**Myndigheten för civilt försvars författningssamling**

Utgivare: Anna Asp
ISSN 3119-2394

**MCFFS 2026:6**
Utkom från trycket den 5 maj 2026

# Myndigheten för civilt försvars föreskrifter om incidentrapportering och informationsskyldighet för väsentliga och viktiga verksamhetsutövare;

beslutade den 28 april 2026.

Myndigheten för civilt försvar föreskriver[1] följande med stöd av 38 § p. 6 och 39 § p. 2–3 cybersäkerhetsförordningen (2025:1507).

## 1 kap. Inledande bestämmelser

### Tillämpningsområde

**1 §** Dessa föreskrifter innehåller bestämmelser om

- rapportering av betydande incidenter enligt 2 kap. 5–8 §§ cybersäkerhetslagen (2025:1506),
- vad som utgör en betydande incident enligt 2 kap. 5 § andra stycket cybersäkerhetslagen, och
- informationsskyldighet vid betydande incidenter och betydande cyberhot enligt 2 kap. 9–10 §§ cybersäkerhetslagen.

Bestämmelser om vad som utgör en betydande incident i 3–4 kap. samt informationsskyldighet vid betydande incidenter och betydande cyberhot i 5 kap. i dessa föreskrifter omfattar inte sektorsverksamhet inom digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster (mellan företag), post- och budtjänster samt rymden.

### Ordförklaringar

**2 §** Uttryck i dessa föreskrifter har samma betydelse som i cybersäkerhetslagen.

[1] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148, i den ursprungliga lydelsen (NIS2-direktivet).

**3 §** I dessa föreskrifter avses med

| | |
|---|---|
| *angreppsindikatorer* | teknisk information som utgör indikatorer på förberedelse till, pågående eller genomfört cyberangrepp, |
| *betydande sårbarhet* | en sårbarhet som har inneburit att en betydande cybersäkerhetsrisk i enlighet med artikel 3 p. 38 i Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828, i den ursprungliga lydelsen (cyberresiliensförordningen), |
| *information i behov av utökat skydd* | information som på grund av externa krav kräver en viss nivå av skydd avseende konfidentialitet, riktighet inklusive autenticitet, eller tillgänglighet alternativt information som verksamhetsutövaren vid värdering bedömer ha behov av motsvarande nivå av skydd, |
| *sektorskritiskt system* | ett system som är nödvändigt för att kunna bedriva intern verksamhet eller tillhandahålla externa tjänster inom sektorsverksamhet, |
| *sektorsverksamhet* | sådan verksamhet som omfattas av cybersäkerhetslagen, |
| *system* | nätverks- och informationssystem enligt 1 kap. 2 § p. 16 cybersäkerhetslagen, |
| *viktig samhällsfunktion* | en samhällsfunktion som är nödvändig för samhällets grundläggande behov, värden eller säkerhet. |

# 2 kap. Rapportering av betydande incidenter

## Hur rapporteringen ska ske

**1 §** När en incident har identifierats som betydande ska uppgifter anges på det sätt och lämnas via de kontaktvägar som har anvisats av Försvarets radioanstalt.

**2 §** Statliga myndigheter som för samma incident redan helt eller delvis uppfyllt rapporteringsplikt enligt förordningen (2022:524) om statliga myndigheters beredskap ska, inom de tidsfrister som anges i cybersäkerhetslagen, komplettera tidigare inlämnade rapporter för att även uppfylla rapporteringsplikten enligt cybersäkerhetslagen.

## Vilka uppgifter ska rapporteras

### Upplysning

**3 §** Upplysning ska lämnas så snart det kan ske, dock senast inom 24 timmar efter att incidenten identifierats som betydande enligt 3–4 kap. Upplysning ska innehålla följande uppgifter

1. verksamhetsutövarens namn, kontaktuppgifter och organisationsnummer,
2. om incidenten är pågående,
3. händelseförlopp samt när och hur incidenten upptäcktes,
4. om incidenten har orsakats av misstänkt avsiktligt skadliga eller misstänkt olagliga handlingar,
5. i det fall incidenten har sitt ursprung hos en leverantör; information om leverantören,
6. påverkan på verksamhetsutövarens sektorsverksamhet,
7. vilka konsekvenser incidenten medför eller riskerar att medföra, och
8. om incidenten har eller riskerar att få gränsöverskridande konsekvenser.

Uppgifterna som lämnas enligt p. 2–8 ska vara baserade på en preliminär bedömning av den betydande incidenten.

### Incidentanmälan

**4 §** Incidentanmälan ska lämnas så snart det kan ske, dock senast 72 timmar efter att verksamhetsutövaren har identifierat incidenten som betydande enligt 3–4 kap.

