



Energistyrelsen

Vejledning: Leverandørstyring

Kontor/afdeling
Beredskab

Dato
06-07-2026



Energistyrelsen

Energistyrelsen

Carsten Niebuhrs Gade 43
1577 København V

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

www.ens.dk



Versionshistorik

Versions-nr.	Ændret	Ændret af	Kommentarer
1	25.06.2026	Luna D. Persson, Kristoffer Colding, Salmina S. Lisberg, Peter K. Egelund og Stine Buemann	Dokumentet blev oprettet.
1.1	06.07.2026	Stine Buemann	Fortrolighedsstempel fjernet.



Indhold

Indledning	4
Bekendtgørelsens krav	5
Procedurer for forsyningskædesikkerhed i leverandørforhold (§ 29)	5
Metoder til at identificere, vurdere og håndtere risici (§ 29, stk. 1, pkt. 1)	5
Metoder til at vurdere modstandsdygtigheden (§ 29, stk. 1, pkt. 2)	6
Krav til leverandøraftalen (§ 30).....	6
Passende foranstaltninger til at styre risici og håndtere hændelser (§ 30, stk. 1, nr. 1)	7
Underretning om væsentlige hændelser (§ 30, stk. 1, nr. 2).....	7
Bistand til rapporteringsforpligtelser (§ 30, stk. 1, nr. 3)	8
Inddragelse i Energistyrelsens tilsyn (§ 30, stk. 1, nr. 4)	8
Involvering i øvelser (§ 30, stk. 1, nr. 5)	9
Inddragelse i beredskabsarbejdet (§ 30, stk. 1, nr. 6).....	10
Kriterier for udlicitering til underleverandører (§ 30, stk. 1, nr. 7).....	10
Ejerskab til data (§ 30, stk. 1, nr. 8)	11
Procedurer for styring af fjernadgange (§ 31)	11
Dokumentation (§ 32, stk. 1 og 2).....	12
Øvrige krav	13



Indledning

Virksomhederne i el-, gas-, brint-, olie-, fjernvarme- og fjernkølingssektoren skal, jf. bekendtgørelse om modstandsdygtighed og beredskab i energisektoren nr. 260 af 6. marts 2025 (bekendtgørelsen) § 29-32 leve op til forskellige krav vedrørende leverandørstyring og forsyningskædesikkerhed.

Denne vejledning er målrettet virksomheder i niveau 2-5 i energisektoren, som indgår i et eller flere leverandørforhold, der understøtter eller helt udliciterer væsentlige processer og leverancer i leveringen af virksomhedens tjenester.

Den enkelte virksomhed har ansvaret for de tjenester, den leverer – også når driften helt eller delvist er outsourcet. Dette indebærer, at virksomheden skal sikre, at der er etableret passende tekniske og organisatoriske sikkerhedsforanstaltninger både internt og hos leverandørerne, samt at parterne overholder bekendtgørelsens krav i leverandørforhold.

Nogle leverandører og underleverandører kan få adgang til virksomhedens net- og informationssystemer, og derfor kan sikkerhedshændelser hos disse få direkte konsekvenser for driften og efterlevelsen af bekendtgørelsens krav. Risici i leverandør- og forsyningskædesikkerheden er dermed en integreret del af virksomhedens samlede risikoprofil og skal håndteres på linje med øvrige drifts-, sikkerheds- og beredskabsrisici.

Formålet med denne vejledning er at understøtte virksomhedernes arbejde med at sikre, at direkte leverandører og underleverandører opfylder virksomhedens behov for forsyningssikkerhed og krav til cybersikkerhed, så virksomhedens levering af tjenesten ikke påvirkes negativt af sårbarheder eller hændelser hos virksomhedens leverandører eller i deres produkter/tjenester.

Vejledningen gennemgår de krav, bekendtgørelsen stiller til virksomheden om procedurer for håndtering af og i forbindelse med indgåelse af en kontrakt med en leverandør, som understøtter eller helt udliciterer væsentlige processer og leverancer i leveringen af virksomhedens tjenester. Undervejs lister vejledningen desuden en række generelle anbefalinger til livscyklussen i leverandørforholdet og de overvejelser, som en virksomhed kan gøre sig i forhold til risikovurdering, kontraktforhold, løbende samarbejder og ophør af samarbejdet. De lovmæssige krav markeres med tydelige henvisninger til de relevante paragraffer i de respektive underafsnit.

