitet på minimum 100.000 m^3.

b) Øvrige virksomheder med positiv lagringspligt.

c) Operatører af olieproduktionsanlæg, herunder offshore olieanlæg, med en årlig produktion af olie på minimum 26.000 m^3 i tre ud af fem år, eller som har en forventet produktion af olie på minimum 26.000 m^3 i et kalenderår.

d) Operatører af olieraffinaderier eller oliebehandlingsanlæg, som har en årlig forarbejdning på minimum 26.000 m^3 råolie i tre ud af fem år, eller som har en forventet forarbejdning af råolie på minimum 26.000 m^3 i et kalenderår.

e)	Operatører af tankstationer med et samlet årligt salg på minimum 600.000 m^3, eller som opererer minimum 100 tankstationer i Danmark.
f)	Virksomhedstyper, som nævnt i pkt. a, b, c og d, som beskæftiger minimum 50 ansatte eller har en årlig omsætning på minimum 10 mio. EUR og en årlig balance på minimum 10 mio. EUR.
3.5.	Tærskelværdier for niveau 1
	Ikke relevant.

4. **Tærskelværdier for virksomheder i fjernvarmesektoren og fjernkølingssektoren**	
4.1.	Tærskelværdier for niveau 5
	Ikke relevant.
4.2.	Tærskelværdier for niveau 4
a)	Operatører af fjernvarme eller fjernkøling, der i to ud af de seneste tre år har solgt minimum 4.525 GWh fjernvarme eller fjernkøling.
4.3.	Tærskelværdier for niveau 3
a)	Operatører af fjernvarme eller fjernkøling, der i to ud af de seneste tre år har solgt minimum 543 GWh fjernvarme eller fjernkøling.
4.4.	Tærskelværdier for niveau 2
a)	Operatører af fjernvarme eller fjernkøling, der i to ud af de seneste tre år har solgt minimum 181 GWh fjernvarme eller fjernkøling.
b)	Operatører af fjernvarme eller fjernkøling, som beskæftiger minimum 50 ansatte eller har en årlig omsætning på minimum 10 mio. EUR og en årlig balance på minimum 10 mio. EUR.
4.5.	Tærskelværdier for niveau 1
a)	Operatører af fjernvarme eller fjernkøling, der i to ud af de seneste tre år har solgt minimum 13,9 GWh fjernvarme eller fjernkøling.

Bilag 2

Skemaer med tærskelværdier for klassificering af anlæg, jf. § 6.

1. Tærskelværdier for anlæg i elsektoren	
1.1.	Tærskelværdier for klasse 5
a)	Anlæg af væsentlig betydning for at opretholde elforsyningen for de sammenhængende elforsyningssystemer på europæisk plan eller væsentlige dele af disse.
b)	Anlæg, der har kapacitet til at producere minimum 1.650 MW el eller forbruge minimum 1.650 MW el fra det kollektive net eller udveksle minimum1. 650 MW el med det kollektive net samt anlæg, der styrer disse processer. Dette omfatter ikke distributionssystemoperatørers anlæg på distributionsnettet.
c)	Brintproducerende anlæg med kapacitet til at forbruge minimum 1.650 MW el fra det kollektive net eller tilbageføre minimum 1650 MW til det kollektive net.
d)	Anlæg af væsentlig betydning for at opretholde distributionen af el til 750.000 slutbrugere eller for distributionen af 3.500 GWh el.
1.2.	Tærskelværdier for klasse 4
a)	Anlæg af væsentlig betydning for at opretholde elforsyningen for de sammenhængende elforsyningssystemer på nationalt plan eller væsentlige dele af disse.
b)	Anlæg, der har kapacitet til at producere minimum 600 MW el eller forbruge minimum 600 MW el fra det kollektive net eller udveksle minimum 600 MW el med det kollektive net samt anlæg, der styrer disse processer. Dette omfatter ikke distributionssystemoperatørers anlæg på distributionsnettet.
c)	Brintproducerende anlæg med kapacitet til at forbruge minimum 600 MW el fra det kollektive net eller tilbageføre minimum 600 MW til det kollektive net.
d)	Anlæg af væsentlig betydning for at opretholde distributionen af el til minimum 250.000 slutbrugere eller for distributionen af minimum 1.200 GWh el.
1.3.	Tærskelværdier for klasse 3
a)	Anlæg af væsentlig betydning for at opretholde elforsyningen for de sammenhængende elforsyningssystemer på regionalt plan eller væsentlige dele af disse.
b)	Anlæg, der har kapacitet til at producere minimum 100 MW el eller forbruge minimum 100 MW el fra det kollektive net eller udveksle minimum 100 MW el med det kollektive net samt anlæg, der styrer disse processer. Dette omfatter ikke distributionssystemoperatørers anlæg på distributionsnettet.
c)	Brintproducerende anlæg med kapacitet til at forbruge minimum 100 MW el fra det kollektive net eller tilbageføre minimum 100 MW til det kollektive net.

