Upplysning

Upplysningen är det första av tre rapporteringsskeden. Upplysningen ska enligt MCFFS (2026:8) om incidentrapportering och informationsskyldighet för väsentliga och viktiga verksamhetsutövare respektive enligt Kommissionens genomförande-förordning (EU) 2024/2690 samt enligt cybersäkerhetslagen (i väntan på PTS kommande föreskrifter om vad som utgör en betydande incident och om informationsplikt enligt cybersäkerhetslagen) rapporteras in inom 24 timmar efter det att verksamhetsutövaren har konstaterat att en inträffad händelse omfattas av rapporteringsplikt. Upplysning ska enligt MCFFS (2026:7) om rapportering av it-incidenter för statliga myndigheter rapporteras in inom 6 timmar efter det att den statliga myndigheten har konstaterat att en inträffad händelse omfattas av rapporteringsplikt.

Sekretessbedömning och behandling av personuppgifter

NCSC uppmanar organisationens rapportör att återvända till denna sida efter att formulärets frågor (nedan) har fyllts i fullständigt. När formuläret är fullständigt ifyllt uppmanar NCSC 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 NCSC 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.

Rättslig grund

Ange den eller de rättsliga grunderna för varför rapporteringsplikt har uppstått. Inlämnade incidentrapporter tas emot av NCSC och skickas till berörda tillsynsmyndigheter beroende på vilken sektor som berörs. Vilken tillsynsmyndighet som ansvarar för respektive sektor kan du hitta i bilaga 3 i vägledningen för incidentrapportering och informationsskyldighet.

Vad är den rättsliga grunden till att rapporteringsplikt har uppstått?
☐ Krav på rapportering enligt MCFFS (2026:8) om incidentrapportering och informationsskyldighet för väsentliga och viktiga verksamhetsutövare
☐ Krav på rapportering enligt MCFFS (2026:7) om rapportering av it-incidenter för statliga myndigheter
☐ Krav på rapportering enligt Kommissionens genomförandeförordning (EU) 2024/2690
☐ Krav på rapportering enligt cybersäkerhetslagen (för de som ska rapportera enligt PTS kommande föreskrifter om vad som utgör en betydande incident och om informationsplikt enligt cybersäkerhetslagen)

Rapporteringsplikt enligt cybersäkerhetslagen MCFFS (2026:8)
Rapporteringplikt uppstår när en incident har betydande konsekvenser. Det finns fyra olika typer av betydande konsekvenser:

- Allvarlig driftstörning (se avsnitt 3.1.1 i vägledningen om incidentrapportering och informationsskyldighet).
- Ekonomisk skada (se avsnitt 3.1.2 i vägledningen om incidentrapportering och informationsskyldighet
- Betydande skada för andra fysiska eller juridiska personer (se avsnitt 3.1.3 vägledningen om incidentrapportering och informationsskyldighet).
- Återkommande incident (se avsnitt 3.1.5 i vägledningen om incidentrapportering och informationsskyldighet).

Enligt definitionen gäller det också att incidenter som kan resultera i sådana konsekvenser också kan vara betydande. Det kan du läsa mer om i vägledningen om incidentrapportering och informationsskyldighet avsnitt 3.1.4.

Vad är det för händelse som har inträffat och som är rapporteringspliktig enligt MCFFS (2026:8) om incidentrapportering och informationsskyldighet för väsentliga och viktiga verksamhetsutövare?

Det har inträffat en händelse som resulterat i…
☐ Allvarlig driftstörning för verksamhetsutövare
☐ Ekonomisk skada för verksamhetsutövare
☐ Betydande skada för andra fysiska eller juridiska personer
☐ Återkommande incident

Det har uppstått ett betydande cyberhot som kommer att resultera i…
☐ En allvarlig driftstörning för verksamhetsutövare
☐ Ekonomisk skada för verksamhetsutövare
☐ Betydande skada för andra fysiska eller juridiska personer

Det har uppstått en betydande sårbarhet som kan resultera i…
☐ En allvarlig driftstörning för verksamhetsutövare
☐ Ekonomisk skada för verksamhetsutövare
☐ Betydande skada för andra fysiska eller juridiska personer

Ange vilken paragraf och punkt enligt MCFFS (2026:8)

Rapporteringsplikt enligt beredskapsförordningen MCFSS (2026:7)
Statliga myndigheter ska rapportera it-incidenter som inträffat i den rapporterande myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för. För mer om rapportering enligt beredskapsförordningen, se vägledningen om incidentrapportering och informationsskyldighet avsnitt 4.1.

