



Energistyrelsen

Vejledning: Kontrakter med it-sikkerheds-tjenester

Checkskema

Kontor/afdeling
Beredskab

Dato
06-07-2026



Energistyrelsen

Energistyrelsen

Carsten Niebuhrs Gade 43
1577 København V

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

www.ens.dk



Versionshistorik

Versions-nr.	Ændret	Ændret af	Kommentarer
1	17.06.2025	Stine Buemann	Dokumentet blev oprettet.
1.1	17.11.2025	Stine Buemann	Tydeliggørelse af fortroligheds-grad i materialet i sidefod og på forsiden. Konsekvensændring af 'BEK' til 'bekendtgørelsen'.
1.2	06.07.2026	Stine Buemann	Fortrolighedsstempel fjernet.



Indhold

Indledning	4
Bekendtgørelsens krav	4
§ 33	4
§ 34	6
Eksempler.....	7
§ 35	9
§ 69	9



Indledning

Virksomhederne i el-, gas-, brint-, olie-, fjernvarme- og fjernkølingssektoren i niveau 2-5 skal, jf. bekendtgørelse om modstandsdygtighed og beredskab i energisektoren nr. 260 af 6. marts 2025 (bekendtgørelsen) § 33, være tilmeldt en it-sikkerhedstjeneste.

Energistyrelsen skal i forbindelse med, at bekendtgørelsen træder i kraft, ikke længere godkende virksomhedens kontrakter med it-sikkerhedstjenesterne. Bekendtgørelsen stiller imidlertid fortsat krav til indholdet af disse kontrakter og til samarbejdet mellem virksomheden og leverandøren. Energistyrelsen følger op på dette i forbindelse med tilsynet hos virksomheden.

Denne vejledning er målrettet virksomheder i niveau 2-5 i energisektoren. Vejledningen er udformet som en checkliste, der gennemgår bekendtgørelsens krav i hovedtræk. Vejledningen redegør både for, hvad kontrakterne skal inkludere, og hvad virksomhederne med fordel også kan overveje at inkludere i aftalen med deres leverandører.

Bekendtgørelsens krav

Bekendtgørelsen stiller relativt få krav til formalia i kontrakterne mellem virksomheden og it-sikkerhedstjenesten. Det er få elementer, som skal fremgå eksplicit af selve leverandøraftalen/kontrakten. De er markeret med en * i skemaet. Derudover er der forholdsvis mange forhold, som skal kunne dokumenteres på anden vis¹, og/eller som det er en god idé at få beskrevet og dokumenteret.

Bemærk, at der også er en del krav til, hvad virksomheden selv skal gøre for at danne grundlag for, at it-sikkerhedstjenesten kan løfte sin opgave. Det kan dog være en fordel for begge parter, hvis I afstemmer forventninger på forhånd og skriver ind i kontrakten, hvordan I følger op.

§ 33

Forhold i leverandøraftalen med it-sikkerhedstjenesten	§	Uddybning	Er det inkluderet i kontrakten?
Varsling om relevante sårbarheder og cybertrusler uden ugrundet ophold* <i>Niveau 2-5</i>	33, stk. 1	I skal sikre jer, at I og it-sikkerhedstjenesten har en fælles forståelse af, hvad der er relevant for jeres virksomhed. Det gør I bl.a. ved at sørge for, at virksomheden kender jeres net- og informationssystemer.	

¹ Det kan fx være et bilag til kontrakten, et mødereferat mellem virksomheden og leverandøren og et fast punkt på dagsordenen til møder med leverandøren.



Vejledning om mitigerende tiltag* <i>Niveau 2-5</i>	§ 33, stk. 1	It-sikkerhedstjenesten skal vejlede jer om mitigerende tiltag – dvs. initiativer, foranstaltninger mv., der kan mindske sandsynligheden for, at et angreb får store konsekvenser for den enkelte virksomhed. Det bør fremgå af kontrakten, hvor ofte og hvordan dette skal ske.	
Hvor hurtigt skal virksomheden have varsler?* <i>Niveau 2-5</i>	33, stk. 2	It-sikkerhedstjenestens varsler skal sendes til jer "uden ugrundet ophold". I kontrakten skal dette defineres nærmere. Hvor lang tid må der gå, fra it-sikkerhedstjenesten opdager eller får kendskab til en ny sårbarhed eller cybertrussel, til I får besked om den? Det bør også fremgå af kontrakten, hvordan I skal have formidlet varslet. Skal I ringes op? Skal sikkerhedstjenesten sende en mail til en døgnbemandet kontrolrumsfunktion? Endelig kan det være afgørende for hastigheden, at varslet formidles i et sprog og på en måde, som man har en vis forventning om, at modtageren, altså virksomheden, kan forstå. Derfor bør I overveje, om kontrakten skal inkludere en beskrivelse af målgruppen og tydeligheden i formidlingen af truslen.	
Nødvendigt kendskab til virksomhedens net- og informationssystemer <i>Niveau 2-5</i>	33, stk. 3	It-sikkerhedstjenesten skal varsle jer om alle relevante it-sårbarheder og cybertrusler. For at de kan gøre dette, er det nødvendigt, at it-sikkerhedstjenesten har tilstrækkelig viden om og kendskab til jeres net- og informationssystemer. Derfor bør det fremgå af kontrakten, præcis hvilke net- og informationssystemer I forventer bliver dækket af aftalen. Er der evt. systemer, som ikke dækkes af aftalen? I bør også aftale, hvad virksomheden selv skal gøre for at holde it-sikkerhedstjenesten opdateret. Hvor ofte informerer virksomheden fx it-sikkerhedstjenesten om ændringer i virksomhedens netværksstruktur? Informerer I it-sikkerhedstjenesten	



