nätUTKAST

# Föreskrifter och allmänna råd om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn

beslutade den xx xx 2020.

Med stöd av 8 § förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster meddelar Statens energimyndighet följande föreskrifter och allmänna råd.

## 1 kap. Inledande bestämmelser och definitioner

Tillämpningsområde

**1 §** I dessa föreskrifter finns bestämmelser för leverantörer av samhällsviktiga tjänster inom energisektorn om riskanalys enligt 12 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster samt om säkerhetsåtgärder enligt 13 och 14 §§ samma lag.

Definitioner

**2 §** Begrepp och uttryck i dessa föreskrifter används i samma betydelse som i lagen om informationssäkerhet för samhällsviktiga och digitala tjänster. Dessutom betyder

*leverantör*: leverantör av tjänster rörande el, olja eller gasförsörjning enligt 3 kap. 1 – 3 §§ Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster, MSBFS 2018:7,

*IT:* nätverk och informationssystem med funktioner för administrativt bruk,

*OT:* nätverk och informationssystem som styr eller mäter en fysisk, analog hårdvara,

*informationssäkerhetskrav:* funktionella krav på säkerhet i nätverk och informationssystem,

*informationssystem:* en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter.

**3 §** Dessa föreskrifter avser en leverantörs nätverk och informationssystem som leverantören använder för att tillhandahålla samhällsviktiga tjänster.

Leverantören ska analysera sina nätverk och informationssystem för att fastställa vilka nätverk och informationssystem som leverantören använder för att tillhandahålla samhällsviktiga tjänster. Leverantören ska dokumentera den metod som används för utförandet av analysen liksom resultatet av analysen.

## 2 kap. Riskanalys

**1 §** Enligt 12 § lagen om informationssäkerhet för samhällsviktiga och digitala tjänster ska leverantörer göra en riskanalys som ska ligga till grund för val av säkerhetsåtgärder enligt 13 och 14 §§ samma lag. I riskanalysen ska leverantören utgå från den analys som utförts enligt 1 kap. 3 §.

**2 §** I samband med riskanalysen ska leverantören göra en omvärldsbevakning för att samla in och analysera information som påverkar riskers konsekvens eller sannolikhet i leverantörens nätverk och informationssystem. Vid utförandet av omvärldsbevakningen ska leverantören särskilt analysera

1. allmänna trender inom cybersäkerhet,
2. tekniska trender och etablerad praxis avseende hotaktörer och sårbarheter i den hårdvara och mjukvara som används inom energisektorn,
3. externa incidenter och hot mot leverantörens nätverk och informationssystem,
4. organisatoriska och tekniska förändringar i leverantörens organisation, samt
5. incidenter i leverantörens nätverks- och informationssystem.

**3 §** I riskanalysen ska leverantören värdera de identifierade riskerna utifrån en bedömning av riskernas sannolikhet och konsekvens. Utifrån leverantörens bedömning av riskernas sannolikhet och konsekvens ska varje risk tilldelas ett riskvärde. Riskerna ska bedömas utifrån hur de påverkar leveransen av den samhällsviktiga tjänsten.

**4 §** En riskanalys ska även innehålla följande uppgifter avseende varje risk som leverantören har identifierat:

1. riskens teoretiska konsekvenser,
2. sannolikhet för att konsekvenser inträffar,
3. konsekvensers allvarlighetsgrad, och
4. befintliga säkerhetsåtgärder som påverkar riskens sannolikhet eller konsekvens.

**5 §** Enligt 12 § lagen om informationssäkerhet för samhällsviktiga och digitala tjänster ska riskanalysen dokumenteras och uppdateras årligen. Vid uppdatering av riskanalysen ska en förnyad riskvärdering ske enligt 2 kap. 3 § mot bakgrund av de säkerhetsåtgärder som har genomförts efter den föregående riskanalysen.

**6 §** I leverantörens riskanalys avseende OT ska särskild hänsyn tas till de unika egenskaperna i och förutsättningarna för leverantörens informationssystem.

## 3 kap. Informationssäkerhetskrav

**1 §** Utöver vad som anges som krav utifrån riskanalys enligt 2 kap. ska leverantören uppfylla informationssäkerhetskrav som anges i 2 – 6 §§.

Leverantören ska dokumentera de processer och metoder som används för att uppfylla informationssäkerhetskraven. Leverantören ska även utföra loggning i syfte att möjliggöra upptäckt och spårning av transaktioner och händelser.

**2 §** Leverantören ska som en del av sitt systematiska informationssäkerhetsarbete

1. ange vem eller vilka personer som har ansvar för informationssäkerhet i leverantörens OT,
2. införa processer avseende säkerhet, liksom verifieringar och uppdateringar i OT, samt
3. fastställa och upprätthålla regler och metoder för fjärråtkomst till leverantörens nätverk och informationssystem.