d)	Anlæg af væsentlig betydning for at opretholde distributionen af el til 30.000 slutbrugere eller for distributionen af 150 GWh el.
1.4.	Tærskelværdier for klasse 2
a)	Anlæg, der har kapacitet til at producere 25 MW el eller forbruge 25 MW el fra det kollektive net eller udveksle 25 MW el med det kollektive net samt anlæg, der styrer disse processer. Dette omfatter ikke distributionssystemoperatørers anlæg på distributionsnettet.
b)	Brintproducerende anlæg med kapacitet til at forbruge 25 MW el fra det kollektive net eller tilbageføre 25 MW til det kollektive net.
c)	Anlæg af væsentlig betydning for at opretholde distributionen af el til 10.000 slutbrugere eller for distributionen af 50 GWh el.
1.5.	Tærskelværdier for klasse 1
	Ikke relevant.

2. Tærskelværdier for anlæg i gassektoren	
2.1.	Tærskelværdier for klasse 5
a)	Anlæg af væsentlig betydning for at opretholde gasforsyningen på europæisk niveau eller væsentlige dele af dette.
b)	Anlæg, der årligt opgraderer til eller injicerer 1.000 mio. Nm^3 gas eller mere i gasnettet eller som årligt producerer eller behandler minimum 1.000 mio. Nm^3 gas.
c)	Gaslagerfaciliteter, der har en samlet udtrækskapacitet på minimum 5 mio. Nm^3 gas pr. dag eller en injektionskapacitet på minimum 3 mio. Nm^3 gas pr. dag.
d)	Opstrømsrørledningsnet.
2.2.	Tærskelværdier for klasse 4
a)	Anlæg af væsentlig betydning for at opretholde gasforsyningen for det samlede danske gasforsyningssystem eller væsentlige dele af dette.
b)	Anlæg, der årligt opgraderer til eller injicerer minimum 375 mio. Nm^3 gas i et gasnet, eller som årligt producerer eller behandler minimum 375 mio. Nm^3 gas.
c)	Gaslagerfaciliteter, der har en samlet udtrækskapacitet på minimum 3 mio. Nm^3 gas pr. dag eller en injektionskapacitet på minimum 1 mio. Nm^3 gas pr. dag.
d)	Anlæg af væsentlig betydning for at opretholde distributionen af 100.000 Nm^3 gas pr. time eller for distributionen af gas til minimum 250.000 slutbrugere.

e)	Anlæg af væsentlig betydning for at opretholde produktionen eller fremføringen af bygas til minimum 250.000 slutbrugere.
2.3.	Tærskelværdier for klasse 3
a)	Anlæg af væsentlig betydning for at opretholde gasforsyningen på regionalt niveau eller væsentlige dele af dette.
b)	Anlæg, der årligt opgraderer til eller injicerer 100 mio. Nm^3 gas i et gasnet, eller som årligt producerer eller behandler minimum 100 mio. Nm^3 gas.
c)	Gaslagerfaciliteter, der har en samlet udtrækskapacitet på minimum 1 mio. Nm^3 gas pr. dag eller en injektionskapacitet på minimum 0,5 mio. Nm^3.
d)	Anlæg af væsentlig betydning for at opretholde distributionen af 10.000 Nm^3 gas pr. time eller for distributionen af gas til minimum 30.000 slutbrugere.
e)	Anlæg af væsentlig betydning for at opretholde produktionen eller fremføringen af bygas til minimum 30.000 slutbrugere.
2.4.	Tærskelværdier for klasse 2
a)	Anlæg, der årligt opgraderer til eller injicerer 26 mio. Nm^3 gas i et gasnet, eller som årligt producerer eller behandler minimum 26 mio. Nm^3 gas.
b)	Gaslagerfaciliteter, der har en samlet udtrækskapacitet på minimum 0,5 mio. Nm^3 gas pr. dag eller en injektionskapacitet på minimum 200.000 Nm^3 gas pr. dag.
c)	Gaslagerfaciliteter, der har en samlet udtrækskapacitet på minimum 0,5 mio. Nm^3 gas pr. dag eller en injektionskapacitet på minimum 200.000 Nm^3 gas pr. dag.
d)	Anlæg af væsentlig betydning for at opretholde produktionen eller fremføringen af bygas til minimum 10.000 slutbrugere.
2.5.	Tærskelværdier for klasse 1
	Ikke relevant.