		om opdateringer i eller udfordringer med systemerne? Deler I viden om hændelser, anomalier og andre observationer?	
Kompetente medarbejdere i egen virksomhed <i>Niveau 2-5</i>	33, stk. 4	I skal sørge for, at I internt har medarbejdere, som kan modtage varslerne og omsætte disse til konkrete tiltag i virksomheden. Dette gælder, uanset hvor alvorligt og akut varslet er. I virksomheden betyder det, at medarbejderne skal uddannes i og trænes til at forstå varslerne og deres alvorlighed. I bør derfor overveje, om it-sikkerhedstjenesten skal bidrage til at højne og/eller vedligeholde vidensniveauet hos jeres medarbejdere – og om dette skal være inkluderet i kontrakten. Det betyder også, at I skal have en bemanning eller en vagtordning, der kan reagere kompetent, uanset hvornår varslet sendes fra it-sikkerhedstjenesten.	
Alle skal nævnes i kontrakten – og den skal opbevares hos alle tilmeldte virksomheder* <i>Niveau 2-5</i>	33, stk. 5	Hvis I indgår en kontrakt med en it-sikkerhedstjeneste i fællesskab med andre virksomheder, skal alle virksomhedernes navne fremgå af kontrakten. Det kan fx være aktuelt, hvis I har fået tilladelse til at indgå samordnet beredskab med andre virksomheder. Alle de virksomheder, som kontrakten dækker, skal opbevare en kopi af den gældende kontrakt. Overvej også at inkludere en beskrivelse af, hvordan informationerne om trusler mv. deles mellem de virksomheder, der er dækket af kontrakten.	

§ 34

Forhold i leverandøraftalen med it-sikkerhedstjenesten	§	Uddybning	Er det inkluderet i kontrakten?
Assistance i forbindelse med en hændelse² <i>Niveau 3-5</i>	34, stk. 1	I skal sikre jer, at it-sikkerhedstjenesten hjælper jeres virksomhed, når I skal håndtere en hændelse.	

² I den tidligere bekendtgørelse er denne form for bistand til virksomheden blevet kaldt "reaktive ydelser".



		Det gælder både i forbindelse med en konkret sikkerhedshændelse og et nedbrud i systemerne. Formålet er dels at skadesbegrænse, dvs. at forhindre, at nedbrud eller et angreb eskalerer til andre net- og informationssystemer. Dels er det afgørende, at I hurtigst muligt kan genoprette de forsyningskritiske net- og informationssystemer. It-sikkerhedstjenesten skal derfor kunne yde teknisk bistand. Endelig skal it-sikkerhedstjenesten hjælpe jer med at sikre bevisindsamling. Selvom det ikke er et krav, at det fremgår af kontrakten, er det svært at forestille sig, at aftalen vil fungere i praksis, hvis ikke de præcise forventninger til de to parter er dokumenteret, inden hændelsen indtræffer. Det er i mange tilfælde en forudsætning for et effektivt samarbejde og krisehåndtering. I bør overveje at inkludere en række beskrivelser i jeres kontrakter, se eksempler nedenfor.	
--	--	---	--

