Systemnamn   
MAll Säkerhetsanalys i Säkerhetsmålsättning

**Innehållsförteckning**

[1 Sammanfattning 4](#_Toc348704744)

[2 Inledning 5](#_Toc348704745)

[2.1 Syfte 5](#_Toc348704746)

[2.2 Omfattning och avgränsning 5](#_Toc348704747)

[3 Basfakta 6](#_Toc348704748)

[3.1 Versionshistorik 6](#_Toc348704749)

[3.2 Granskat av 6](#_Toc348704750)

[3.3 Referenser 6](#_Toc348704751)

[3.4 Begrepp och förkortningar 6](#_Toc348704752)

[4 Identifiering och analys av skyddsvärda tillgångar 7](#_Toc348704753)

[4.1 Informationstillgångar 7](#_Toc348704754)

[4.2 Systemdokumentation 8](#_Toc348704755)

[*4.3* Personuppgifter i *Systemnamn* 8](#_Toc348704756)

[4.4 Klassificering av materiel ingående i *Systemnamn* 8](#_Toc348704757)

**Så här används denna mall:**

* Instruktionen om vad som ska stå under varje rubrik anges i en punktlista under respektive rubrik. Denna text ska raderas innan dokumentet färdigställs.
* Text som är skriven utan punktlista är text som kan användas också i det färdigställda dokumentet.
* Ersätt *Systemnamn* med systemets namn.
* Redigera dokumentets metadata genom att fylla i relevant information under ”Egenskaper” (eng. ”Properties”) så som namn på systemet och version på dokumentet. Uppdatera därefter fältkoder.
* Ta bort rubriker som inte är relevanta och lägg till egna rubriker där så behövs.
* Radera denna sida.

**Denna mall för Säkerhetsanalys innehåller bl a instruktioner om följande:**

* Informationsklassning
* Bakgrund till hur man gör informationsklassning
* Konsekvensbedömning med avseende på
  + Sekretess
  + Tillgänglighet
  + Riktighet
* Hur man hämtar informationsflöden från verksamheten
* Informationsflöde från såväl externa som interna parter

# Sammanfattning

* Under denna rubrik görs en kort summering (max 1 A4-sida) av Identifiering och analys av skyddsvärda tillgångar inkluderat det primära resultatet och de slutsatser som kan dras. En text som redovisar om någon del av det framtagna materialet belagts med sekretess (även vid icke försvarssekretess) bör också redovisas här.

# Inledning

* Säkerhetsanalysen ger underlag för hot-, risk- och sårbarhetsanalysen. Identifiering och analys av skyddsvärda tillgångar ligger till grund för och utgör en bilaga till säkerhetsmålsättningen i auktorisations- och ackrediteringsprocessen. Säkerhetsmålsättningen utgör en del i beslutsunderlagen för beslutspunkterna B2 och B5, enligt Försvarsmaktens IT-livscykelmodell [ref 1].
* Till stöd för analys används Handbok för Försvarsmaktens säkerhetsskyddstjänst sekretessbedömning [ref 3].

Säkerhetsanalysen utgör en del av säkerhetsmålsättning för Systemnamn. Säkerhetsmålsättning ingår i beslutsunderlaget för beslutspunkt B2 och B5 enligt Försvarsmaktens IT livscykelmodell [ref 1].

## Syfte

* Syftet med säkerhetsanalysen är att lista den information som hanteras för definierad verksamhet, informationsflöde samt hur informationen är säkerhetsklassad. För varje typ av information görs en bedömning och klassning av känslighet ur sekretess-, riktighet och tillgänglighetssynpunkt samt bedömningar om informationens skyddsvärde. Även en prioritering av de skyddsvärda tillgångarna redovisas.

Syftet med detta dokument är att identifiera och utgöra en analys av skyddsvärda tillgångar i verksamheten och *Systemnamn* samt göra en bedömning och klassning ur sekretess-, riktighets- samt tillgänglighetssynpunkt samt bedömning av konsekvensnivåer.