Endelig inkluderer vejledningen en liste over områder, hvor bekendtgørelsen også nævner forhold vedrørende leverandøraftaler, som virksomheden selv skal indarbejde i sit eget beredskab.



Denne vejledning kan med fordel suppleres af en række af de vejledninger¹, Energistyrelsen har udarbejdet om andre emner i bekendtgørelsen, som fx "Kontrakter med it-sikkerhedstjenester", "Logning og monitorering", "Netværkssegmentering", "Udarbejdelse af beredskabsplaner for niveau 2-5-virksomheder" og "Øvelsesplanlægning". Alle vejledningerne kan findes på Energistyrelsens lukkede beredskabs-site.

Bekendtgørelsens krav

Procedurer for forsyningskædesikkerhed i leverandørforhold (§ 29)

Virksomhederne i sektoren skal have procedurer for forsyningskædesikkerhed i sine leverandørforhold. Formålet med bestemmelsen er, at den enkelte virksomhed sikrer sig, at virksomheden træffer passende og forholdsmæssige foranstaltninger i forhold til produkter og tjenester, som virksomheden anvender i leveringen af sine tjenester.

Helt konkret stiller bekendtgørelsen krav om, at procedurerne skal indeholde beskrivelser af to ting:

Metoder til at identificere, vurdere og håndtere risici (§ 29, stk. 1, pkt. 1)

Virksomhedens procedurer skal beskrive de metoder, som virksomheden anvender til at identificere, vurdere og håndtere risici, der er specifikke for hver direkte leverandør og tjenesteudbyder i forsyningskæden. Det gælder også risici, der er forbundet med afhængigheder af underleverandører og internationale forhold i en aftale med en direkte leverandør og tjenesteudbyder. I kan overveje:

- Har I fx faste parametre og målepunkter, som I vurderer potentielle leverandører ud fra?
- Hvordan kortlægger I, om jeres leverandør fx er afhængig eller påvirkes af udefrakommende faktorer?
- Gennemfører I eventuelt audits hos kommende og eksisterende leverandører?
- Er der nogle hensyn, I vægter højere end andre?
- Er der leverancer, som skal undergå grundigere risikovurdering end andre? Og hvordan beslutter I det?
- Har I eventuelt erfaringer med at implementere foranstaltninger, der kan reducere eller helt fjerne risici?

¹ Der findes også en række konkrete standarder, som virksomhederne kan overveje at bruge, fx SektorCERT's "Håndbog om SektorCERTs 25 anbefalinger" (www.sektorcert.dk) og Center for Internet Security's "The 18 CIS Critical Security Controls" (www.cisecurity.org).



Overvej også, om der eventuelt opstår nye risici for virksomheden som en del af leverandørforholdet.

Formatet på risikovurderingen kan variere efter behov og kontekst, men Energistyrelsen anbefaler generelt, at virksomheden indarbejder processerne for risikovurderingen af leverandører i virksomhedens øvrige arbejde med risici. På den måde kan risici i leverandørforholdene indgå i virksomhedens samlede risikobillede.

Metoder til at vurdere modstandsdygtigheden (§ 29, stk. 1, pkt. 2)

Virksomhedernes procedurer skal også inkludere en beskrivelse af de metoder, virksomheden bruger til at vurdere modstandsdygtigheden af de leverede produkter og tjenester. Det omfatter blandt andet, hvordan virksomheden vurderer kvaliteten af de tekniske og organisatoriske foranstaltninger, som leverandøren har implementeret til at håndtere risici i net- og informationssystemer.

Formålet er at sikre, at leverancer lever op til virksomhedens krav til drift, sikkerhed og beredskab, både før de tages i brug og i hele deres livscyklus.

I den forbindelse bør virksomheden tage stilling til:

- Udfører I Factory Acceptance Tests (FAT) og Site Acceptance Tests (SAT), inden I flytter applikationer eller lignende fra udviklings- til produktionsmiljøet?
- Hvilke faggrupper og organisatoriske lag må og kan vurdere, om de leverede produkter lever op til kravene – både i kontrakten og til sikkerhed og beredskab generelt?
- Hvornår i processen vurderer I produktet eller leverancen? Og gør I det eventuelt flere gange i processen?

Krav til leverandøraftalen (§ 30)

Når en virksomhed indgår en aftale med en leverandør af et produkt eller en tjeneste, der kan påvirke forsyningssikkerheden eller sikkerheden i virksomhedens net- og informationssystemer, er der en række forhold, som skal være aftalt på forhånd.