**3 §** Leverantören ska upprätta en systemförteckning över sin IT och OT genom att

1. kartlägga och analysera de IT- och OT-tjänster samt nätverk och informationssystem som används vid tillhandahållande av samhällsviktiga tjänster,
2. inventera vilka hårdvaror som används i leverantörens IT och OT,
3. inventera vilka mjukvaror som används i leverantörens IT och OT,
4. identifiera vilka interna och externa informationstillgångar liksom vilka hårdvaror och mjukvaror som är mest kritiska för leverantörens tillhandahållande av samhällsviktiga tjänster, samt
5. upprätta en nätverkskarta avseende leverantörens IT och OT.

Systemförteckningen ska hållas uppdaterad.

**4 §** Leverantören ska skydda sin IT och OT genom att

1. segmentera sitt nätverk och filtrera trafiken mellan olika nätverkssegment,
2. minimera användandet av administrationsrättigheter,
3. installera säkerhetsuppdateringar snarast möjligt och enligt beprövade metoder,
4. använda proportionella autentiseringsmetoder,
5. om möjligt använda antivirusprogram på alla enheter som är uppkopplade mot IT och OT, samt
6. begränsa fysisk tillgång till IT och OT.

**5 §** Leverantören ska arbeta för att förebygga och minimera incidenter genom att

1. härda IT och OT hårdvara innan de börjar användas,
2. hantera förändringar i IT och OT med metoder som minimerar risken för störningar eller förändringar i IT:s och OT:s cybersäkerhet, samt
3. hantera hårdvara i IT och OT som har upphört att användas för att säkerställa att känslig information inte avslöjas.

**6 §** Leverantören ska minimera verkningar av incidenter genom att

1. säkerhetskopiera applikationer och information från de delar av IT och OT som är kritiska för tillhandahållande av samhällsviktiga tjänster och regelbundet testa återställning av säkerhetskopior, samt
2. prioritera att nätverk och informationssystem är så redundanta som möjligt utifrån deras väsentlighet för tillhandahållande av den samhällsviktiga tjänsten och utifrån deras tekniska förutsättningar.

## 4 kap. Säkerhetsåtgärder

**1 §** Leverantören ska införa säkerhetsåtgärder dels för att hantera risker enligt 2 kap., dels för att tillgodose informationssäkerhetskrav enligt 3 kap. En säkerhetsåtgärd ska antingen sänka en risks värde eller tillgodose ett informationssäkerhetskrav.

**2 §** Enligt 12 § lagen om informationssäkerhet för samhällsviktiga och digitala tjänster ska leverantören göra en riskanalys som ska ligga till grund för val av säkerhetsåtgärder. I riskanalysen ska det ingå en åtgärdsplan. Åtgärdsplanen ska innehålla följande information avseende varje säkerhetsåtgärd som leverantören har identifierat:

1. vilken risk säkerhetsåtgärden avser,
2. vilket nätverk och informationssystem som säkerhetsåtgärden ska utföras inom,
3. person hos leverantören som ansvarar för säkerhetsåtgärden,
4. planerat datum för genomförande av säkerhetsåtgärden,
5. säkerhetsåtgärdens påverkan på riskens sannolikhet eller konsekvens enligt vad som anges i 2 kap. 3 §, samt
6. riskvärde enligt 2 kap 3 § efter säkerhetsåtgärdens införande.

**3 §** Enligt 14 § lagen om informationssäkerhet för samhällsviktiga och digitala tjänster ska leverantören vidta åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem som denne använder för att tillhandahålla den samhällsviktiga tjänsten. Vid införandet av åtgärder för att uppfylla informationssäkerhetskrav enligt 3 kap. ska leverantören identifiera:

1. vilket nätverk och informationssystem som säkerhetsåtgärden ska utföras inom,
2. person hos leverantören som ansvarar för säkerhetsåtgärden, samt
3. planerat datum för genomförande av säkerhetsåtgärden.

**4 §** Säkerhetsåtgärder ska prioriteras med beaktande av leverantörens riskvärdering enligt 2 kap. 3 § samt med beaktande av de ekonomiska och tidsmässiga resurser som genomförandet av säkerhetsåtgärderna beräknas kräva.

## 5 kap. Undantag

**1 §** När särskilda skäl föreligger får Statens energimyndighet medge undantag från bestämmelserna i dessa föreskrifter.

## Ikraftträdande

Dessa föreskrifter träder ikraft den xx xx 2020.