3. Tærskelværdier for anlæg i oliesektoren	
3.1.	Tærskelværdier for klasse 5
a)	Anlæg med betydning for olieforsyningen på europæisk niveau.
b)	Olieproduktionsanlæg og offshore olieanlæg med en årlig produktion af olie på minimum 1 mio. m^3 i tre ud af fem år, eller som har en forventet produktion af olie på minimum 1 mio. m^3 i et kalenderår.

c)	Olieraffinaderier og oliebehandlingsanlæg med en årlig forarbejdning på minimum 1 mio. m^3 råolie i tre ud af fem år, eller som har en forventet forarbejdning af råolie på minimum 1 mio. m^3 i et kalenderår.
3.2.	Tærskelværdier for klasse 4
a)	Olierørledninger og olietransmissionsanlæg med betydning for olieforsyningen på nationalt niveau.
b)	Olieraffinaderier med betydning for olieforsyningen på nationalt niveau.
c)	Olieproduktionsanlæg og offshore olieanlæg med en årlig produktion af olie på minimum 375.000 m^3 i tre ud af fem år, eller som har en forventet produktion af olie på minimum 375.000 m^3 i et kalenderår.
d)	Olieraffinaderier og oliebehandlingsanlæg med en årlig forarbejdning på minimum 375.000 m^3 råolie i tre ud af fem år, eller som har en forventet forarbejdning af råolie på minimum 375.000 m^3 i et kalenderår.
3.3.	Tærskelværdier for klasse 3
a)	Olieterminaler eller –lagre med en samlet kapacitet på minimum 300.000 m^3.
b)	Olieproduktionsanlæg og offshore olieanlæg med en årlig produktion af olie på minimum 100.000 m^3 i tre ud af fem år, eller som har en forventet produktion af olie på minimum 100.000 m^3 i et kalenderår.
c)	Olieraffinaderier og oliebehandlingsanlæg med en årlig forarbejdning på minimum 100.000 m^3 råolie i tre ud af fem år, eller som har en forventet forarbejdning af råolie på minimum 100.000. m^3 i et kalenderår.
3.4.	Tærskelværdier for klasse 2
a)	Olieterminaler og –lagre med en samlet kapacitet på minimum 100.000 m^3.
b)	Olieproduktionsanlæg og offshore olieanlæg med en årlig produktion af olie på minimum 26.000 m^3 i tre ud af fem år, eller som har en forventet produktion af olie på minimum 26.000 m^3 i et kalenderår.
c)	Olieraffinaderier og oliebehandlingsanlæg med en årlig forarbejdning på minimum 26.000 m^3 råolie i tre ud af fem år, eller som har en forventet forarbejdning af råolie på minimum 26.000 m^3 i et kalenderår.
3.5.	Tærskelværdier for klasse 1
	Ikke relevant.

4. Tærskelværdier for anlæg i fjernvarmesektoren og fjernkølingssektoren

4.1.	Tærskelværdier for klasse 5
	Ikke relevant.
4.2.	Tærskelværdier for klasse 4
a)	Anlæg med væsentlig betydning for at opretholde forsyningen af minimum 4.525 GWh fjernvarme eller fjernkøling, herunder kraftvarmeværker, fjernkølingsanlæg, spids- og reservelastanlæg, ledningsnet, pumpestationer, varmevekslerstationer, varmepumper og kontrolrum, der styrer, regulerer eller overvåger varmeleverancer.
4.3.	Tærskelværdier for klasse 3
a)	Anlæg med væsentlig betydning for at opretholde forsyningen af minimum 543 GWh fjernvarme eller fjernkøling, herunder kraftvarmeværker, fjernkølingsanlæg, spids- og reservelastanlæg, ledningsnet, pumpestationer, varmevekslerstationer, varmepumper og kontrolrum, der styrer, regulerer eller overvåger varmeleverancer.
4.4.	Tærskelværdier for klasse 2
a)	Anlæg med væsentlig betydning for at opretholde forsyningen af minimum 181 GWh fjernvarme eller fjernkøling, herunder kraftvarmeværker, fjernkølingsanlæg, spids- og reservelastanlæg, ledningsnet, pumpestationer, varmevekslerstationer, varmepumper og kontrolrum, der styrer, regulerer eller overvåger varmeleverancer.
4.5.	Tærskelværdier for klasse 1
	Ikke relevant.