Leverancerne kan fx være (ikke udtømmende liste):

- Drift og vedligehold af IT- eller OT-systemer (fx SCADA, energistyringssystemer eller netværksinfrastruktur).
- Cloud- og hostingtjenester.
- Software og applikationer med adgang til forretningskritiske data eller systemer.
- Fjernadgangsløsninger og supportaftaler.
- Komponenter og udstyr til produktions- eller distributionsanlæg (fx styresystemer, sensorer eller kommunikationsudstyr).



- Sikkerhedstjenester, herunder overvågning, incident response eller penetrationstest.

Det er nødvendigt at fastlægge klare rammer for samarbejdet, både for at nedbringe risikoen for, at der opstår tvister eller tvivl om parternes forpligtelser over for hinanden, og fordi virksomheden er forpligtet til at sikre sig, at leverandøren lever op til de krav, der stilles til sikkerhed og beredskab i bekendtgørelsen.

Bekendtgørelsen stiller krav om, at nedenstående er formaliseret i aftalen, men virksomheden bestemmer i de fleste tilfælde selv, om det skal indgå i selve kontrakten, i en rammeaftale eller i et bilag til selve kontrakten.

Energistyrelsen kan under bekendtgørelsens bestemmelser ikke føre tilsyn med leverandøren. Men Energistyrelsen kan påbyde virksomhederne at sikre sig, at leverandøren lever op til relevante bestemmelser i bekendtgørelsen. Energistyrelsen kan også anmode om, at leverandøren deltager i tilsynet.

De følgende underafsnit vedrører i bekendtgørelsen først og fremmest de produkter og tjenester, der kan påvirke forsyningssikkerheden eller sikkerheden i virksomhedens net- og informationssystemer. I kan dog også med fordel overveje, om der er andre ydelser, som aftalekravene kan være relevante for.

Passende foranstaltninger til at styre risici og håndtere hændelser (§ 30, stk. 1, nr. 1)

Virksomheden skal stille krav om, at leverandøren har passende foranstaltninger til at styre risici for og håndtering af hændelser i forbindelse med de tjenester og produkter, som leverandøren er ansvarlig for.

Foranstaltningerne skal være proportionelle med den specifikke leverances betydning for leveringen af tjenesten.

Underretning om væsentlige hændelser (§ 30, stk. 1, nr. 2)

Virksomheden skal sikre sig, at leverandøren informerer virksomheden om alle hændelser, der kan påvirke de produkter og tjenester, parterne har indgået aftale om.

I bør på forhånd aftale:

- Hvordan og hvor hurtigt skal underretningen ske?
- Hvor lang tid må der gå, fra leverandøren opdager en hændelse, til I får besked om den?



- Hvor hurtigt skal I have informationen, før I selv kan overholde bekendtgørelsens krav om indberetning inden for henholdsvis 24 og 72 timer?²
- Hvordan skal viden om hændelsen distribueres? Skal I fx ringes op på en døgnbemandet kontrolrumsfunktion?

Det kan være afgørende for hastigheden, at viden om en hændelse formidles i et sprog og på en måde, som virksomheden med rimelighed kan forventes at forstå. I bør derfor også overveje, om kontrakten skal inkludere en beskrivelse af målgruppen og sproget.

Bistand til rapporteringsforpligtelser (§ 30, stk. 1, nr. 3)

I skal som virksomhed underrette Energistyrelsen om enhver hændelse, som har væsentlig indflydelse på leveringen af virksomhedens tjenester.³ I skal sørge for, at jeres aftale med leverandøren sikrer, at leverandøren bidrager til, at I kan overholde jeres rapporteringsforpligtelser.

I bør derfor på forhånd afklare, hvor de leverede produkter og ydelser har afgørende betydning for virksomhedens mulighed for at levere sin tjeneste. Dermed kan I også lettere konkretisere, hvad der skal betragtes som en væsentlig hændelse.⁴

Aftal på forhånd, hvordan, hvor hurtigt og i hvilket format leverandøren kan levere input, og hvor hurtigt I forventer at få disse. Interviewer I fx leverandøren? Skal leverandøren udfylde en foruddefineret blanket? Må input bestå af en mail med fritext?

Vær i den forbindelse særligt opmærksom på, at bekendtgørelsen stiller krav om underretning inden for henholdsvis 24 timer og 72 timer samt evaluering af hændelsen inden for en måned efter hændelsens afslutning.⁵

Inddragelse i Energistyrelsens tilsyn (§ 30, stk. 1, nr. 4)

Energistyrelsen fører tilsyn med virksomhedernes overholdelse af bestemmelserne i bekendtgørelsen og lov om styrket beredskab i energisektoren, nr. 258 af 6. marts 2025.