Incidentanmälan ska innehålla en uppdatering av uppgifter som har lämnats enligt 3 § samt följande uppgifter

1. när incidenten inträffade,
2. när incidenten upphörde eller en uppskattning av hur länge incidenten förväntas pågå,
3. en bedömning om incidentens orsak,

4. påverkan på system,
5. i tillämpliga fall, information om angreppsindikatorer, och
6. i tillämpliga fall, påverkan på information i behov av utökat skydd.

Verksamhetsutövare som tillhandahåller betrodda tjänster ska komma in med information enligt första stycket inom 24 timmar.

**Slutrapport eller lägesrapport**

**5 §** Slutrapport ska lämnas senast en månad efter incidentanmälan eller en månad efter att incidenten har hanterats. Den ska innehålla en uppdatering av uppgifter som har lämnats enligt 3–4 §§ samt följande uppgifter

1. en slutlig bedömning av den betydande incidentens konsekvenser, där bedömningen i tillämpliga fall ska innehålla information om
   a) det uppskattade antalet mottagare av verksamhetsutövarens tjänster som drabbats av incidenten,
   b) berört geografiskt område,
   c) ekonomisk skada,
   d) gränsöverskridande konsekvenser, och
   e) påverkan på viktiga samhällsfunktioner,
2. så långt möjligt en detaljerad beskrivning av incidentens grundorsak,
3. en beskrivning av vilka tekniska och organisatoriska åtgärder som har vidtagits för att hantera incidenten, och, i tillämpliga fall, som har vidtagits eller kommer att vidtas för att
   a) hantera och minimera konsekvenserna av incidenten, och
   b) undvika att liknande incidenter inträffar.

**6 §** Om incidenten fortfarande är pågående efter en månad ska verksamhetsutövaren istället för en slutrapport lämna en lägesrapport. Den ska innehålla följande uppgifter:

1. varför incidenten fortfarande är pågående,
2. en uppskattning av hur länge incidenten förväntas pågå,
3. om incidenten fortfarande påverkar eller riskerar att påverka verksamhetsutövarens sektorsverksamhet, och
4. i tillämpliga fall, information om angreppsindikatorer.

# 3 kap. Generella rapporteringskriterier

## Allvarlig driftstörning för verksamhetsutövaren

**1 §** Med betydande incident som har orsakat allvarlig driftstörning för verksamhetsutövare avses en incident där otillgänglighet eller nedsatt funktionalitet i ett eller flera sektorskritiska system har inneburit att

1. sektorsverksamhet endast har kunnat bedrivas i begränsad utsträckning i mer än 12 timmar,

2. personal har behövt använda alternativa arbetssätt för att bedriva sektorsverksamhet i mer än 48 timmar,
3. information i behov av utökat skydd tillhörande verksamhetsutövaren som behandlas i ett eller flera sektorskritiska system har blivit tillgänglig för obehöriga, förvanskats eller förstörts, eller
4. ett eller flera sektorsspecifika kriterier om allvarlig driftstörning för verksamhetsutövare i kap. 4 uppfylls.

**2 §** Med betydande incident som kan orsaka allvarlig driftstörning för verksamhetsutövaren avses en incident där det inom verksamhetsutövarens system har uppstått

1. ett betydande cyberhot som sannolikt kan orsaka eller bidra till att orsaka konsekvenser enligt 1 §, eller
2. en betydande sårbarhet som möjliggör konsekvenser enligt 1 §.

**Ekonomisk skada för verksamhetsutövaren**

**3 §** Med betydande incident som har orsakat ekonomisk skada för verksamhetsutövaren avses en incident som sammantaget har inneburit en kostnad, enligt 5 §, som överstiger fem procent av den berörda verksamhetsutövarens totala årsomsättning under föregående räkenskapsår.

För verksamhetsutövare inom offentlig förvaltning gäller istället fem procent av verksamhetsutövarens anslag eller totala intäkter under föregående räkenskapsår.

**4 §** Med betydande incident som kan orsaka ekonomiska skada för verksamhetsutövaren avses en incident där det inom verksamhetsutövarens system har uppstått:

1. ett betydande cyberhot som sannolikt kan orsaka eller bidra till att orsaka konsekvenser enligt 3 §, eller
2. en betydande sårbarhet som möjliggör konsekvenser enligt 3 §.

**5 §** Verksamhetsutövaren ska vid bedömning av den ekonomiska skadan beakta följande direkta och indirekta kostnader

1. kostnader för återställning av information som har förlorats eller förvanskats,
2. kostnader för utbyte eller återställning av system,
3. externa rådgivningskostnader för incidenthanteringstjänster, juridisk rådgivning, it-forensiska tjänster och saneringstjänster,
4. tillkommande personalkostnader,
5. kostnader på grund av att avtalsförpliktelser inte har fullgjorts, och
6. uteblivna intäkter till följd av oplanerade produktionsbortfall.