Bilag 3

Oplysninger, som virksomheder skal indsende til Energistyrelsen til brug for Energistyrelsens niveauinddeling af virksomheder og klassificering af anlæg, jf. § 9.

1) Virksomhedens navn, adresse og CVR-nummer.
2) Den relevante delsektor, som virksomheden er omfattet af, jf. § 2 i lov om styrket beredskab i energisektoren.
3) Beskrivelse af den eller de tjenester, som virksomheden leverer til den relevante delsektor, jf. nr. 2.
4) Ajourførte kontaktoplysninger på virksomheden, herunder e-mailadresser, IP-intervaller og telefonnumre.
5) De medlemsstater i Den Europæiske Union, hvor virksomheden leverer tjenester.
6) Virksomhedens bevilling til energiproduktion.
7) Oplysninger om den samlede energimængde, som virksomheden håndterer inden for en nærmere fastsat tidsperiode, herunder:
   a) Kapaciteten af den elektricitet, som elproducenter, udpegede elektricitetsmarkedsoperatører og markedsdeltagere, der leverer tjenester, som vedrører aggregering, fleksibelt elforbrug eller energilagring kan producere, forbruge eller udveksle med det kollektive net.
   b) Kapaciteten af den elektricitet, som operatører af ladepunkter kan håndtere eller udveksle med det kollektive net. Oplysningerne omfatter både den samlede effekt af de installerede ladepunkter samt den tilgængelige kapacitet for den samlede portefølje af ladepunkter.
   c) Kapaciteten af den elektricitet, som operatører af brintproduktion kan forbruge fra det kollektive elnet.
   d) Mængden af el, som distributionssystemoperatører i det seneste fulde kalenderår har distribueret.
   e) Mængden af gas, som gasforsyningsvirksomheder, LNG-systemoperatører, naturgasvirksomheder, operatører af naturgasraffinaderier og –behandlingsanlæg og operatører inden for brintlagring årligt injicerer i eller opgraderer til et gasnet eller årligt behandler eller producerer. Mængden skal opgøres i Nm3.
   f) Lagersystemoperatørers udtrækskapacitet og injektionskapacitet opgjort i Nm3 gas pr. dag.
   g) Mængden af gas, som distributionssystemoperatører og operatører inden for brinttransmission håndterer. Mængden skal opgøres i Nm3 gas pr. time.
   h) Kapaciteten samt den transporterede mængde gas, som operatører af opstrømsrørledningsnet kan håndtere og som virksomheden har solgt eller på anden måde håndteret i det seneste fulde kalenderår.
   i) Mængden af olie, som operatører af olieproduktionsanlæg, herunder offshore olieanlæg, har produceret årligt de seneste fem år samt den forventede produktion af olie i det indeværende kalenderår.
   j) Den samlede kapacitet af de olielagre, herunder olieterminaler, som operatører af olielagre ejer.
   k) Mængden af olie, som operatører af olieraffinaderier og oliebehandlingsanlæg har forarbejdet årligt de seneste fem år samt den forventede forarbejdning af olie i det indeværende kalenderår.
   l) Kapaciteten samt den transporterede mængde olie, som operatører af olietransmission kan håndtere og som virksomheden har solgt eller på anden måde håndteret i det seneste fulde kalenderår.
   m) Det samlede mængde olieprodukter, som operatører af tankstationer har solgt det seneste kalenderår. Mængden skal opgøres i m3. Desuden skal operatører af tankstationer oplyse det samlede antal tankstationer, som denne ejer.
   n) Mængden af varme og køling, som operatører af fjernvarme og fjernkøling har solgt årligt de seneste tre kalenderår.
8) Oplysninger om det antal slutbrugere, som virksomheden forsyner, herunder:
   a) Antallet af slutbrugere i distributionssystemoperatørers forsyningsområde

b) Antallet af slutbrugere, til hvilke operatører af bygas fremfører bygas.

9) Oplysninger om virksomhedens anlæg efter nr. 10-15, herunder antal anlæg, type af anlæg, anlæggets geografiske placering og energimængden, som anlægget samlet set kan håndtere eller har håndteret inden for en nærmere fastsat tidsperiode.

10) Produktionsanlæg, anlæg med systembærende egenskaber, stationer til el-distribution og el-transmission og forbindelser i el-systemet, som håndterer energimængder svarende til tærskelværdierne for anlæg i elsektoren, jf. skema 1 i bilag 2, herunder kraftværker, nødstartsanlæg, transformerstationer, kabelovergangsstationer, stationsanlæg, kabelanlæg, luftledningsanlæg, ledningsstrækninger, tilbageførelsesanlæg, forbindelseslinjer, anlæg med vindmøller (inkl. havmøller), solceller, batterier og brintproducerende anlæg.