På Statens energimyndighets vägnar

 Robert Andrén

 XX

# Allmänna råd för Energimyndighetens föreskrift om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn.

## Allmänna råd till 1 kap. om inledande bestämmelser och definitioner

**1 §**

*Utöver Statens energimyndighets föreskrifter om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn finns Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter om:*

* *anmälan och identifiering av leverantörer av samhällsviktiga tjänster, MSBFS 2018:7,*
* *informationssäkerhet för leverantörer av samhällsviktiga tjänster, MSBFS 2018:8,*
* *rapportering av incidenter för leverantörer av samhällsviktiga tjänster, MSBFS 2018:9,*
* *frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet, MSBFS 2018:11.*

**2 §**

*I begreppet ”IT” ingår bland annat e-post, delade filytor och applikationer för personaladministration, ekonomi, försäljning och produktivitet. Begreppet IT kallas ibland ”Kontors-IT”. Även nätverk som innefattar dessa informationssystem omfattas av i begreppet IT.*

*I begreppet ”OT” ingår bl.a. det som kallas ICS (Industrial Control Systems), SCADA (Supervisory Control And Data Acquisition), styrsystem och cyberfysiska system. Även nätverk som innefattar dessa informationssystem omfattas av begreppet OT,*

**3 §**

*Vid fastställandet av vad som ingår i leverantörens tillhandahållande av samhällsviktiga tjänster, och vad som därmed omfattas av leverantörens riskanalys, kan leverantören använda den kartläggning som ska utföras enligt 3 kap. 3 § punkt 1 och 4 denna föreskrift.*

*I analysen bör leverantören ta ställning till vilka delar av leverantörens nätverk och informationssystem som behövs för att kunna upprätthålla kontinuerligt tillhandahållande av samhällsviktiga tjänster, samt vilka delar av nätverket och informationssystemet som kan påverka tillhandahållandet om de inte fungerar på grund av bristande säkerhet.*

*I analysen bör leverantören även ta ställning till vilka applikationer och verktyg som krävs för att åtgärda brister som medför att de informationssäkerhetskrav som anges i 3 kap inte uppfylls.*

## Allmänna råd till 2 kap. om Riskanalys

**2 §**

*Omvärldsbevakningen bör utföras regelbundet och vara en integrerad del av leverantörens verksamhet.*

**3 §**

*Sannolikhet kan värderas på olika sätt. Värderingen kan exempelvis ske genom att ange en procent av sannolikheten och omvandla den till poäng (exempelvis 0 – 25 % ges 1 poäng, 26 – 50 % ges 2 poäng o.s.v.). Ett annat exempel är att jämföra riskers sannolikhet med varandra och rangordna riskerna sinsemellan.*

*Konsekvens av en risk kan också värderas på olika sätt. Beroende på verksamhet kan konsekvensen av en risk värderas utifrån exempelvis ekonomisk effekt, antal användare som berörs, återställningstid för tillhandahållandet av den samhällsviktiga tjänsten vid avbrott eller möjligheten att återuppta tillhandhållandet av den samhällsviktiga tjänsten.*

**4 §**

*Leverantörens bedömning i riskanalysen av de incidenter som kan uppstå i leverantörens nätverk och informationssystem bör avse både incidenter som sker direkt i dessa liksom sådana incidenter som uppstår utanför leverantörens nätverk och informationssystemen som påverkar dem.*

*Leverantören bör i riskanalysen ta ställning till risker som påverkar säkerhet, tillgänglighet, riktighet eller konfidentialitet i leverantörens nätverk och informationssystem.*

*Incidenter som bör ingå i en riskanalys kan exempelvis vara antagonistiska angrepp, tekniska fel, fel orsakade av människan eller naturpåverkan.*

**5 §**

*Utöver den årliga uppdateringen bör riskanalysen uppdateras dels efter allvarliga incidenter, dels efter stora förändringar av leverantörens nätverk och informationssystem eller stora förändringar i leverantörens organisation. I samband med uppdatering av riskanalysen bör en uppdatering även ske av den åtgärdsplan som ingår i riskanalysen.*

**6 §**

*Exempel på egenskaper och förutsättningar inom OT som kan behöva tas särskild hänsyn till är följande:*

1. *Realtidsfunktionalitet är ofta en förutsättning för tillhandahållande av samhällsviktiga tjänster. Även en mycket kort störning kan få stora konsekvenser.*
2. *En mindre störning i OT kan få följdverkningar och innebära stor påverkan på omkringliggande informationssystem.*
3. *Informationssystem i OT kan vara av äldre snitt och inte avsedda att vara uppkopplade enligt nuvarande användning. Detta kan medföra särskild sårbarhet i leverantörens nätverk och informationssystem.*