² Læs mere i den eller de relevante sektorplaner samt i vejledningen "Indberetning og evaluering af hændelser", som kan findes på Energistyrelsens lukkede beredskabssite.

³ Læs mere i den eller de relevante sektorplaner samt i vejledningen "Indberetning og evaluering af hændelser", som kan findes på Energistyrelsens lukkede beredskabssite.

⁴ Læs mere om kravene til fortegnelser i §§ 14-17 i bekendtgørelsen.

⁵ Læs mere i den eller de relevante sektorplaner samt i vejledningen "Indberetning og evaluering af hændelser", som kan findes på Energistyrelsens lukkede beredskabssite.



Virksomheden skal i kontrakten sikre sig, at den direkte leverandør kan indgå i disse tilsyn, enten ved fysisk fremmøde eller ved at stå til rådighed for telefon-/onlineinterviews i det tidsrum, tilsynet er varslet.

Involvering i øvelser (§ 30, stk. 1, nr. 5)

Virksomheden skal gennemføre et antal øvelser over en femårig periode. Bekendtgørelsen definerer en række krav til, hvor ofte øvelserne skal gennemføres, hvem der skal involveres, og hvilke øvelseselementer (emner) virksomheden skal træne.⁶

Bekendtgørelsen bestemmer i bilag 4, at virksomheden skal træne leverandøren i to obligatoriske øvelseselementer.⁷

- Nr. 13: Inddragelse af leverandører i håndteringen af hændelser.
- Nr. 14: Inddragelse af leverandører af forsyningskritiske net- og informationssystemer i håndtering af hændelser.

Når I indgår en kontrakt med en direkte leverandør, som kan få en central rolle i håndteringen af en hændelse med væsentlig indflydelse på leveringen af virksomhedens tjenester, skal I derfor aftale rammerne for, at leverandøren indgår i jeres øvelser.

I bør som virksomhed blandt andet vurdere, hvordan I bliver betrykkede i, at virksomheden kan levere sine produkter og tjenester i en skarp situation:

- Er det, når I sammen har gennemgået procedurerne for hændeshåndtering i en skrivebordsøvelse?
- Eller skal leverandøren testes i mobiliseringshastighed, kendskab til jeres systemer eller detailkompetencer i et eller flere udvalgte scenarier?
- Ønsker I at have mulighed for at gennemføre uvarslede øvelser?
- Hvor ofte i løbet af den femårige periode ønsker I at træne leverandøren?
- Har I et ønske om, at en vis procentdel eller centrale medarbejdere hos leverandøren har deltaget i øvelsesaktiviteter?

⁶ Læs mere om dette i vejledningen "Øvelsesplanlægning – udarbejdelse af den femårige øvelsesplan", som kan findes på Energistyrelsens lukkede beredskabssite.

⁷ Derudover stiller bekendtgørelsen særskilt krav om aktivering af virksomhedens it-sikkerhedstjeneste i øvelseselement 15. Læs mere om indgåelse af aftaler med it-sikkerhedstjenesten i vejledningen "Kontrakter med it-sikkerhedstjenester", som findes på Energistyrelsens lukkede beredskabssite.



Husk også, at I skal evaluere øvelsen i en rapport til Energistyrelsen inden for tre måneder efter øvelsen.⁸ Hvis I ønsker, at leverandøren skal bidrage til rapportens indhold, kan det også være en god idé af afstemme forventningerne til form på og indhold i opsamlingen i jeres aftale.

Inddragelse i beredskabsarbejdet (§ 30, stk. 1, nr. 6)

Virksomheden skal i leverandøraftalen sikre sig, at leverandøren kan inddrages i virksomhedens beredskabsarbejde i det omfang, det er relevant.

Virksomheden bør på et risikobaseret grundlag vurdere, i hvilket omfang leverandøren skal bidrage til opgaveløsningen og de koordinerende aktiviteter i beredskabsarbejdet.

Fx stiller bekendtgørelsen i § 18, stk. 4, krav om, at virksomheden gennemfører sin risiko- og sårbarhedsvurdering (ROS)⁹ med inddragelse af relevante medarbejdere og leverandører med teknisk og organisatorisk kendskab til virksomhedens processer, anlæg, net- og informationssystemer, netværksinfrastruktur og leverandørforhold. Hvis der er spørgsmål i ROS, som leverandøren er den bedste til at svare på, skal I sikre jer, at leverandøren er forpligtet til at deltage i analysearbejdet et vist omfang.