11) Anlæg i gassektoren, der håndterer energimængder efter tærskelværdierne for anlæg i gassektoren, jf. skema 2 i bilag 2, herunder kompressorstationer, gaslagerfaciliteter, beskyttelsesanlæg, stationer (M/R stationer, tilbageførelsesanlæg, linjeventilstationer, ledningsstrækninger), ledninger (transmissionsledninger), opstrømsrørledningsnet, naturgasraffinaderier og –behandlingsanlæg, gasproduktionsanlæg, opgraderingsanlæg, LNG-faciliteter samt kontrolrum, der styrer, regulerer eller overvåger gasleverancer.

12) Brintproducerende anlæg, som forbruger eller udveksler elektricitet svarende til tærskelværdierne for anlæg i elsektoren, jf. skema 1 i bilag 2 samt anlæg inden for brintlagring og brinttransmission, der håndterer mængder svarende til tærskelværdierne for anlæg i gassektoren jf. skema 2 i bilag 2.

13) Anlæg i oliesektoren, der håndterer energimængder efter tærskelværdierne for anlæg i oliesektoren, jf. skema 3 i bilag 2, herunder olieproduktionsanlæg, olieraffinaderier, oliebehandlingsanlæg, olielagre, olieterminaler og olietransmissionsanlæg, herunder olierørledninger.

14) Antal anlæg i fjernvarme- og fjernkølingssektoren, som håndterer energimængder svarende til tærskelværdierne for anlæg i fjernvarmesektoren, jf. skema 4 i bilag 2, herunder kraftvarmeværker, fjernkølingsanlæg, spids- og reservelastanlæg, ledningsnet, pumpestationer, varmevekslerstationer, varmepumper og kontrolrum.

15) Kontrolrum, der styrer, regulerer eller overvåger leverancer til et energisystem svarende til tærskelværdierne i bilag 1 og bilag 2.

16) Oplysninger om virksomhedens omsætning, balance og medarbejderantal de seneste to afsluttede kalenderår. Der ønskes følgende oplysninger fra de seneste to afsluttede kalenderår:
   a) Om virksomheden havde en omsætning på minimum 10 mio. EUR.
   b) Om virksomheden havde en omsætning på minimum 50 mio. EUR.
   c) Om virksomheden havde en balance på minimum 10 mio. EUR.
   d) Om virksomheden havde en balance på minimum 50 mio. EUR.
   e) Om virksomheden havde minimum 50 ansatte.
   f) Om virksomheden havde minimum 250 ansatte.

Bilag 4

Øvelseselementer, jf. § 20

1. Virksomhedens krisestyringsorganisation.
2. Sikring af forsat drift.
3. Genopretning af forsyning.
4. Mobilisering af ekstra ressourcer og materialer.
5. Intern kommunikation.
6. Ekstern kommunikation.
7. Information til forbrugere.
8. Brugen af alternative kommunikationsmidler.
9. Modtagelse af og kvittering for udmeldinger om ændringer i sektorberedskabsniveau og sektorberedskabsforanstaltninger.
10. Iværksættelse af sektorberedskabsforanstaltninger i henhold til sektorberedskabsniveauet.
11. Modtagelse og håndtering af varsler om cybertrusler og sårbarheder.
12. Procedurerne i det samordnede beredskab.
13. Inddragelse af leverandører i håndteringen af hændelser.
14. Inddragelse af leverandører af forsyningskritiske net- og informationssystemer i håndteringen af hændelser.
15. Aktivering af virksomhedens it-sikkerhedstjeneste.
16. Nødprocedure for isolering af forsyningskritiske net- og informationssystemer i produktionsmiljøet.
17. Nødprocedure for alternativ drift af net- og informationssystemer og aktivering af redundante systemer.
18. Genopretning af forsyningskritiske net- og informationssystemer fra backup., herunder genopretning af kildekode og systemdata for egenudviklet- eller specialudviklet software.
19. Normalisering efter nøddrift af net- og informationssystemer.