## Allmänna råd till 3 kap. om Informationssäkerhetskrav

*I uppfyllnaden av informationssäkerhetskrav bör leverantören ta ställning till de egenskaper och förutsättningar som identifierats vid utförd riskanalys enligt 2 kap. 6 §.*

**1 §**

*I arbetet med att uppfylla informationssäkerhetskrav bör leverantören även ta ställning till vilken typ av övervakning och larmfunktioner som krävs för att åtgärder ska fungera.*

*Systemloggar bör hanteras med hög säkerhet för att undvika att de riskerar att manipuleras. Leverantören bör även införa analysverktyg för att möjliggöra upptäckt av otillåtna aktiviteter, och för att kunna spåra aktiviteter i forensiskt eller problemlösande syfte. Loggning bör ske av olika typer av transaktioner, exempelvis av nätverkstrafik mellan segment, nätverkstrafik externt mot internet, förändringar i konfiguration av nätverkets skalskydd eller tilldelning av administratörsrättigheter. Leverantören bör testa och kalibrera larmfunktioner för att säkerställa att rätt person inom organisationen tillhandahålls relevant information.*

**2 §**

*Processer enligt punkt 2 bör vara dokumenterade för att uppnå tydlighet om vem hos leverantören som ska utföra arbetet, hur det ska utföras, liksom vem som är mottagare av resultatet från processerna.*

**3 §**

*Vid kartläggningen och analysen bör leverantören ta ställning till hur kritiskt informationssystemet är för tillhandahållande av samhällsviktiga tjänster, liksom hur känslig informationen är som hanteras i informationssystemet.*

*Om något av leverantörens informationssystem är externt bör särskild vikt läggas vid hur sådant externt informationssystem är uppkopplat mot leverantörens övriga nätverk och informationssystem.*

*Leverantören bör hantera hårdvaruinventering genom att upprätta en s.k. ”vitlista” med godkänd hårdvara. Nätverket bör övervakas så att leverantören uppmärksammar om en otillåten enhet kopplas upp mot leverantörens IT eller OT.*

*Leverantören bör hantera mjukvaruinventering genom att upprätta en s.k. ”vitlista” med godkänd mjukvara. Mjukvaran bör övervakas så att leverantören uppmärksammar om något otillåtet installeras i leverantörens IT eller OT.*

*Systemförteckningen kan vara manuellt upprättad eller genererad genom övervakningsapplikationer. Om verktyg som skannar leverantörens nätverk och informationssystem används för upprättande av systemförteckningen bör verktyget konfigureras för att möjliggöra underrättelser om nya informationssystem identifieras i samband med skanningsprocessen.*

**4 §**

*Vid segmentering av nätverk bör leverantören ta ställning till vilken typ av information som finns i segmentet, vilka säkerhetsfunktioner som är införda och om segmentet kommunicerar externt.*

*För att minimera användande av administrationsrättigheter bör leverantören dels konfigurera sina behörighetsregler så att en administratör bara använder höjda behörigheter i de fall det är nödvändigt, dels säkerställa att så få personer som möjligt har tillgång till höjd behörighet.*

*När leverantören väljer proportionella autentiseringsmetoder bör leverantören ta ställning till*

1. *vilken behörighetsnivå en användarprofil har,*
2. *i vad mån åtkomst sker på distans eller från leverantörens lokaler samt*
3. *känsligheten i den information som hanteras via inloggningen.*

*Loggning bör ske avseende allt tillträde till den hårdvara och de lokaler vari leverantörens centrala nätverk och informationssystem är beläget.*

**5 §**

*Enheter kan härdas bl.a. genom avstängning av förkonfigurerade tjänster, ändring av lösenord på förinställda användarprofiler och avstängning av schemalagda arbeten.*

**6 §**

*Redundans kan införas på olika tekniska nivåer (t.ex. hårdvara för förvaring, databas, nätverk eller ett helt datacenter), och kan även innebära krav på manuella, analoga arbetssätt.*

## Allmänna råd till 4 kap. om Säkerhetsåtgärder

**1 §**

*För att sänka en risks värde bör åtgärden minska riskens sannolikhet (vara förebyggande) eller minska riskens konsekvens (avse redundans och kontinuitet).*

*Leverantören bör utvärdera planerade säkerhetsåtgärder för att säkerställa att de inte leder till nya risker i leverantörens nätverk och informationssystem.*

**4 §**

*Vid prioritering av säkerhetsåtgärder bör leverantören utvärdera*

1. *säkerhetsåtgärdens ändamål,*
2. *det aktuella informationssystemets kritikalitet för tillhandahållande av samhällsviktiga tjänster enligt den analys som ska göras enligt 3 kap. 3 §, punkt 4, samt*
3. *informationssystemets tekniska förutsättningar.*