Om den ekonomiska skadan vid tidpunkten för rapportering inte kan fastställas ska verksamhetsutövaren uppskatta dessa belopp.

**Betydande skada för andra fysiska eller juridiska personer**

**6 §** Med betydande incident som har påverkat andra fysiska eller juridiska personer genom att vålla betydande skada avses en incident som

1. har inneburit att information i behov av utökat skydd som verksamhetsutövaren behandlar för annan juridisk person eller minst 500 fysiska personer har blivit tillgänglig för obehöriga, förvanskats eller förstörts,
2. har inneburit en föroreningsskada enligt 10 kap. 1 § miljöbalken, eller
3. verksamhetsutövaren har fått kännedom om att den inneburit
    a) att en juridisk person som tillhandahåller en viktig samhällsfunktion har gått in i stabsläge eller på annat sätt har eskalerat eller ändrat sin organisation på grund av incidenten,
    b) allvarlig personskada eller sjukdom, eller
    c) dödsfall.

**7 §** Med betydande incident som kan påverka andra fysiska eller juridiska personer genom att vålla betydande skada avses en incident där det inom verksamhetsutövarens system har uppstått

1. ett betydande cyberhot som sannolikt kan orsaka eller bidra till att orsaka konsekvenser enligt 6 §, eller
2. en betydande sårbarhet som möjliggör konsekvenser enligt 6 §.

**Återkommande incidenter**

**8 §** Incidenter som var för sig inte anses som en betydande incident ska anses vara en betydande incident om de

1. har inträffat minst två gånger inom sex månader,
2. bedöms ha samma grundorsak, och
3. sammantaget medfört ekonomisk skada för verksamhetsutövaren enligt 3 §.

# 4 kap. Sektorsspecifika rapporteringskriterier om allvarlig driftstörning för verksamhetsutövaren

## Offentlig förvaltning

**1 §** Med betydande incident som har orsakat allvarlig driftstörning för verksamhetsutövare avses en incident där

1. otillgänglighet eller nedsatt funktionalitet i ett eller flera sektorskritiska system har inneburit att
    a) sektorsverksamhet endast har kunnat bedrivas i begränsad utsträckning i mer än fyra timmar,

b) personal har behövt använda alternativa arbetssätt för att bedriva sektorsverksamhet i mer än tolv timmar, eller

2. ett eller flera sektorsspecifika kriterier om allvarlig driftstörning för verksamhetsutövare enligt 2–9 §§ uppfylls.

# Energi

### Elektricitet och fjärrvärme eller fjärrkyla

**2 §** Med betydande incident som har orsakat allvarlig driftstörning för verksamhetsutövare avses en incident där

1. otillgänglighet eller nedsatt funktionalitet i ett eller flera sektorskritiska system har inneburit att
   a) externa tjänster inom sektorsverksamhet inte har kunnat tillhandahållas till minst 2 000 slutanvändare eller 50 procent av slutanvändarna i mer än två timmar,
   b) personal har behövt använda alternativa arbetssätt för att bedriva sektorsverksamhet i mer än sex timmar, eller
2. system för styrning och övervakning av transmissionsnät, regionnät eller elproduktion inte har kunnat användas på avsett sätt i mer än en timme.

### Gas och vätgas

**3 §** Med betydande incident som har orsakat allvarlig driftstörning för verksamhetsutövare avses en incident där otillgänglighet eller nedsatt funktionalitet i ett eller flera sektorskritiska system har inneburit att

1. styrning och övervakning inom ramen för systemansvarstjänst inte har kunnat genomföras på avsett sätt i mer än en timme, eller
2. personal har behövt använda alternativa arbetssätt för att bedriva sektorsverksamhet i mer än sex timmar.

### Olja

**4 §** Med betydande incident som har orsakat allvarlig driftstörning för verksamhetsutövare avses en incident där otillgänglighet eller nedsatt funktionalitet i ett eller flera sektorskritiska system har inneburit att

1. styrning och övervakning av ledning, överföring och distributionsnätverk, anläggningar för oljeproduktion, raffinaderier, bearbetningsanläggningar eller anläggningar för lagring och överföring av olja inte har kunnat genomföras på avsett sätt i mer än två timmar, eller
2. personal har behövt använda alternativa arbetssätt för att bedriva sektorsverksamhet i mer än sex timmar.