Vad är det för händelse som har inträffat och som är rapporteringspliktig enligt MCFFS (2026:7) om rapportering av it-incidenter för statliga myndigheter?

Det har inträffat en it-incident som …
☐ Negativt har påverkat säkerheten hos den information som har bedömts ha ett behov av utökat skydd
☐ Har inneburit att informationssystem som behandlar information som har bedömts ha behov av utökat skydd inte har kunnat upprätthålla avsedd funktionalitet
☐ Negativt har påverkat myndighetens förmåga att utföra sitt uppdrag
☐ I övrigt allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller i tjänster som myndigheten tillhandahåller åt en annan organisation

Rapporteringsplikt enligt genomförandeförordningen (EU) 2024/2690
Bestämmelser om vad som utgör en betydande incident för verksamhetsutövare inom sektorerna digitala leverantörer, förvaltning av IKT-tjänster (mellan företag) samt digital infrastruktur, exklusive tillhandahållare av allmänna elektroniska kommunikationsnät respektive allmänt tillgängliga elektroniska kommunikationstjänster, återfinns i EU-kommissionens genomförandeförordning. För mer information, besök PTS webbplats.

Vad är det för händelse som har inträffat och som är rapporteringspliktig enligt Kommissionens genomförandeförordning (EU) 2024/2690?

Det har inträffat en incident som har resulterat i…
☐ En allvarlig driftstörning för verksamhetsutövare
☐ Ekonomisk skada för verksamhetsutövare
☐ Betydande skada för andra fysiska eller juridiska personer
☐ Återkommande incident

Det har inträffat en incident som kan resultera i…
☐ Allvarlig driftstörning för verksamhetsutövare
☐ Ekonomisk skada för verksamhetsutövare
☐ Betydande skada för andra fysiska eller juridiska personer

Ange vilken paragraf och punkt i EU-kommissionens genomförandeförordning 2024/2690 som föranleder rapporteringsplikten

Annan rapporteringsplikt enligt cybersäkerhetslagen

De verksamhetsutövare som varken omfattas av MCFFS (2026:8) eller genomförandeförordningen (EU) 2024/2690 rapporterar betydande incidenter enligt cybersäkerhetslagens övergripande bestämmelser i avvaktan på föreskrifter från PTS. Detta gäller post- och budtjänster, rymden samt tillhandahållare av allmänna elektroniska kommunikationsnät och tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster inom sektorn digital infrastruktur.

Vad är det för händelse som har inträffat och som är rapporteringspliktig enligt cybersäkerhetslagen?

Det har inträffat en incident som har resulterat i…
☐ En allvarlig driftstörning för verksamhetsutövare
☐ Ekonomisk skada för verksamhetsutövare
☐ Betydande skada för andra fysiska eller juridiska personer

Det har inträffat en incident som kan resultera i…
☐ Allvarlig driftstörning för verksamhetsutövare
☐ Ekonomisk skada för verksamhetsutövare
☐ Betydande skada för andra fysiska eller juridiska personer

Information om rapportören

Uppgifter om rapportör och organisation

Ange ert svenska organisationsnummer i format nnnnnn-nnnn. För verksamhetsutövare som inte har något svenskt organisationsnummer ska det ska det utländska organisationsnumret för verksamhetsutövarens huvudsäte anges.

Verksamhetsutövaren	
Organisationsnamn	Organisationsnummer*
Kontaktperson (förnamn och efternamn)	
E-postadress	Telefonnummer

Information om leverantör vid leveranskedjeincident

Incident hos leverantör

Ange om incidenten har inträffat hos en leverantör eller underleverantör till er. En leverantör är en organisation som levererar, det vill säga producerar eller transporterar, en digital produkt. Om incidenten har inträffat hos er leverantör, ska ni ange leverantörens namn, leverantörens organisationsnummer och tjänstens namn samt beskriva tjänsten.

