



För rapportering av betydande incidenter enligt cybersäkerhetslagen (2025:1506) – Upplysning

Detta formulär används för Upplysning enligt cybersäkerhetslagen.
Verksamhetsutövare ska inkomma med en upplysning så snart som möjligt
men senast 24 timmar efter att ha fått kännedom om incidenten.

Sekretessbedömning och behandling av personuppgifter

Myndigheten för civilt försvar uppmanar organisationens rapportör att återvända till denna sida efter att formulärets frågor (nedan) har fyllts i fullständigt. När formuläret är fullständigt ifyllt uppmanar Myndigheten för civilt försvar organisationen och den rapportör att se över (och vid behov gå tillbaka och justera) uppgifterna en sista gång för att kontrollera om:

- Information som omfattas av sekretess för skydd av Sveriges säkerhet har inkluderats i något fritextfält. Om sådan information har inkluderats ska antingen rapporteringen ske enligt särskild ordning eller fritextfälten rensas från sådan information.
- Personuppgifter som inte är nödvändiga att förmedla till Myndigheten för civilt försvar som en del i det som ska rapporteras har inkluderats i något fritextfält. Om sådan information har inkluderats ska fritextfälten rensas från sådan information.

OBS! Detta är en interaktiv pdf där vissa val inte kan kombineras. Var noga med att spara text som ni skrivit in i fritextfälten i en annan fil innan ni klickar på Nej- eller Okänt-svar, eftersom den inskrivna texten annars kommer att gå förlorad.



Bedömer organisationen att den information som har lämnats i formuläret omfattas av sekretess?

Ja, de lämnade uppgifterna omfattas av...

OSL 15 kap. 1 § (Utrikessekretess)

OSL 15 kap. 2 § (Försvarssekretess)

OSL 18 kap. 8 § (Säkerhets- eller bevakningsåtgärd)

OSL 18 kap. 13 § (Risk- och sårbarhetsanalyser, m.m.)

OSL 19 kap. 1 § (Affärs- och driftförhållanden)

OSL 21 kap. 7 § (Behandling i strid med dataskyddsregleringen)

Annan sekretessgrund

Motivera vald(a) sekretessgrund(er)

Fyll i vilken information ni anser omfattas av sekretess samt motivering till vald sekretessgrund här.

Nej, uppgifterna omfattas inte
av sekretess.

Kan inte bedöma



1. Ange kontaktinformation för incidenten

Här uppger ni information om den egna organisationen och kontaktuppgifter till rapportör.

Verksamhetsutövarens namn

Organisationsnummer

Myndighetens ärendenummer

Ärendenummer från Myndigheten för civilt försvar (ärendenummer lämnas i samband med notifiering under dagtid) eller tidpunkt för notifiering.

"Myndighetens ärendenummer" anges för verksamhetsutövare som omfattas av Cybersäkerhetslagen och samtidigt är statlig myndighet.

1.1 Sektor som påverkats av incidenten

Uppge den sektor eller de sektorer enligt bilaga 1 eller 2 i NIS2-direktivet som påverkats av incidenten.

Energi

Transporter

Bankverksamhet

Finansmarknadsinfrastruktur

Hälso- och sjukvård

Dricksvatten

Avloppsvatten

Digital infrastruktur

Förvaltning av IKT-tjänster
(mellan företag)

Offentlig förvaltning

Rymden

Post- och budtjänster

Avfallshantering

Tillverkning, produktion och
distribution av kemikalier

Produktion, bearbetning och
distribution av livsmedel

Tillverkning

Digitala leverantörer

Forskning

Kontaktuppgifter till er kontaktperson eller kontaktfunktion för incidenten.

Namn

Mejladress

Telefonnummer



2. Vad är skälet till att rapporteringsplikt har uppstått?

Beskriv varför incidenten bedöms vara rapporteringspliktig enligt cybersäkerhetslagen.

3. Ange följande tidpunkter

Ange datum (**K2**) och säkert (**K3**) eller osäkert datum (**K4**), samt klockslag (**K5**) och säkert (**K6**) eller osäkert klockslag (**K7**). Välj Okänt klockslag (**K8**) om klockslaget är helt okänt. Om varken datumet eller klockslaget är känt anges svarsalternativet Okänt på den raden (**K9**).

Tidpunkt	K2	K3	K4	K5	K6	K7	K8	K9
----------	----	----	----	----	----	----	----	----

När inträffade
incidenten?

När blev ni
uppmärksammade
på incidenten?

När inleddes hante-
ringen av incidenten?

När upphörde
incidenten?

När återgick drabbade
informationssystem
till normaldrift?



4. Vad har hänt?

Beskriv kortfattat vad som har inträffat och vilka konsekvenser incidenten har eller riskerar att medföra. Verksamhetsutövare som rapporterar enligt cybersäkerhetslagen uppmanas även redogöra ifall incidenten har eller kan resultera i gränsöverskridande konsekvenser.

5. Hur upptäcktes problemet?



6. Finns det en brottsmisstanke?

Ja

Nej

Okänt / Kan inte bedöma

6.1 Har ni polisanmält incidenten?

Ja

Nej, men vi kommer att göra det

Nej, men vi utreder behovet av det

Nej, det behövs inte

Okänt / Kan inte bedöma

Ja, referensnummer till polisanmälan är:
