Systemnamn   
mall Säkerhetkrav

**Innehållsförteckning**

[1 Sammanfattning 4](#_Toc348704812)

[2 Inledning 5](#_Toc348704813)

[2.1 Syfte 5](#_Toc348704814)

[2.2 Omfattning och avgränsning 5](#_Toc348704815)

[3 Basfakta 6](#_Toc348704816)

[3.1 Versionshistorik 6](#_Toc348704817)

[3.2 Granskat av 6](#_Toc348704818)

[3.3 Referenser 6](#_Toc348704819)

[3.4 Bilagor 6](#_Toc348704820)

[3.5 Begrepp och förkortningar 6](#_Toc348704821)

[4 Verksamhetskrav 8](#_Toc348704822)

[5 Författningskrav 9](#_Toc348704823)

[6 Strategi för uppfyllande av MUST KSF 10](#_Toc348704824)

[7 Säkerhetsmål 11](#_Toc348704825)

[7.1 Tekniska säkerhetsmål 11](#_Toc348704826)

[7.2 Administrativa och organisatoriska säkerhetsmål 11](#_Toc348704827)

[7.3 Fysiska säkerhetsmål 12](#_Toc348704828)

**Så här används denna mall:**

* Säkerhetsmål ska skrivas på FM-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, inklusive punktlistan nedan.

**Säkerhetsmålsättningen ska omfatta:**

* Mål för sekretess, riktighet, tillgänglighet och spårbarhet.
* Tekniska, administrativa och organisatoriska samt fysiska mål. Administrativa och organisatoriska samt de fysiska målen stödjer BOA (Beslut om användning) och även alternativa lösningar i STAU.
* Författningsanalys genomförs i de fall då andra aspekter än rikets säkerhet är aktuellt exempelvis för internationella regelverk. Tekniska aspekter kring rikets säkerhet tas om hand av MUST KSF och verksamhetskraven.

# Sammanfattning

* Under denna rubrik görs en kort summering (max 1 A4-sida) av säkerhetsmålsättningen inkluderat det primära resultatet och de slutsatser som kan dras.
* Sammanfattningen ska innehålla det primära resultatet från:
  + Verksamhetsbeskrivning
  + Säkerhetsanalys

# Inledning

## Syfte

Arbetet med framtagning av användningsfall är utgångspunkten för de analyser, krav, bedömningar och säkerhetsmål som utgör grunden för säkerheten i och kring ett IT-system. Dokumentet innehåller de relevanta mätbara, entydiga och kompletta säkerhetskrav, som skall uppfyllas för att säkerheten och kring IT-systemet skall anses vara godtagbar. Säkerhetskraven tas fram med hjälp av verksamhetsbeskrivning, säkerhetsanalys, hotanalys samt i gällande fall författningskrav. Författningsanalys genomförs i de fall då andra aspekter än rikets säkerhet är aktuellt. Tekniska aspekter kring rikets säkerhet tas om hand av MUST KSF och verksamhetskraven. I detta dokument återges Systemnamns säkerhetskrav. För detaljerad beskrivning av respektive analys se dokumentets bilagor.

## Omfattning och avgränsning

* Ange omfattning och eventuella avgränsningar för arbetet med att ta fram verksamhetens säkerhetskrav via användningsfall.
* 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.
* Var noggrann med avgränsningen så att arbetet inte blir för omfattande samt att det blir tydligt avseende vilka/vilket system användningsfallen avser. B1-beslutet eller UTTEM kan eventuellt ge input till avgränsning.
* Under denna rubrik kan det även vara lämpligt att ange på vilken systemnivå IT-systemet är (om det består av ”system av system”) och i sådana vilket scenario enligt ”Verifiering system av system” som det rör sig om [ref 4].