Om det inte är möjligt att avgöra om incidenten har sitt ursprung hos en leverantör, välj då ”Okänt”. Om det senare bedöms att incidenten haft sitt ursprung hos en leverantör, ska ni uppdatera informationen.

Leverantörens tjänst

Beskriv tjänsten som leverantören tillhandahåller och som har påverkats av incidenten.

Är organisationens incident ett resultat av en incident som har inträffat hos en leverantör?		
☐ Ja	☐ Nej	☐ Okänt

Ange information om leverantören	
Ange leverantörens organisationsnamn	Organisationsnummer
Ange tjänstens namn	
Beskriv tjänsten	

Incidentens händelseförlopp och upptäckt

Händelseförlopp och hantering

Händelseförlopp avser vad som inträffat hos er organisation fram till rapporteringstillfället. Hantering avser de åtgärder och åtaganden ni genomfört för att påverka och begränsa incidenten.

Beskriv incidentens händelseförlopp och vad ni har gjort för att hantera incidenten

Pågående incident

Incidenten anses vara pågående tills dess verksamhetsutövaren kan återgå till normaldrift eller tills dess verksamhetsutövaren bedömer att hanteringen av incidenten är avslutad.

Är incidenten pågående?	
☐ Ja	☐ Nej

Tidpunkt för upptäckt

Uppge när incidenten upptäcktes hos er organisation. Om ni tidigare uppgett att incidenten uppstått hos en leverantör, uppge också när leverantören upptäckte incidenten. Ange exakt tidpunkt för datum och klockslag om den är känd, annars avrunda eller ange intervall. Om det inte går att avgöra, välj då ”Okänt datum” respektive ”Okänt klockslag”.

Ange viktiga tidpunkter i händelseförloppet

När uppmärksammades incidenten hos er organisation?			
Okänt datum ☐	Datum	Okänt klockslag ☐	Klockslag

När uppmärksammades incidenten hos er leverantör?			
Okänt datum ☐	Datum	Okänt klockslag ☐	Klockslag

Hur uppmärksammades er organisation på incidenten?
☐ Organisationens egna personal upptäckte den
☐ Organisationens tekniska detekteringssystem upptäckte incidenten
☐ Organisationen upptäckte incidenten på annat sätt
☐ Det nationella cybersäkerhetscentret uppmärksammade oss på incidenten
☐ En myndighet uppmärksammade oss på incidenten
☐ En av organisationens leverantörer uppmärksammade oss på incidenten
☐ Användare av en av organisationens tjänster uppmärksammade oss på incidenten
☐ Media uppmärksammade oss på incidenten
☐ Vi blev uppmärksammade på annat sätt

Avsiktlig skadlig eller olaglig handling
Om incidenten bedöms orsakats av avsiktlig skadlig eller olaglig handling, ska ni motivera vad denna bedömning grundar sig på.

Bedömer ni att incidenten har orsakats av en avsiktligt skadlig eller olaglig handling?	
☐ Ja	☐ Nej

Beskriv varför ni bedömer att incidenten orsakades av en avsiktligt skadlig eller olaglig handling

Sektorsverksamhet hos organisationen som har påverkats av incidenten

Sektor och sektorsverksamhet
Uppge endast sektor och sektorsverksamhet som ni själva bedriver och som har påverkats av incidenten. Välj först sektor och sedan sektorsverksamhet. Med sektorsverksamhet avses sådan verksamhet som omfattas av cybersäkerhetslagen.

Information om sektorsverksamhet
Sektorsverksamhet är sådan verksamhet som er organisation bedriver i enlighet med cybersäkerhetslagen. För mer information se NIS2-direktivets bilaga I och II.

Erbjudna tjänster
Om incidenten är rapporteringspliktig enligt EU-kommissionens genomförande-förordning, ska ”Erbjudna tjänster” rapporteras istället för Sektorsverksamhet.
För mer vägledning, se PTS webbplats.

