**Säkerhetsincident företag – Instruktion**

**Steg 1: Anmälan om säkerhetsincident**

Vid en befarad eller konstaterad säkerhetshotande händelse skall, utan dröjsmål en   
anmälan om säkerhetsincident göras till FMV Säkerhetsskyddsavdelning.

Exempel på säkerhetshotande händelser kan vara:

* IT-relaterad störning eller påverkan
* Inbrott eller tillgrepp
* Befarad eller faktisk förlust av sekretess och/eller säkerhetsskyddsklassificerade uppgifter/materiel
* Brister i säkerhetsskydd (Inkluderar även underleverantörer)
* Misstanke om spionage eller sabotage

Underlaget fylls i och skickas med epost till:

* security@fmv.se

**Steg 2: Rapportering av säkerhetsincident**

Efter att en säkerhetsincident anmälts åligger det anmälaren att skyndsamt inkomma med säkerhetsrapport. Säkerhetsrapporten syftar till att beskriva omständigheter för händelsen samt eventuella konsekvenser eller skada som incidenten orsakat.

Inga krav ställs på rapportens format, men berört företag skall sträva efter att detaljerat förse incidentrapporten med svar för minst följande information.

* När och var händelsen inträffat
* Vad som inträffat
* Händelseförlopp
* Vem eller vilka som involverats
* Åtgärder; vidtagna och planerade
* Bedömning; varför händelsen inträffat
* Bedömning; vilken är skadan
* Förslag på åtgärder för att reducera skada
* Kontaktuppgifter till den som upprättar rapporten

**VÄRDERA SEKRETESSEN**

INCIDENTANMÄLAN IFYLLS ENDAST MED INFORMATION UR MALL NEDAN.

SEKRETESS- OCH SÄKERHETSSKYDDSKLASSAD RAPPORT INSÄNDS ENDAST MED GODKÄNDA METODER EX. REK- OCH VÄRDEPOST ELLER GENOM KURIR

Anmälan om säkerhetsincident:

Ifyllt underlag mailas till Säkerhetsskyddsavdelningen vid FMV: SECURITY@FMV.SE

|  |  |
| --- | --- |
| **Berört verksamhetsområde/projekt på FMV:**  Klicka här för att ange text. | **Säkerhetsincident-id** (fylls i av FMV): |

\*Obligatorisk uppgift

Kontaktuppgifter

|  |  |
| --- | --- |
| Tidpunkt för underlagets skapande \*  Klicka här för att ange datum. | Företag \*  Klicka här för att ange text. |
| För- och efternamn rapportör \*  Klicka här för att ange text. | Telefonnummer rapportör \*  Klicka här för att ange text. |
| Uppdrag/projekt där händelsen inträffat \*  Klicka här för att ange text. | Mailadress rapportör\*  Klicka här för att ange text. |
| Ort/orter som berörs av händelsen | Säkerhetsskyddsavtal, nivå  1  2  3 |
| Aktörsdriven  Aktörsdriven incident innebär att någon (en aktör) med avsikt har orsakat en händelse som har eller kan ha påverkat verksamheten på ett negativt sätt.  Exempel på aktörsdrivna incidenter kan vara:  - Inbrott/stöld  - Misstanke om olovlig verksamhet rörande ex. sabotage eller spioneri  - Kontakttagnings- och värvningsförsök  Icke aktörsdriven  En icke aktörsdriven incident innebär vi själva oavsiktligt, oftast genom slarv, har orsakat en händelse som har eller kan ha påverkat verksamheten på ett negativt sätt.  Exempel på icke aktörsdrivna incidenter kan vara:  - Förlust/Felaktig hantering av sekretessbelagd handling eller materiel  - Olåst säkerhetsskåp eller annat skyddsvärt utrymme  - Felaktig/bristfällig säkerhetsprövning | |
| Ärendet bedöms som brådskande.  Ärendet bedöms som icke brådskande. | |
| **Tillgång/skyddsvärde \***  *Händelsen berör ett eller flera av nedan angivna tillgångar, ex. en stulen dator är både en förlust av information och materiel)*  **Information (all typ av media)**  Förlust  Felaktig hantering  skadlig kod/intrång  Signalskyddsincident  Övriga incidenter mot info  **Materiel**  Påverkad tillgång  Åverkan  Förlust  Felaktig hantering  Förlust av vapen/am  Övriga incidenter mot mtrl  **Personal**  Hot mot personal  Utfall (spontan eller RK)  Misstanke mot personal  Övriga incidenter mot personal  **Anläggning**  Inbrott  Åverkan  Övriga incidenter mot anläggningar  **Verksamhet**  Främmande underrättelsetjänst  Kriminalitet  Sabotage  Subversion  Terrorism | |
| **Preliminär konsekvensbedömning av händelsen.** \*  *Är du osäker på nivån väljer du alltid den högre konsekvensen.*  RÖD  HÄNDELSE  Händelsen riskerar att få eller har fått mycket stora konsekvenser för FMV och/eller kunds verksamhet.  FMV förtroendekapital kan till mycket stor del skadas genom negativ massmedial uppmärksamhet  Informationsförlust på den här nivån är KVALIFICERAT HEMLIG (KH) eller HEMLIG (H)  Information rörande hela eller stora delar av ett vapensystem.  **Ekonomiska konsekvenser (> 1000 milj kr)**  **Försvarsfunktion/materielsystem, 10-25 år att återskapa förmågan**  Bedömd konsekvens  ORANGE  HÄNDELSE  Händelsen riskerar att få eller har fått stora konsekvenser för FMV och/eller kunds verksamhet.  FMV förtroendekapital kan till stor del skadas genom negativ massmedial uppmärksamhet  Informationsförlust på den här nivån är KONFIDENTIELL (K).  Information rörande enskilda vapensystem, vapen eller ammunitionseffekter.  **Ekonomiska konsekvenser (10- 100 milj kr)**  **Bruksprodukt, 2-5 år att återskapa förmågan.**  GUL  HÄNDELSE  Händelsen riskerar att få eller har fått små konsekvenser för FMV och/eller kunds verksamhet.  FMV förtroendekapital kan till liten del skadas genom negativ massmedial uppmärksamhet  Informationsförlust på den här nivån är BEGRÄNSAT HEMLIG (B) och övrig sekretess enl OSL.  Information rörande vapen och ammunitionseffekter hanteras ej i den nivå.  **Ekonomiska konsekvenser (< 10 milj kr)**  **Bruksprodukt, upp till 2 år att återskapa förmågan.** | |