Incidentanmälan

Incidentanmälan är det andra av tre rapporteringsskeden. Incidentanmälan ska enligt MCFFS (2026:8) om incidentrapportering och informationsskyldighet för väsentliga och viktiga verksamhetsutövare, MCFFS (2026:7) om rapportering av it-incidenter för statliga myndigheter respektive enligt Kommissionens genomförandeförordning (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 72 timmar efter det att verksamhetsutövaren har konstaterat att en inträffad händelse omfattas av rapporteringsplikt. Undantaget till detta är verksamhetsutövare som enligt cybersäkerhetslagen tillhandahåller betrodda tjänster. Sådana verksamhetsutövare ska inkomma med en incident- anmälan senast 24 timmar efter det att verksamhetsutövaren har konstaterat att rapporteringsplikt har uppstått och att den rapporteringspliktiga incidenten påverkar tillhandahållandet av de betrodda tjänsterna.

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.

Incidentens status

Är incidenten fortsatt pågående?	
☐ Ja	☐ Nej

Pågående incident

Om incidenten fortfarande pågår efter det att upplysningen har lämnats, ange hur länge den förväntas fortsätta efter det att incidentanmälan skickats in. Beskriv också vad som har hänt och vilka åtgärder som har vidtagits sedan upplysningen skickades in.

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

Hur länge bedömer ni att incidenten kommer pågå?
☐ Upp till 24 timmar
☐ Upp till 72 timmar
☐ Upp till en vecka
☐ Upp till en månad
☐ Längre än en månad
☐ Kan ej bedöma

Beskriv incidentens händelseförlopp och vad ni har gjort för att hantera den sedan ni lämnade in upplysningen

Viktiga tidpunkter i händelseförloppet

Ange när incidenten inträffade i den egna organisationen och när organisationen inledde hantering av incidenten. Ange även när incidenten upphörde om den inte är pågående. Om tidpunkterna inte är kända, eller inte går att bedöma i nuläget, ange tidpunkt okänd. Med hantering av incidenten avses åtgärder som har vidtagits sedan incidenten upptäcktes och som exempelvis syftar till att förhindra spridning eller begränsa konsekvenser.

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

När inledde er organisation hantering av incidenten?			
Okänt datum ☐	Datum	Okänt klockslag ☐	Klockslag

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

Incidentens orsak

Läs mer om orsaker i vägledningen om incidentrapportering och informationsskyldighet, avsnitt 4.2.2.

Ange vad som har orsakat incidenten	
☐ Systemfel	☐ Mänskligt misstag
☐ Angrepp	☐ Naturhändelse
☐ Annan orsak	☐ Okänt

Beskrivning av orsak

Beskriv hur den angivna orsaken gav upphov till incidenten utifrån den kunskap som finns tillgänglig i nuläget.

Beskriv hur den angivna orsaken gav upphov till incidenten

Om ni har angett incidenten orsakats av angrepp, beskriv hur angreppet genomfördes

Angreppsindikatorer är teknisk information som utgör tecken på förberedelse till, pågående eller genomfört cyberangrepp. Angreppsindikatorer ska uppges om ett cyberangrepp är orsaken till incidenten. Läs mer i vägledningen om incidentrapportering och informationsskyldighet, avsnitt 4.2.2.

Har ni tillgång till angreppsindikatorer som NCSC kan samla in?	
☐ Ja	☐ Nej
Nationellt cybersäkerhetscenter kommer att återkomma med anvisningar om hur angreppsindikatorerna ska rapporteras in	

Incidentens påverkan på system

Läs mer om olika system i vägledningen om incidentrapportering och informationsskyldighet, avsnitt 4.2.2.

Vilken eller vilka typer av system i er organisation har påverkats av incidenten?
☐ **Administrativt system** – It-system som används för administrativ databehandling, kontorsautomation eller affärssystem.
☐ **System dedikerat till information eller kommunikation** – System som lagrar, hanterar eller överför information, till exempel e-post, dokumenthantering, intranät eller kommunikationsplattformar.
☐ **System för processtyrning/operativ teknik (OT)** – System som styr eller övervakar fysiska processer och utrustning, till exempel i industri, produktion, energi eller vattenförsörjning.
☐ **System för säkerhetslösningar** – System som skyddar verksamheten, till exempel brandväggar, antivirus, inloggningslösningar eller övervakningssystem.
☐ **Annat system** – System som inte passar in i någon av kategorierna ovan.
☐ Organisationens system har inte påverkats
☐ **Okänt system** - Används när det inte går att avgöra vilket eller vilka system som påverkats av incidenten.

På vilka sätt har incidenten påverkat organisationens system?
För mer information om tillgänglighet, riktighet inklusive autenticitet samt konfidentialitet se vägledningen om incidentrapportering och informationsskyldighet kapitel 2.

Hur har konfidentialiten hos organisationens system påverkats?
☐ Samtliga av organisationens system har blivit tillgängliga för obehöriga interna användare.
☐ Vissa av organisationens system har blivit tillgängliga för obehöriga interna användare.
☐ Samtliga av organisationens system har blivit tillgängliga för obehöriga externa användare.
☐ Vissa av organisationens system har blivit tillgängliga för obehöriga externa användare.
☐ Konfidentialiteten hos organisationens system har påverkats på annat sätt.
☐ Konfidentialiteten hos organisationens system har inte påverkats.
☐ Det är okänt om konfidentialiteten hos organisationens system har påverkats.