## Omfattning och avgränsning

* Ange omfattning och eventuella avgränsningar för säkerhetsanalysen.
* Exempel på omfattning är vilka delsystem och gränsytor som avses ingå.
* Exempel på avgränsning är angränsande system som inte ingår, delkomponenter som inte anses vara IT-system/relevanta ur informationssäkerhetspunkt osv.
* Ta även hänsyn till avgränsningar eller särskild hantering avseende material som hanteras i särskild ordning med hänsyn till dess klassning.

# Basfakta

## Versionshistorik

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ver | Datum | Status | Beskrivning | Fastställt av |
|  |  |  |  |  |

## Granskat av

|  |  |  |
| --- | --- | --- |
| Namn | Organisation | Kompetensområde |
|  |  |  |

## Referenser

* I tabellen nedan listas exempel på referenser.

|  |  |  |
| --- | --- | --- |
| Ref. nr. | Dokument | Dok. nr. |
|  | Direktiv för Försvarsmaktens informationsteknikverksamhet (DIT 04) | HKV 09 626:783 69 |
|  | Handbok för Försvarsmaktens Säkerhetstjänst, Informationsteknik, (H SÄK IT), 2006 års utgåva. | M7745-734062 |
|  | Handbok för Försvarsmaktens Säkerhetsskyddstjänst Sekretessbedömning, (H SÄK Sekrbed), 1999 års utgåva. | M7745-734081 |
|  | H Säk Sekrbed A | M7739-352028 |
|  | H Säk Sekrbed B | HKV 2011-03-25 10 440:53353 |
|  | Handbok för Försvarsmaktens Säkerhetstjänst Säkerhetsskydd, (H SÄK Skydd), 2007 års utgåva. | M7739-352005 |
|  | Säkerhetsskyddsförordning | SFS (1996:633) |
|  | Försvarsmaktens föreskrifter om säkerhetsskydd | FFS 2003:7 |
|  | Försvarsmaktens interna bestämmelser om IT-säkerhet | FIB 2006:2 |
|  | Offentlighets- och sekretesslagen | 2009:400 |
|  | Personuppgiftslagen | 1998:204 |
|  | Riktlinjer vid inplacering av hemliga uppgifter i informationssäkerhetsklass | 2004-05-18 HKV 10 440:68631 |
|  | *Systemnamn* Verksamhetsanalys |  |
|  | Metodbeskrivning Säkerhetsmålsättning |  |
|  | KSF Krav på IT-säkerhetsförmågor hos IT-system v3.0 | 10 750:64354 Bilaga 1 |

## Begrepp och förkortningar

Se *Systemnamn* Säkerhetsmålsättning.