Eksempler

Ansvarsfordeling		Hvad har it-sikkerhedstjenesten ansvar for, og hvad skal I selv sørge for?	
Ydelsens karakter		Hvornår aktiveres it-sikkerhedstjenesten i forbindelse med en hændelse? Hvilke kriterier skal være til stede? Er der evt. situationer, hvor it-sikkerhedstjenesten ikke er forpligtet til at levere ydelsen?	
Faste procedurer for aktivering		Hvad er den maksimale responstid for aktivering og fysisk fremmøde? Hvor lang tid må der gå, før it-sikkerhedstjenesten skal være i gang med at vejlede jer om tiltag til skadesbegrænsning? Og må det evt. foregå online?	
Kompetencer		Hvilke kompetencer skal de konsulenter, som it-sikkerhedstjenesten stiller til rådighed, have? Det	



		tekniske vidensniveau bør matche de trusler, sårbarheder og systemer, der er aktuelle hos jer.	
Øvelser og afprøvning		Er der mulighed for at efterprøve de aftalte tidspunkter for varsling og aktivering? Bemærk, at det er et krav i element 15 i bilag 4 til bekendtgørelsen, at "Aktivering af virksomhedens it-sikkerhedstjeneste" skal øves. Derfor kan det være en god idé at overveje at inkludere betingelserne for træningen af dette i kontrakten. Er øvelsen dækket af kontrakten? Eller afregner I det fra gang til gang? Hvor ofte ønsker I, at it-sikkerhedstjenesten deltager i øvelser? I hvor høj grad skal it-sikkerhedstjenesten deltage? Skal de blot være til rådighed for test af varslings-tid? Eller ønsker I, at de bidrager til den tekniske problemløsning i en eller flere fuldskalaøvelser i løbet af øvelsesperioden? Det kan også være, at I har behov for, at it-sikkerhedstjenesten er med til at vælge, hvad I skal øve, og hvilke scenarier I bør vælge. I kan også overveje, om it-sikkerhedstjenesten skal bidrage til gennemførelse af awareness-tiltag, jf. § 26, stk. 2.	
Hvad gør I, hvis flere er ramt?		Hvordan vil it-sikkerhedstjenesten prioritere jer, hvis der er nedbrud hos flere af it-sikkerhedstjenestens kunder på samme tid?	
Procedure for adgang til virksomhedens net- og informationssystemer		Hvordan giver I it-sikkerhedstjenesten kendskab og adgang til jeres systemer? Kan det ske via fjernadgang? Eller skal it-sikkerhedstjenesten møde op fysisk for at betjene jeres systemer? Hvordan sikrer I, at denne adgang ikke misbruges?	
Hvem kommunikerer om hvad?		Kan I eventuelt få brug for hjælp til kommunikation til kunder, offentligheden og myndighederne?	



		Er der emner, aspekter mv., som I under ingen omstændigheder ønsker, at it-sikkerhedstjenesten kommunikerer om?	
--	--	---	--

§ 35

Forhold i leverandøraftalen med it-sikkerhedstjenesten	§	Uddybning	Er det inkluderet i kontrakten?
Videreformidling af oplysninger <i>Niveau 2-5</i>	35, stk. 1	Oplysninger om sårbarheder og hændelser fra virksomhedens it-sikkerhedstjeneste, som kan have betydning for forsyningen i energisektoren, skal kunne videreformidles til andre virksomheder uden ugrundet ophold. Det betyder bl.a., at I skal have ret til at videredistribuerer relevant information fra jeres it-sikkerhedstjeneste til andre energivirksomheder. Informationerne skal kunne distribueres på alle tidspunkter af døgnet til de rigtige modtagere og i et sprog, der kan forstås af modtagergruppen. I bør aftale med it-sikkerhedstjenesten, hvordan I gør dette, og hvem der har ansvar for hvad. I kan også inkludere en beskrivelse af, hvem der har ansvar for at kortlægge og vedligeholde processen.	

§ 69

Forhold i leverandøraftalen med it-sikkerhedstjenesten	§	Uddybning	Er det inkluderet i kontrakten?
Logning og monitorering <i>Niveau 2-5</i>	69, stk. 1	I skal planlægge logning og monitorering sammen med jeres it-sikkerhedstjeneste, så I sikrer, at it-sikkerhedstjenesten får adgang til de informationer, de skal bruge i deres hændelses- og krisehåndtering. Kravene til både logning og monitorering er konkretiseret i bekendtgørelsen § 65-68³.	

³ Læs mere i Energistyrelsens vejledning 'Logning og monitorering', som kan findes på Energistyrelsens lukkede beredskabssite.



		Det kan i aftalen fx være relevant at beskrive, hvordan it-sikkerhedstjenesten håndterer fortrolighed, og hvordan dataudvekslingen mellem it-sikkerhedstjenesten og et sensornetværk foregår. Aftalen kan fx inkludere: - Opsætning af sensorer i virksomhedens netværk. - En liste over acceptable og uacceptable anomalier. - Procedurer for opdatering og tests af sensornetværket.	
Afgivning af logs inden for 24 timer <i>Niveau 4-5</i>	69, stk. 2	Virksomhederne skal kunne afgive logs til it-sikkerhedstjenesten inden for 24 timer. Det er en forudsætning for den effektive levering af logs, at I forinden er blevet enige om formatet, og hvordan I leverer de ønskede data.	