Bilag 5

Sektorer af særligt kritisk betydning

Sektor	Delsektor	Type enhed
1. Energi	a) Elektricitet	– Elektricitetsvirksomheder som defineret i artikel 2, nr. 57), i Europa-Parlamentets og Rådets direktiv (EU) 2019/944[1)], der varetager »levering« som defineret i nævnte direktivs artikel 2, nr. 12).
		– Distributionssystemoperatører som defineret i artikel 2, nr. 29), i direktiv (EU) 2019/944.
		– Transmissionssystemoperatører som defineret i artikel 2, nr. 35), i direktiv (EU) 2019/944.
		– Producenter som defineret i artikel 2, nr. 38), i direktiv (EU) 2019/944.
		– Udpegede elektricitetsmarkedsoperatører som defineret i artikel 2, nr. 8), i Europa-Parlamentets og Rådets forordning (EU) 2019/943[2)] – Markedsdeltagere som defineret i artikel 2, nr. 25), i forordning (EU) 2019/943, der leverer tjenester, der vedrører aggregering, fleksibelt elforbrug eller energilagring som defineret i artikel 2, nr. 18), 20) og 59), i direktiv (EU) 2019/944. – Operatører af ladestationer, der er ansvarlige for forvaltningen og driften af en ladestation, som leverer en ladetjeneste til slutbrugere, herunder i en mobilitetstjenesteudbyders navn og på dennes vegne.
	b) Fjernvarme og fjernkøling	– Operatører af fjernvarme eller fjernkøling som defineret i artikel 2, nr. 19), i Europa-Parlamentets og Rådets direktiv (EU) 2018/2001[3)].
	c) Olie	– Olierørledningsoperatører.
		– Operatører af olieproduktionsanlæg, -raffinaderier og -behandlingsanlæg, olielagre og olietransmission.
		– Centrale lagerenheder som defineret i artikel 2, litra f), i Rådets direktiv 2009/119/EF[4)].
	d) Gas	– Forsyningsvirksomheder som defineret i artikel 2, nr. 8), i Europa-Parlamentets og Rådets direktiv 2009/73/EF[5)].
		– Distributionssystemoperatører som defineret i artikel 2, nr. 6), i direktiv 2009/73/EF.
		– Transmissionssystemoperatører som defineret i artikel 2, nr. 4), i direktiv 2009/73/EF.
		– Lagersystemoperatører som defineret i artikel 2, nr. 10), i direktiv 2009/73/EF.
		– LNG-systemoperatører som defineret i artikel 2, nr. 12), i direktiv 2009/73/EF.
		– Naturgasvirksomheder som defineret i artikel 2, nr. 1), i direktiv 2009/73/EF.
		– Operatører af naturgasraffinaderier og -behandlingsanlæg.
	e) Brint	– Operatører inden for brintproduktion, -lagring og -transmission.
2. Transport	a) Luft	– Luftfartsselskaber som defineret i artikel 3, nr. 4), i forordning (EF) nr. 300/2008, der anvendes til kommercielle formål.

		– Lufthavnsdriftsorganer som defineret i artikel 2, nr. 2), i Europa-Parlamentets og Rådets direktiv 2009/12/EF[6)], lufthavne som defineret i nævnte direktivs artikel 2, nr. 1), herunder de hovedlufthavne, der er anført i afsnit 2 i bilag II til Europa-Parlamentets og Rådets forordning (EU) nr. 1315/2013[7)] ; og enheder med tilknyttede anlæg i lufthavne.
		– Trafikledelses- og kontroloperatører, der udøver flyvekontroltjenester som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EF) nr. 549/2004[8)].
	b) Jernbane	– Infrastrukturforvaltere som defineret i artikel 3, nr. 2), i Europa-Parlamentets og Rådets direktiv 2012/34/EU[9)].
		– Jernbanevirksomheder som defineret i artikel 3, nr. 1), i direktiv 2012/34/EU, herunder operatører af servicefaciliteter som defineret i nævnte direktivs artikel 3, nr. 12).
	c) Vand	– Rederier, som udfører passager- og godstransport ad indre vandveje, i højsøfarvand eller kystnært farvand som defineret for søtransport i bilag I til Europa-Parlamentets og Rådets forordning (EF) nr. 725/2004[10)], bortset fra de enkelte fartøjer, som drives af disse rederier.
		– Driftsorganer i havne som defineret i artikel 3, nr. 1), i Europa-Parlamentets og Rådets direktiv 2005/65/EF[11)], herunder deres havnefaciliteter som defineret i artikel 2, nr. 11), i forordning (EF) nr. 725/2004; og enheder, der opererer anlæg og udstyr i havne.
		– Operatører af skibstrafiktjenester som defineret i artikel 3, litra o), i Europa-Parlamentets og Rådets direktiv 2002/59/EF[12)].
	d) Vejtransport	– Vejmyndigheder som defineret i artikel 2, nr. 12), i Kommissionens delegerede forordning (EU) 2015/962[13)], der er ansvarlige for trafikledelse, med undtagelse af offentlige enheder, for hvilke trafikledelse eller drift af intelligente transportsystemer er en ikkeværsentlig del af deres generelle aktivitet.
		– Operatører af intelligente transportsystemer som defineret i artikel 4, nr. 1), i Europa-Parlamentets og Rådets direktiv 2010/40/EU[14)].
3. Bankvirksomhed		Kreditinstitutter som defineret i artikel 4, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013[15)].
4. Finansielle markedsinfrastrukturer		– Operatører af markedspladser som defineret i artikel 4, nr. 24), i Europa-Parlamentets og Rådets direktiv 2014/65/EU[16)].
		– Centrale modparter (CCP'er) som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012[17)].
5. Sundhed		– Sundhedstjenesteydere som defineret i artikel 3, litra g), i Europa-Parlamentets og Rådets direktiv 2011/24/EU[18)].
		– EU-referencelaboratorier, der er omhandlet i artikel 15, i Europa-Parlamentets og Rådets forordning (EU) 2022/2371[19)].
		– Enheder, der udfører forsknings- og udviklingsaktiviteter vedrørende lægemidler som defineret i artikel 1, nr. 2), i Europa-Parlamentets og Rådets direktiv 2001/83/EF[20)].