# 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) | M7745-734062 |
|  | Försvarsmaktens interna bestämmelser om IT-säkerhet | FIB 2006:2 |
|  | Instruktion Verifiering system av system | 13FMV5921-12:1 |
|  | UTTEM *Systemnamn* |  |
|  | Metodbeskrivning användningsfall | 13FMV5921-8:2 |

## Bilagor

* I tabellen nedan listas säkerhetsmålsättningens bilagor.

|  |  |
| --- | --- |
| Bilaga. nr. | Dokument |
|  | *Systemnamn* Verksamhetsbeskrivning |
|  | *Systemnamn* Säkerhetsanalys |

## Begrepp och förkortningar

* Fyll på tabellen nedan efterhand med nya begrepp och förkortningar.

Tabellen nedan anger begrepp och förkortningar som används i säkerhetsmålsättningen och dess bilagor.

|  |  |
| --- | --- |
| Begrepp/Förkortning | Definition |
| Försvarsmaktens IT-livscykelmodell | En gemensam livscykelmodell för all IT-verksamhet inom Försvarsmakten. |
| Hot | Möjlig oönskad händelse som orsakar eller kan orsaka negativa konsekvenser för verksamheten. |
| IT-system | IT-system med teknik som hanterar och utbyter information med omgivningen. |
| IT-verksamhet | Verksamhet för IT-system. |
| Produktägare (PÄ) | Den som är utsedd att vara produktägare enligt 4 § i FIB 2007:5: Till produktägare får utses den chef som har ansvaret för den verksamhet som ett IT-system huvudsakligen skall stödja. CIO, eller den han eller hon bestämmer, utser produktägare. Ett beslut att utse någon till produktägare skall dokumenteras.  (2 och 4 §§ Försvarsmaktens interna bestämmelser (FIB 2007:5) om IT-verksamhet, [Ref 3])  Roll i Försvarsmaktens IT-livscykelmodell. |
| Riktighet | Korrekthet i data och information (DIT 04) |
| Risk | Produkten av sannolikheten för ett framgångsrikt angrepp och därmed uppkommande av skada. (H SÄK IT) |
| Spårbarhet | Spårbarhet innebär att verksamheten och tillhörande IT-system skall innehålla funktioner, som gör det möjligt att entydigt härleda utförda operationer på objekt till enskilda subjekt. |
| Sårbarhet | Svaghet i ett IT-system eller i en verksamhet, i form av bristande förmåga att motstå hot. |
| Tillgänglighet | Tillgänglighet innebär möjligheten att utnyttja resurser efter behov i förväntad utsträckning och inom önskad tid. |
| UTTEM | Utkast taktisk-teknisk-ekonomisk målsättning |

# Verksamhetskrav

* Infoga tabell med verksamhetskrav från verksamhetsbeskrivningen. Endast kolumnerna med löpnummer och kravtext flyttas över. Dessutom läggs en kolumn till med spårbarhet till vilket säkerhetsmål i kapitel 7 som möter kravet.
* I tabellen nedan anges exempel på verksamhetskrav. Ta bort dessa och ersätt med verkliga krav för IT-systemet i fråga.

Efter genomförd verksamhetsbeskrivning redovisas nedan de krav som bedöms relevanta för Systemnamn ur ett IT-säkerhetsperspektiv. I kolumnen ”Nr” anges löpnummer för respektive verksamhetskrav. Kolumnen ”Krav” anger kravet medan kolumnen ”SM” anger spårbarhet till säkerhetsmålen i kapitel 7.

|  |  |  |
| --- | --- | --- |
| Nr | Verksamhetskrav | SM |
|  | *Systemnamn* ska vara försett med av Försvarsmakten godkänt krypto. | SM 1 |
|  | Användare ska autentiseras vid användning av *Systemnamn*. | SM 2 |
|  | Dataöverföring för anslutna informationssystem och/eller sensorer skall kunna fortsätta samtidigt som radiokanal används. | SM 3 |
|  | Kvaliteten på det överförda talet skall vara så bra att det medger röstigenkänning och sinnesstämning/nyanser i röst ska förmedlas. | SM 4 |
|  | Installation av ny programvara ska utföras av administratör. | SM 8 |
|  | Installation av ny programvara får ej ske under skarpt uppdrag. | SM 8 |
|  |  |  |

# Författningskrav

* Lagar och förordningar förutsätts följas, författningskraven nedan är endast tilläggskrav utöver dessa.
* Författningsanalys genomförs i de fall då andra aspekter än rikets säkerhet är aktuellt t.ex. internationella regelverk. Tekniska aspekter kring rikets säkerhet tas om hand av MUST KSF och verksamhetskraven.
* Infoga tabell med krav från författningsanalysen. Endast kolumnerna med löpnummer och kravtext flyttas över. Dessutom läggs en kolumn till med spårbarhet till vilket säkerhetsmål i kapitel 7 som möter kravet.