Hur har riktigheten (inklusive autenticiteten) hos organisationens system påverkats?
☐ Samtliga av organisationens system avstår från att utföra uppgifter som organisationen har konfigurerat dem att utföra.
☐ Vissa av organisationens system avstår från att utföra uppgifter som organisationen har konfigurerat dem att utföra.
☐ Samtliga av organisationens system utför andra uppgifter än de som organisationen har konfigurerat dem att utföra.
☐ Vissa av organisationens system utför andra uppgifter än de som organisationen har konfigurerat dem att utföra.
☐ Riktigheten (inklusive autenticiteten) hos organisationens system har påverkats på annat sätt.
☐ Riktigheten (inklusive autenticiteten) hos organisationens system har inte påverkats.
☐ Det är okänt om riktigheten (inklusive autenticiteten) hos organisationens system har påverkats.

Hur har tillgängligheten hos organisationens system påverkats?
☐ Samtliga av organisationens system har blivit otillgängliga för behöriga interna användare.
☐ Vissa av organisationens system har blivit otillgängliga för behöriga interna användare.
☐ Samtliga av organisationens system har blivit otillgängliga för behöriga externa användare.
☐ Vissa av organisationens system har blivit otillgängliga för behöriga externa användare.
☐ Tillgängligheten hos organisationens system har påverkats på annat sätt.
☐ Tillgängligheten hos organisationens system har inte påverkats.
☐ Det är okänt om tillgängligheten hos organisationens system har påverkats.

Beskriv övergripande hur systemet fungerar i ett normalläge, vad det används till samt hur systemet har påverkats sedan incidenten inträffade.

Beskriv systemet eller systemen och hur det eller de har påverkats

Incidentens påverkan på information i system

Vilka typer av information i behov av utökat skydd har påverkats av incidenten?
☐ **Verksamhetskritisk information** – information som är avgörande för att verksamheten ska fungera.
☐ **Konfidentiell information** – Information som endast får delas med behöriga personer.
☐ **Information som är viktig för mottagare av era tjänster** – information som era kunder eller användare är beroende av, till exempel för att kunna använda en tjänst eller fatta beslut.
☐ **Känslig information** – information som kräver extra skydd och som kan orsaka skada, ekonomisk förlust eller andra typer av negativa konsekvenser för individer eller organisationer om den blir tillgänglig för obehöriga.
☐ **Personuppgifter** – information som kan kopplas till en enskild person, till exempel namn, personnummer eller kontaktuppgifter.
☐ **Annan information i behov av utökat skydd** – information som inte passar in i ovanstående kategorier men som ändå kräver extra skydd. Det handlar om 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.
☐ Information i behov av utökat skydd har inte påverkats.
☐ Okänt om information i behov av utökat skydd har påverkats.

På vilka sätt har incidenten påverkat organisationens information som är i behov av utökat skydd?

Hur har konfidentialiten hos organisationens information i behov av utökat skydd påverkats?
☐ Informationsmängder som innhåller sådan information har blivit tillgänglig för obehöriga interna användare.
☐ Informationsmängder som innhåller sådan information har blivit tillgänglig för obehöriga externa användare.
☐ Sådan informations konfidentialitet har påverkats på annat sätt.
☐ Sådan informations konfidentialitet har inte påverkats.
☐ Det är okänt om sådan informations konfidentialitet har påverkats.

Hur har riktigheten (inklusive autenticiteten) hos organisationens information i behov av utökat skydd påverkats?
☐ Informationsmängder som ska innehålla sådan information kan inte upprättas på ett korrekt sätt.
☐ Informationsmängder som innehåller sådan information har ändrats.
☐ Sådan informations riktighet (inklusive autenticitet) har påverkats på annat sätt.
☐ Sådan informations riktighet (inklusive autenticitet) har inte påverkats.
☐ Det är okänt om sådan informations riktighet (inklusive autenticitet) har påverkats.

Hur har tillgängligheten hos organisationens information i behov av utökat skydd påverkats?
☐ Informationsmängder som innhåller sådan information har blivit otillgänglig för behöriga interna användare.
☐ Informationsmängder som innehåller sådan information har blivit otillgänglig för behöriga externa användare.
☐ Sådan informations tillgänglighet har påverkats på annat sätt.
☐ Sådan informations tillgänglighet har inte påverkats.
☐ Det är okänt om sådan informations tillgänglighet har påverkats.

Beskriv hur informationen i behov av utökat skydd har påverkats

Incidentens konsekvenser för mottagare av organisationens sektorsverksamhet

Ange områden inom vilka mottagare av er tjänster påverkas eller riskerar att påverkas negativt av incidenten. För mer information om mottagare av tjänster, se vägledningen om incidentrapportering och informationsskyldighet avsnitt 4.2.3 samt kapitel 5.

Ange inom vilka områden ni levererar sådan sektorsverksamhet som har påverkats eller riskerar att påverkas av incidenten	
☐ Demokrati och beredskap	☐ Utrikeshandel
☐ Legitimering	☐ Ekonomisk säkerhet
☐ Energiförsörjning	☐ Livsmedelsförsörjning och dricksvatten
☐ Elektroniska kommunikationer och post	☐ Hälsa, vård och omsorg

Ange inom vilka områden ni levererar sådan sektorsverksamhet som har påverkats eller riskerar att påverkas av incidenten	
☐ Räddningstjänst och skydd av civilbefolkningen	☐ Förskola, utbildning och forskning
☐ Industri, byggande och handel	☐ Ordning och säkerhet
☐ Försörjning av grunddata	☐ Militärt försvar
☐ Transporter	☐ Samtliga områden

Ange vilka slags konsekvenser incidenten medför eller riskerar att medföra för mottagare av organisationens sektorsverksamhet

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