Lägesrapport

En slutrapport ska lämnas inom en månad från incidentanmälan enligt cybersäkerhetslagen, och inom en månad från upplysningen enligt MCFFS (2026:7) om rapportering av it-incidenter för statliga myndigheter. Om incidenten fortfarande är pågående efter en månad ska verksamhetsutövaren eller den statliga myndigheten istället för en slutrapport lämna en lägesrapport. I sådana fall ska därefter en slutrapport lämnas senast en månad efter incidenten har hanterats.

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.

Beskriv hur incidenten har utvecklats, vad ni har gjort för att hantera den samt varför incidenten fortfarande ändå är pågående

Hur länge bedöms incidenten pågå

Bedömning av hur länge en incident kommer pågå avser den tid från det att lägesrapporten lämnas in.

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

Påverkar incidenten fortfarande organisationens sektorsverksamhet?
☐ Ja, sektorsverksamheten är fortfarande påverkad
☐ Nej, men det finns en risk att sektorsverksamheten blir påverkad
☐ Nej

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

Har ni tillgång till angreppsindikatorer som NCSC kan samla in?	
☐ Ja, sektorsverksamheten är fortfarande påverkad	☐ Nej

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