## Transporter

### Sjöfart, lufttransport och vägtransport

**5 §** Med betydande incident som har orsakat allvarlig driftstörning för verksamhetsutövare avses en incident där otillgänglighet eller nedsatt funktionalitet i ett eller flera sektorskritiska system har inneburit att

1. sektorsverksamhet endast har kunnat bedrivas i begränsad utsträckning i mer än en timme,
2. externa tjänster inom sektorsverksamhet inte har kunnat tillhandahållas i mer än en timme och kan antas ha påverkat minst 1 000 användare eller ett sammanhängande geografiskt område om minst 10 000 km2, eller
3. personal har behövt använda alternativa arbetssätt för att bedriva sektorsverksamhet i mer än sex timmar.

### Järnvägstransport och kollektivtrafik

**6 §** Med betydande incident som har orsakat allvarlig driftstörning för verksamhetsutövare avses en incident där otillgänglighet eller nedsatt funktionalitet i ett eller flera sektorskritiska system har inneburit att

1. sektorsverksamhet endast kunnat bedrivas i begränsad utsträckning och kan antas ha påverkat mer än fem procent av planerade avgångar under ett trafikdygn per trafikslag, eller
2. personal har behövt använda alternativa arbetssätt för att bedriva sektorsverksamhet i mer än sex timmar.

## Hälso- och sjukvård

### Vårdgivare

**7 §** Med betydande incident som har orsakat allvarlig driftstörning för verksamhetsutövare avses en incident där

1. otillgänglighet eller nedsatt funktionalitet i ett eller flera sektorskritiska system har inneburit att
    a) en eller flera delar av verksamhetsutövarens sektorsverksamhet endast har kunnat bedrivas i begränsad utsträckning i mer än en timme,
    b) personal har behövt använda alternativa arbetssätt för att bedriva sektorsverksamhet i mer än sex timmar,
2. anmälningsskyldighet inträffat enligt 3 kap. 5 § första stycket patientsäkerhetslagen (2010:659), eller
3. ambulans och ambulanssjukvård som avses i 7 kap. 6 § hälso- och sjukvårdslagen (2017:30) inte har kunnat tillhandahållas.

## Dricksvatten

**8 §** Med betydande incident som har orsakat allvarlig driftstörning för verksamhetsutövare avses en incident där

1. sektorskritiska system har varit otillgängliga eller har haft nedsatt funktionalitet i mer än fyra timmar, eller
2. personal har behövt använda alternativa arbetssätt för att bedriva sektorsverksamhet i mer än åtta timmar.

## Avloppsvatten

**9 §** Med betydande incident som har orsakat allvarlig driftstörning för verksamhetsutövare avses en incident där

1. sektorskritiska system har varit otillgängliga eller haft nedsatt funktionalitet i mer än fyra timmar, eller
2. personal har behövt använda alternativa arbetssätt för att bedriva sektorsverksamhet i mer än åtta timmar.

# 5 kap. Informationsskyldighet vid betydande incidenter och betydande cyberhot

**1 §** Verksamhetsutövare ska, så snart det kan ske, informera mottagare om en betydande incident som har påverkat en eller flera externa tjänster som tillhandahålls till mottagare och ska då lämna följande uppgifter

1. vad den betydande incidenten består i,
2. i tillämpliga fall, vilka åtgärder som mottagarna av verksamhetsutövarens tjänster behöver vidta för att begränsa den betydande incidentens konsekvenser, och
3. i tillämpliga fall, vad konsekvenserna kan bli om mottagarna inte vidtar åtgärder enligt p. 2.

Information enligt första stycket ska inte lämnas om verksamhetsutövaren bedömer att sådan information kan försvåra hantering av den betydande incidenten eller förvärra dess konsekvenser.

**2 §** Verksamhetsutövare ska, så snart det kan ske, informera mottagare om ett betydande cyberhot som kan påverka system som tillhandahålls till mottagare och som inte utgör en betydande incident. Verksamhetsutövaren ska lämna följande uppgifter

1. vad cyberhotet består i,
2. i tillämpliga fall, vilka åtgärder mottagarna behöver vidta för att minimera risken för att cyberhotet resulterar i en incident, och
3. i tillämpliga fall, vad konsekvenserna kan bli om mottagarna inte vidtar dessa rekommenderade åtgärder.

Information enligt första stycket p. 1 ska inte lämnas om verksamhetsutövaren bedömer det som olämpligt med hänsyn till att det kan öka risken för att en incident uppstår.

---

Denna författning träder i kraft 1 juli 2026.

Myndigheten för civilt försvar

ANNA STARBRINK

Josefin Andersson
Avdelningen för cybersäkerhet och samhällsviktiga kommunikationer



**Beställningsadress:**
Norstedts Juridik, 106 47 Stockholm
Telefon: 08-657 95 00
E-post: order@forlagssystem.se
Webbadress: www.nj.se/offentligapublikationer
Beställningsnummer: 19126-06