Der kan også være tilfælde, hvor virksomheden har brug for leverandørens input eller kvalificering af (dele af) beredskabsplaner, detailinstrukser mv. I disse tilfælde skal virksomheden også sikre sig, at leverandøren kan bidrage til opgaverne, eller at det er muligt for virksomheden at tilkøbe denne ydelse.

Bekendtgørelsen stiller også krav om, at virksomhedernes beredskabsplaner indeholder en beskrivelse af den operationelle ansvarsfordeling mellem virksomheden og dennes samarbejdspartnere og leverandører i forbindelse med håndteringen af en hændelse. Det er selvfølgelig afgørende, at forventningsafstemningen om ansvarsområder mv. er på plads, inden hændelsen indtræffer. Derfor er det nødvendigt at inkludere beskrivelsen af ansvarsfordelingen i leverandøraftalen.

Kriterier for udlicitering til underleverandører (§ 30, stk. 1, nr. 7)

Leverandøraftalen skal indeholde en beskrivelse af, under hvilke kriterier og forhold og i hvilket omfang virksomheden kan acceptere, at leverandøren udliciterer væsentlige dele af sin leverandøraftale til en eller flere underleverandører.

⁸ Læs mere om dette i vejledningen "Evaluering af beredskabsøvelser", som findes på Energistyrelsens lukkede beredskabssite.

⁹ Læs mere om risiko- og sårbarhedsvurderingerne (ROS) på Energistyrelsens lukkede beredskabssite.



Må leverandøren fx hente underleverancer i udlandet? Virksomheden skal sikre sig, at de krav, som virksomheden har stillet til leverandørens overholdelse af relevante bestemmelser i bekendtgørelsen, videreføres til underleverandøren. Virksomheden bør fx være konkret i beskrivelsen af, hvordan leverandøren giver underleverandøren adgang til oplysninger om og systemer i virksomheden, og af om der er særlige krav til sikkerhedsgodkendelser¹⁰ af underleverandøren.

Virksomheden skal betinge sig, at en leverandør ikke kan udlicitere (dele af) leverandøraftalen, medmindre virksomheden godkender dette.

Ejerskab til data (§ 30, stk. 1, nr. 8)

Virksomheden skal sikre sig, at I bevarer ejerskabet til de data, som er nødvendige for leveringen af virksomhedens tjeneste – også når leverandørforholdet ophører.

Det samme gælder de data, som er fortrolige, jf. § 26 i lov om styrket beredskab i energisektoren, nr. 258 af 6. marts 2025. Det gælder fx forhold om organisatorisk beredskab, fysisk sikring og cybersikkerhed i virksomheden og informationer, som er indgået i vurderingen af sikkerhedsgodkendelser.

Overvej, om I skal inkludere en beskrivelse af, hvordan leverandøren opbevarer data undervejs i kontraktperioden, og hvordan I ønsker, at data bliver opbevaret efter endt samarbejde (eller når data er overdraget til virksomheden).

Virksomheder i niveau 4 og 5 skal være særligt opmærksomme på, at de skal opbevare logs i 13 måneder.¹¹ Derfor skal de sikre sig, at de får overdraget disse logs eller fortsat har adgang til data, når aftalen ophører.

Procedurer for styring af fjernadgange (§ 31)

Virksomheden skal have en procedure for, hvordan I styrer fjernadgange til direkte leverandører og tjenesteudbydere, som kan tilgå virksomhedens forsyningskritiske net- og informationssystemer.

Hvis leverandøren har brug for at få adgang til de forsyningskritiske net- og informationssystemer, skal procedurerne for, hvordan dette håndteres, tildeles og administreres, fremgå af leverandøraftalen.

¹⁰ Læs mere i vejledningen "Sikkerhedsgodkendelser i energisektoren", som kan findes på Energistyrelsens lukkede beredskabssite.

¹¹ Læs mere i vejledningen "Logning og monitorering", som findes på Energistyrelsens lukkede site.



Bekendtgørelsens regler¹² for adgangsstyring, både fysisk og logisk, gælder også for leverandørerne. Det gælder fx kravene om tidsbegrænset adgang, arbejdsbetingsbehov samt detektion og håndtering af cyberangreb. Det er virksomhedens ansvar i leverandørstyringen at sikre, at leverandøren lever op til disse krav.