# Identifiering och analys av skyddsvärda tillgångar

* Identifiera vilka skyddsvärda tillgångar som finns i verksamheten.
* För identifieringen av skyddsvärda tillgångar görs även en informationsklassning och bedömning konsekvensnivå för de skyddsvärda tillgångarna.
* För varje tillgång anges vilket informationssäkerhetsområde som berör tillgången, det vill säga om det berörs av sekretess, riktighet eller tillgänglighet.
* I informationsklassningen anges vilken klassning varje tillgång får. För bakgrundsbeskrivning till informationsklassning och konsekvensbedömning se metodbeskrivningen för säkerhetsanalys, [ref 14].
* För uppgifter som omfattas av sekretess enligt OSL (2009:400) ska en konsekvensbedömning göras:
  + Uppgifter som omfattas av Offentlighets- och sekretesslagen.
  + Uppgifter som är verksamhetskritisk information.
  + Uppgifter som obehöriga inte får ta del av, som inte får förändras, som måste finnas tillgänglig eller som måste kunna härledas till en användare t.ex. stridsledningsdata, elektroniska fakturor, personuppgifter, patientjournaler, underrättelser eller komplex materiel.
  + Bakgrundsinformation till värderingen av konsekvensnivå återfinns i Metodbeskrivning för säkerhetsmålsättning, [ref 14] samt KSF Krav på IT- säkerhetsförmågor hos IT-system v3.0, [ref 15].
  + Informationen ska bl a användas för att avgöra konsekvensnivå vid bedömningen av vilka säkerhetskrav som ska tillämpas för IT-systemet utifrån MUST KSF 3.0.
* Informationsklassningen av de skyddsvärda tillgångarna används sedan i verksamhetsbeskrivningen där den konkretiseras till specifika användningsfall och informationsflöden.
* Analysera vilka prioriteter verksamheten har. Ansvarig i verksamheten måste delta i denna bedömning. Resultatet dokumenteras i tabellen nedan och blir sedan drivande i framtida arbete. Prioritering av skyddsvärda tillgångar utförs för att verksamhetens perspektiv ska komma fram och är kopplat till förmåga och uppgift. Prioritering tillsammans med informationens klassning blir dimensionerande i arbetet med utvecklingen av IT-systemet.
* Tabellerna nedan är i fyllda med exempel på hur man fyller i ”Område” och ”Klassning”. Dessa tas bort från mallen och ersätts med värden som gäller för IT-systemet i fråga.
* Informationstillgångar, systemdokumentation, personuppgifter och klassificering av materiel är angivet som exempel på skyddsvärda tillgångar. Fyll på med egna rubriker efter vad som är tillämpligt för systemet i fråga.

## Informationstillgångar

* I tabellen listas exempel på informationsmängder. Uppdatera tabellen enligt vad som är tillämpligt för systemet i fråga.

Tabellen nedan redovisar informationsklassning för delsystem ingåendes i *Systemnamn*. Kolumnen ”Informationsmängd” anger vilken typ av information som avses. ”Klassning” anger bedömd informationssäkerhetsklass och i kolumnen ”Prioritet” anges verksamhetens prioritering av de skyddsvärda tillgångarna. I ”Kommentar” ges förtydliganden av klassningen eller annan relevant information.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Informationsmängd | Område | Klassning | Prioritet | Kommentar |
| E-post | Riktighet | B | Hög |  |
| Tal | Sekretess | H/R | Låg |  |
|  |  |  | Medel |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Systemdokumentation

* I tabellen listas exempel på systemdokumentation. Ta bort information som inte är tillämplig för systemet i fråga och komplettera med ytterligare information om så behövs.

Tabellen nedan redovisar informationsklassning för systemdokumentation för *Systemnamn*. Kolumnen ”Informationsmängd” anger vilken typ av information som avses. ”Klassning” anger bedömd informationssäkerhetsklass och i kolumnen ”Prioritet” anges verksamhetens prioritering av de skyddsvärda tillgångarna. I ”Kommentar” ges förtydliganden av klassningen eller annan relevant information.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Informationsmängd | Område | Klassning | Prioritet | Kommentar |
| Installationsbeskrivning | Riktighet | B | Hög |  |
| Beskrivningshandbok | Sekretess | H/R | Låg |  |
| Underhållsdokumentation |  |  | Medel |  |
| Utbildningsmaterial |  |  |  |  |
| Satslistor |  |  |  |  |
| Reservdelskatalog |  |  |  |  |
| Återvinningsmanual |  |  |  |  |

## Personuppgifter i *Systemnamn*

* Om personuppgifter förekommer i IT-systemet så anges det här. Ange då även vilka delsystem som omfattas.

## Klassificering av materiel ingående i *Systemnamn*

* Ange vilken klassificering materielet som ingår i IT-systemet har. Det är alltså materieltsystemet *utan* information som avses. Om materielet omfattas av sekretess är det oftast kommersiell sekretess det rör sig om, vilket kravställs från leverantören av IT-systemet.
* Denna information kan eventuellt fås från UTTEM.