		– Enheder, der fremstiller farmaceutiske råvarer og farmaceutiske præparater som omhandlet i hovedafdeling C, hovedgruppe 21, i NACE rev. 2. – Enheder, som fremstiller medicinsk udstyr, som den anser for at være kritisk i en folkesundhedsmæssig krisesituation (»liste over kritisk medicinsk udstyr til folkesundhedsmæssige krisesituationer«) i den i artikel 22 i Europa-Parlamentets og Rådets forordning (EU) 2022/123[21)] anvendte betydning.
6. Drikkevand		Leverandører og distributører af drikkevand som defineret i artikel 2, nr. 1), litra a), i Europa-Parlamentets og Rådets direktiv (EU) 2020/2184[22)] bortset fra distributører, for hvilke distribution af drikkevand er en ikkevæsentlig del af deres generelle aktivitet med distribution af andre råvarer og varer.
7. Spildevand		Virksomheder, der indsamler, bortskaffer eller behandler byspildevand, husspildevand eller industrispildevand som defineret i artikel 2, nr. 1), 2) og 3), i Rådets direktiv 91/271/EØF[23)], bortset fra virksomheder, for hvilke indsamling, bortskaffelse eller behandling af byspildevand, husspildevand eller industrispildevand er en ikkevæsentlig del af deres generelle aktivitet.
8. Digital infrastruktur		– Udbydere af internetudvekslingspunkter.
		– DNS-tjenesteudbydere, bortset fra operatører af rodnavneservere.
		– Topdomænenavneadministratorer.
		– Udbydere af cloudcomputingtjenester.
		– Udbydere af datacentertjenester.
		– Udbydere af indholdsleveringsnetværk.
		– Tillidstjenesteudbydere.
		– Udbydere af offentlige elektroniske kommunikationsnet.
		– Udbydere af offentligt tilgængelige elektroniske kommunikationstjenester.
9. Forvaltning af IKT-tjenester (business-to-business)		– Udbydere af administrerede tjenester. – Udbydere af administrerede sikkerhedstjenester.
10. Offentlig forvaltning		– Offentlige forvaltningsenheder under den centrale forvaltning som defineret af en medlemsstat i overensstemmelse med national ret.
		– Offentlige forvaltningsenheder på regionalt plan som defineret af en medlemsstat i overensstemmelse med national ret.
11. Rummet		Operatører af jordbaseret infrastruktur, der ejes, forvaltes og drives af medlemsstater eller private parter, og som understøtter levering af rumbaserede tjenester, undtagen udbydere af offentlige elektroniske kommunikationsnet.

1) Europa-Parlamentets og Rådets direktiv (EU) 2019/944 af 5. juni 2019 om fælles regler for det indre marked for elektricitet og om ændring af direktiv 2012/27/EU (EUT L 158 af 14.6.2019, s. 125).

2) Europa-Parlamentets og Rådets forordning (EU) 2019/943 af 5. juni 2019 om det indre marked for elektricitet (EUT L 158 af 14.6.2019, s. 54).

3) Europa-Parlamentets og Rådets direktiv (EU) 2018/2001 af 11. december 2018 om fremme af anvendelsen af energi fra vedvarende energikilder (EUT L 328 af 21.12.2018, s. 82).

