



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

Sekretessbedömning och behandling av personuppgifter

Myndigheten för civilt försvar uppmanar organisationens rapporteringsansvarige 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 rapporteringsansvarige 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 (se bilaga för mer information) 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.

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 1 5kap. 1 § (Utrikessekretess)

OSL 15 kap. 2 § (Förvarssekretess)

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

Kan ej bedöma

1. Ange kontaktinformation för incidenten

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

Verksamhetsutövarens namn

Organisationsnummer

Myndighetens ärendenummer

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

Verksamhetsutövare som omfattas av Cybersäkerhetslagen och som inte är statliga myndigheter behöver inte uppges någon information under "Myndighetens ärendenummer".

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

Hälsa- och sjukvård

Dricksvatten

Avloppsvatten

Digital infrastruktur

Förvaltning av IKT-tjänster
(mellan företag)

Offentlig förvaltning

Rymden

Post- och budtjänster



1.1 Sektor som påverkats av incidenten

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. Har incidenten inträffat i en tjänst som tillhandahålls av en eller flera externa aktörer?

Ja, uppgifterna om tjänsten och aktören/aktörerna är:

Externa aktörens namn

Organisationsnummer

Tjänstens namn

Beskrivning av tjänsten och vad er organisation använder den till

Nej

Okänt



4. 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 hanteringen
av incidenten?

När upphörde
incidenten?

När återgick drabbade
informationssystem
till normaldrift?

5. Vad är det för typ av incident?

Incidenter kan antingen ske i miljön runtomkring ett informationssystem ("incident i kringmiljö"), eller i informationssystem ("incident i informationssystem"). Exempel på incidenter i kringmiljön är att en el- eller fiberkabel har kapats. Exempel på incidenter i informationssystem är att skadlig kod har installerats (en "installationsincident" nedan). Kryssa därför antingen i en incidenttyp i 5.1. eller vad det var för slags informationssystem som incidenten skedde i genom att välja en typ av system i 5.2. och sen incidenttypen i 5.3.

5.1 Om det är en incident i kringmiljö – vad för typ av incident är det?

Incident i värmeållning eller kylning	Incident i klimathållning
Incident i lokal	Incident i korrekt tid-, takt eller positionsförsörjning
Incident i energiförsörjning	Incident i förbindelse
Övrig incident i kringmiljö	Okänd incident i kringmiljö

5.2 Om det är en incident i ett informationssystem – vad för typ av informationssystem är det?

Administrativt system (exempelvis kontorslösningar)	System för processtyrning eller kontroll (exempelvis fastighetsautomations- system, MES- och logistiksystem)
Informationssystem dedikerat för kommunikation (exempelvis DNS, billing, trafikflödessystem)	System för säkerhetslösningar (exempelvis behörighetssystem, larm, lås, övervakning)
Övrigt informationssystem	Okänt informationssystem

5.3 Om det är en incident i ett informationssystem – vad för typ av incident är det?

Konfigurationsincident – en incident som har uppstått genom att informations- systemet har felkonfigurerats	Förlustincident – en incident som har uppstått genom att mjukvara eller hårdvara har tagits bort/raderats/slutat fungera/förstörts
Installationsincident – en incident där ett fel har uppstått genom att mjukvara eller hårdvara har tillförts till/installerats i informationssystemet	Kompatibilitetsincident – en incident där ett fel har uppstått i samspillet mellan mjukvaror, eller mellan mjukvara och hårdvara, eller mellan hårdvaror i informationssystemet
Överbelastningsincident – en incident där ett fel har uppstått genom att informationssystem har "stressats" så mycket att det inte längre fungerar som det ska	Informationssäkerhetsincident – en incident där information i informa- tionssystemet, snarare än informations- system i sig, har påverkats
Övrig incident i informationssystem	Okänd incident i informationssystem

5.4 Om det är en annan eller en okänd typ av incident, kryssa här.

Övrig typ av incident	Okänd typ av incident
-----------------------	-----------------------



6. Vilka konsekvenser har incidenten haft på informationssystem?

Ange minst ett svar per kolumn.