Virksomheden skal være opmærksom på, at bekendtgørelse om sikkerhedsgodkendelse i energisektoren nr. 1075 af 27. august 2025 stiller krav om sikkerhedsgodkendelser af medarbejdere og eksterne konsulenter i virksomheder i niveau 3-5 med adgang til en række definerede funktioner.¹³

Dokumentation (§ 32, stk. 1 og 2)

Virksomheden skal sikre sig, at alle de krav til organisatorisk beredskab, fysisk sikring og cybersikkerhed, der er beskrevet i ovenstående, fremgår af leverandøraftalen.

Leverandøren skal kunne dokumentere, at den overholder de krav, som virksomheden stiller i sin leverandøraftale.

Bekendtgørelsen stiller ikke krav til, hvordan denne dokumentation skal udformes eller foregå. Alt efter den konkrete kontrakt og det specifikke samarbejde mellem parterne kan det være forskelligt, hvad en virksomhed vurderer relevant. Under alle omstændigheder vil det være i virksomhedens interesse, at samarbejdet styres på en meningsgivende måde.

I nogle virksomheder har man en kontaktperson eller leverandøransvarlig, som kan bidrage til, at der i samarbejdet er løbende opmærksomhed på de konkrete sikkerhedsopgaver, som leverandøren skal bidrage til. Andre virksomheder opretter dedikerede grupper, der fungerer som samarbejdsorganisationer, hvor der er et tæt praktisk samarbejde og koordinering, og hvor man håndterer dokumentationen af overholdelsen af kravene løbende.

Energistyrelsen anbefaler, at virksomheden anvender sin eksisterende praksis for leverandørsamarbejde. Hvis virksomheden allerede har processer for, hvordan I følger op med leverandører og sikrer levering og efterlevelse af krav, så kan I med fordel tilføje håndteringen af bekendtgørelsens krav til disse. Hvis I ikke allerede har dokumenterede processer for leverandørkontrol, bør I enten oprette processer og dokumentere disse eller tydeligt dokumentere eksisterende processer.

¹² Kravene er beskrevet i bekendtgørelsens § 51-57.

¹³ Læs mere i vejledningen "Sikkerhedsgodkendelser i energisektoren", som kan findes på Energistyrelsens lukkede beredskabssite.



Virksomheden kan også overveje, om der er behov for et mere konkret opsyn med leverandøren, alt efter hvordan blandt andet leverancer, kritikalitet og sikkerhed er vurderet i risikovurderingen.

For nogle virksomheder kan det give mening at gennemføre løbende opfølgning og kontrol med sine leverandører. Dette kan fx gennemføres af de medarbejdere, der er en del af det løbende samarbejde, eller af medarbejdere, der ikke til dagligt arbejder direkte med leverandøren, men som har erfaring med leverandørstyring.

For nogle virksomheder kan det måske endog give mening at gennemføre kontrolbesøg eller audits hos leverandøren, enten ved brug af virksomhedens egne medarbejdere eller ved en ekstern part (fx i form af revisionserklæringer). Det kan have stor værdi at få en ekstern vurdering af forhold, processer og sikkerhed, men det skal også give mening i forhold til virksomhedens behov, ønsker og vurderinger af relevante risici.

Øvrige krav

Bekendtgørelsen nævner også leverandøren i forbindelse med en række forhold, som virksomheden skal sikre sig i eget beredskab. En del af dem er allerede berørt i vejledningen, men derudover kan følgende nævnes:

- § 14, stk. 2: Fortegnelserne over de anlæg, der er nødvendige for, at virksomheden kan levere sine tjenester, skal blandt andet beskrive afhængigheder af leverandører.
- § 15, stk. 2: Fortegnelserne over de net- og informationssystemer, som virksomheden anvender i leveringen af sine tjenester, skal blandt andet beskrive afhængigheder af leverandører.
- § 19, stk. 3, pkt. 4: Virksomhedens beredskabsplaner skal blandt andet indeholde procedurer for fremskaffelse af kritiske reservedele fra eget lager eller leverandører.
- § 27, stk. 2: Virksomhedernes risikovurdering af projekter, hvor der indgår leverandørforhold, skal inkludere en vurdering af risici, som følger af leverandørforholdet.
- § 37, stk. 2: Virksomheden skal tage stilling til, hvilke leverandører der må og kan få adgang til forskellige dele af virksomhedens anlæg, herunder mulighed for at færdes uledsaget på anlægget eller dele heraf.