4) Rådets direktiv 2009/119/EF af 14. september 2009 om forpligtelse for medlemsstaterne til at holde minimumslagre af råolie og/eller olieprodukter (EUT L 265 af 9.10.2009, s. 9).

5) Europa-Parlamentets og Rådets direktiv 2009/73/EF af 13. juli 2009 om fælles regler for det indre marked for naturgas og om ophævelse af direktiv 2003/55/EF (EUT L 211 af 14.8.2009, s. 94).

6) Europa-Parlamentets og Rådets direktiv 2009/12/EF af 11. marts 2009 om lufthavnsafgifter (EUT L 70 af 14.3.2009, s. 11).

7) Europa-Parlamentets og Rådets forordning (EU) nr. 1315/2013 af 11. december 2013 om Unionens retningslinjer for udvikling af det transeuropæiske transportnet og om ophævelse af afgørelse nr. 661/2010/EU (EUT L 348 af 20.12.2013, s. 1).

8) Europa-Parlamentets og Rådets forordning (EF) nr. 549/2004 af 10. marts 2004 om rammerne for oprettelse af et fælles europæisk luftrum (»rammeforordningen«) (EUT L 96 af 31.3.2004, s. 1).

9) Europa-Parlamentets og Rådets direktiv 2012/34/EU af 21. november 2012 om oprettelse af et fælles europæisk jernbaneområde (EUT L 343 af 14.12.2012, s. 32).

10) Europa-Parlamentets og Rådets forordning (EF) nr. 725/2004 af 31. marts 2004 om bedre sikring af skibe og havnefaciliteter (EUT L 129 af 29.4.2004, s. 6).

11) Europa-Parlamentets og Rådets direktiv 2005/65/EF af 26. oktober 2005 om bedre havnesikring (EUT L 310 af 25.11.2005, s. 28).

12) Europa-Parlamentets og Rådets direktiv 2002/59/EF af 27. juni 2002 om oprettelse af et trafikovervågnings- og trafikinformationssystem for skibsfarten i Fællesskabet og om ophævelse af Rådets direktiv 93/75/EØF (EFT L 208 af 5.8.2002, s. 10).

13) Kommissionens delegerede forordning (EU) 2015/962 af 18. december 2014 om supplerende regler til Europa-Parlamentets og Rådets direktiv 2010/40/EU for så vidt angår tilrådighedsstillelse af EU-dækkende tidstro trafikinformationstjenester (EUT L 157 af 23.6.2015, s. 21).

14) Europa-Parlamentets og Rådets direktiv 2010/40/EU af 7. juli 2010 om rammerne for indførelse af intelligente transportsystemer på vejtransportområdet og for grænsefladerne til andre transportformer (EUT L 207 af 6.8.2010, s. 1).

15) Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og om ændring af forordning (EU) nr. 648/2012 (EUT L 176 af 27.6.2013, s. 1).

16) Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af direktiv 2002/92/EF og direktiv 2011/61/EU (EUT L 173 af 12.6.2014, s. 349).

17) Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 om OTC-derivater, centrale modparter og transaktionsregistre (EUT L 201 af 27.7.2012, s. 1).

18) Europa-Parlamentets og Rådets direktiv 2011/24/EU af 9. marts 2011 om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser (EUT L 88 af 4.4.2011, s. 45).

19) Europa-Parlamentets og Rådets forordning (EU) 2022/2371 af 23. november 2022 om alvorlige grænseoverskridende sundhedstrusler og om ophævelse af afgørelse nr. 1082/2013/EU (EUT L 314 af 6.12.2022, s. 26).

20) Europa-Parlamentets og Rådets direktiv 2001/83/EF af 6. november 2001 om oprettelse af en fællesskabskodeks for humanmedicinske lægemidler (EFT L 311 af 28.11.2001, s. 67).

21) Europa-Parlamentets og Rådets forordning (EU) 2022/123 af 25. januar 2022 om styrkelse af Det Europæiske Lægemiddelagenturs rolle i forbindelse med kriseberedskab og krisestyring med hensyn til lægemidler og medicinsk udstyr (EUT L 20 af 31.1.2022, s. 1).

22) Europa-Parlamentets og Rådets direktiv (EU) 2020/2184 af 16. december 2020 om kvaliteten af drikkevand (EUT L 435 af 23.12.2020, s. 1).

23) Rådets direktiv 91/271/EØF af 21. maj 1991 om rensning af byspildevand (EFT L 135 af 30.5.1991, s. 40).