Konfidentialitet	Riktighet	Tillgänglighet
Behöriga användare har fått för höga behörigheter till informationssystem	Konfigurationer har lagts till i informationssystem	Behöriga användare har fått för låga behörigheter till informationssystem
Tillgång för obehöriga kan upprättas till informationssystem	Konfigurationer har ändrats i informationssystem	Tillgång för behöriga användare kan inte upprättas till informationssystem
Obehöriga har tillgång till informationssystem	Konfigurationer har tagits bort i informationssystem	Avbrott har uppstått i behöriga användares befintliga tillgång till informationssystem
Information kan tas emot från obehöriga användare i informationssystem	Konfigurationer i informationssystem har gjorts otillförlitliga	Information kan inte tas emot från behöriga användare i informationssystem
Information från obehöriga användare kan behandlas i informationssystem	Informationssystemet utför inte uppgifter det ska utföra	Information från behöriga användare kan inte behandlas i informationssystem
Information från obehöriga användare kan skickas i informationssystem	Informationssystemet utför uppgifter det inte ska utföra	Information från behöriga användare kan inte skickas i informationssystem
Uppgifter utförs på obehörigas begäran i informationssystem	Informationssystemet utför inte uppgifter det är konfigurerat att utföra	Uppgifter utförs inte på behöriga användares begäran i informationssystem
Informationssystemet kan konfigureras av obehöriga användare	Informationssystemet utför uppgifter det inte är konfigurerat att utföra	Informationssystemet kan inte konfigureras av behöriga användare
Konfidentialiteten har påverkats negativt på annat sätt	Riktigheten har påverkats negativt på annat sätt	Tillgängligheten har påverkats negativt på annat sätt
Konfidentialiteten har inte påverkats negativt	Riktigheten har inte påverkats negativt	Tillgängligheten har inte påverkats negativt
Det är okänt om konfidentialiteten har påverkats negativt	Det är okänt om riktigheten har påverkats negativt	Det är okänt om tillgängligheten har påverkats negativt



7. Vilka konsekvenser har incidenten haft på information?

7.1 Vad för typ av information, om någon, har påverkats av incidenten?

Information som är verksamhetskritisk	Information som är känslig	Information som omfattas av sekretess
Personuppgifter	Information som är viktig för användare av organisationens tjänst	
Annan information	Information har inte påverkats	Det är okänt om information har påverkats

7.2 Vad för typ av påverkan har incidenten haft på information?

Ange minst ett svar per kolumn.

Konfidentialitet	Riktighet	Tillgänglighet
Behöriga användare har fått för höga behörigheter till informationstillgångar	Information har lagts till i informationstillgångar	Behöriga användare har fått för låga behörigheter till informationstillgångar
Tillgång för obehöriga kan upprättas till informationstillgångar	Information har ändrats i informationstillgångar	Tillgång för behöriga användare kan inte upprättas till informationstillgångar
Obehöriga har tillgång till informationstillgångar	Information har tagits bort i informations-tillgångar	Avbrott har uppstått i behöriga användares befintliga tillgång till informationstillgångar
Konfidentialiteten har påverkats negativt på annat sätt	Information har gjorts otillförlitlig i informationstillgångar	Tillgängligheten har påverkats negativt på annat sätt
Konfidentialiteten har inte påverkats negativt	Riktigheten har påverkats negativt på annat sätt	Tillgängligheten har inte påverkats negativt
Det är okänt om konfidentialiteten har påverkats negativt	Riktigheten har inte påverkats negativt	Det är okänt om tillgängligheten har påverkats negativt
	Det är okänt om riktigheten har påverkats negativt	



8. Vilka konsekvenser har incidenten haft på organisationens förmåga att bedriva sin verksamhet?

9. Påverkar incidenten en tjänst som ni tillhandahåller till externa aktörer?

Tjänstens namn

Beskrivning av tjänsten och vad externa aktörer använder den till

Ange vilka slags aktörer som använder tjänsten

Allmänheten	Företag	Kommuner	
Myndigheter	Regioner	Andra	Okänt
Nej, incidenten påverkar inte en sådan tjänst		Okänt om incidenten påverkar en sådan tjänst	

10. Vad bedömer ni att incidenten orsakades av?

Incidenter som att döma av hur de beskrivs (i val av orsak eller i fritext) kan antas ha sin grund i en brottslig handling kommer att vidarebefordras till Polismyndigheten där en polisanmälan kan komma att upprättas. Läs mer på mcf.se.

Mänsklig handling i antagonistiskt syfte	Mänsklig handling utan antagonistiskt syfte	Systemfel
Naturhändelse	Övrig orsak	Okänd orsak



11. Vem eller vad var först med att uppmärksamma er organisation om incidenten?

Er organisations	Annan myndighets	Annan organisations	Andra	Okänt
Personal	Personal	Personal	Privat-personer	Okänt
Tekniska system	Tekniska system	Tekniska system	Media	
Annat	Annat	Annat	Annat	

OBS! Om incidenten kan misstänkas ha grund i en brottslig gärning ska den polisanmälas.

12. Har ni polisanmält incidenten?

Incidenter som att döma av hur de beskrivs (i val av orsak eller i fritext) kan antas ha sin grund i en brottslig handling kommer att vidarebefordras till Polismyndigheten där en polisanmälan kan komma att upprättas. Läs mer på mcf.se.

Ja, referensnumret till polisanmälan är:

Nej, men vi kommer att göra det	Nej, men vi utreder behovet av det	Nej, det behövs inte	Okänt
---------------------------------	------------------------------------	----------------------	-------



13. Redogör för incidenten, dess konsekvens(er) och (grund)orsak(er), hur den upptäcktes samt vad ni gör för att hantera incidenten och dess konsekvenser

Beskriv även om incidenten har eller kunde få gränsöverskridande konsekvenser.