Ange de sektorer som er organisation tillhör och de sektorsverksamheter som ni bedriver som har påverkats av incidenten	
Sektor	Sektorsverksamhet

Sektorsverksamheterna som påverkats av incidenten

Beskriv hur incidenten påverkat den eller de sektorsverksamheter som er organisation bedriver. Det är endast sektorsverksamhet som påverkats av incidenten som behöver beskrivas.

Beskriv hur de ovan angivna sektorsverksamheterna har påverkats av incidenten

Incidentens gränsöverskridande konsekvenser

Konsekvenser utanför Sverige

Verksamhetsutövaren ska lämna information om incidenten påverkat de sektorsverksamheter eller tjänster som levereras utanför Sverige i andra EU/EES-medlemsstater eller övriga stater. Med att erbjuda tjänster menas att aktivt rikta sig till marknaden utanför Sverige. Om konsekvenser uppstått utanför Sverige, ange ”Ja” och ange i vilka länder det gäller samt beskriv hur dessa yttrat sig.

Har incidenten fått konsekvenser utanför Sverige?		
☐ Ja	☐ Nej	☐ Okänt

Om incidenten har haft konsekvenser inom EU/EES, ange i vilka medlemstater		
☐ Belgien	☐ Italien	☐ Portugal
☐ Bulgarien	☐ Kroatien	☐ Rumänien
☐ Cypern	☐ Lettland	☐ Slovakien
☐ Danmark	☐ Liechtenstein	☐ Slovenien
☐ Estland	☐ Litauen	☐ Spanien
☐ Finland	☐ Luxemburg	☐ Tjeckien
☐ Frankrike	☐ Malta	☐ Tyskland
☐ Grekland	☐ Nederländerna	☐ Ungern
☐ Irland	☐ Norge	☐ Österrike
☐ Island	☐ Polen	
☐ Samtliga EU/EES-medlemstater		

Om incidenten har haft konsekvenser utanför EU/EES, ange i vilka länder

Beskriv vilka gränsöverskridande konsekvenser som incidenten har haft

Operativt stöd från CERT-SE vid pågående incident

CERT-SE:s uppgift är att stödja det svenska samhället i arbetet med att hantera och förebygga it-säkerhetsincidenter. Uppdraget omfattar både privat och offentlig sektor med fokus på samhällsviktig verksamhet. CERT-SE:s verksamhet bedrivs inom ramen för NCSC. Vid en it-incident kan CERT-SE hjälpa till med bland annat rådgivning till drabbade verksamheter för att lindra påverkan och återställa funktion. CERT-SE nås på telefonnummer 010-240 40 40.

Vill ni få operativt stöd att hantera den pågående incidenten av CERT-SE?	
☐ Ja	☐ Nej
Om ni väljer ja, kommer CERT-SE att kontakta er med hjälp av de kontaktuppgifter ni har angivit i upplysningen. CERT-SE återkommer vanligen inom en arbetsdag, eller nästkommande vardag. Om ni väljer nej kan CERT-SE ändå komma att kontakta er även om ni inte behöver stöd att hantera incidenten.	

Om cyberportalen är otillgänglig eller om du inte kan logga in använder du reservförfarandet. Välj förfarande efter hur känsligt innehållet är. Du hittar mer information på ncsc.se/csl.

- **Inte säkerhetsskyddsklassificerade uppgifter:** Ladda ned och fyll i reservformuläret samt ta del av rutinen på webbplatsen för digital inlämning via säker länk. Om webbplatsen inte är tillgänglig, rapportera genom rekommenderat brev till adressen nedan.
- **Säkerhetsskyddsklassificerade uppgifter:** Alla betydande incidenter är rapporteringspliktiga. Det är dock frivilligt att lämna säkerhetsskyddsklassificerade uppgifter vid ifyllandet av formuläret. Om rapporten innehåller säkerhetsskyddsklassificerade uppgifter ska rapporten skickas som ett rekommenderat brev. Lägg rapporten i ett eget kuvert inuti försändelsekuvertet. Använd bud eller värdepost om det går fortare. **OBS! Incidenter i säkerhetsskyddklassad verksamhet ska inte rapporteras enligt CSL.**

Postadress: FRA/NCSC, Box 301, 161 26 Bromma