Efter genomförd författningsanalys redovisas nedan de krav som bedöms relevanta för Systemnamn ur ett IT-säkerhetsperspektiv. KSF 3.0 förutsätts omhänderta tekniska krav som kan härledas till lagar och förordningar. Författningskraven nedan är endast tilläggskrav utöver dessa. I kolumnen ”Nr” anges löpnummer för respektive krav från författningsanalysen. Kolumnen ”Krav” anger kravet medan kolumnen ”SM” anger spårbarhet till säkerhetsmålen i kapitel 7.

|  |  |  |
| --- | --- | --- |
| Nr | Författningskrav | SM |
|  |  |  |
|  |  |  |

# Strategi för uppfyllande av MUST KSF

* Här ges en kort beskrivning av hur IT-systemet avser uppfylla MUST Krav på säkerhetsfunktioner (KSF).
* Strategin måste samverka med systemdesignen i stort samt förankras och ”styra” övrig design.
* Beskrivningen ska vara kort, det är ej omfattande IT-säkerhetsarkitekturarbete som avses.
* T.ex. så kan man beskriva att IT-systemet uppdelas i olika informationssäkerhetsdomäner med separation.
* Bedömning av exponeringsnivån i verksamhetsbeskrivningen samt konsekvensnivån i säkerhetsanalysen bör framgå här.
* Input kan erhållas från genomförd säkerhetsanalys, användningsfall samt identifiering och informationsklassning av informationsflöde.

# Säkerhetsmål

* Formulera säkerhetsmål utifrån identifierade krav i kapitel 4, och 5 ovan.
* Ett krav kan utmynna i flera säkerhetsmål.
* Ett säkerhetsmål kan möta flera krav.
* Då säkerhetsmålen ska utformas utifrån till exempel författningsanalysen så är det viktigt att plocka ur och beskriva kärnan, det vill säga lagrummet, och inte hela författningar.
* Säkerhetsmålen ska formuleras så att de är relevanta, mätbara, entydiga och kompletta.
* Tillse att de olika säkerhetsmålen inte är motstridiga.
* Säkerhetsmålen delas upp tekniska, administrativa och organisatoriska samt fysiska säkerhetsmålen.
* De tekniska säkerhetsmålen blir input till den tekniska kravspecifikationen.
* De administrativa och organisatoriska samt fysiska säkerhetsmålen stödjer BOA (Beslut om användning) och även alternativa lösningar i STAU.
* Det är endast de säkerhetsmålen som är kopplade till utvecklingen av detta system som beskrivs nedan, dvs. ytterligare administrativa krav kan tillkomma.
* I tabellen nedan anges exempel på säkerhetsmål. Ta bort dessa och ersätt med verkliga säkerhetsmål för IT-systemet i fråga.

Säkerhetsmålen anges som tekniska, administrativa och organisatoriska samt fysiska och har erhållits utifrån verksamhetskrav samt i gällande fall formella författningskrav. Författningsanalys genomförs i de fall då andra aspekter än rikets säkerhet är aktuellt. Tekniska aspekter kring rikets säkerhet tas om hand av MUST KSF. Varje styrande krav från verksamheten och regelverk ställer krav på säkerhetsskydd för uppgifter som faller under säkerhetsskyddslagstiftningen och skydd för övriga uppgifter och skall mötas av mätbara säkerhetsmål. Det är endast de säkerhetsmål som är kopplade till utvecklingen av detta system som beskrivs nedan, dvs. ytterligare administrativa krav kan tillkomma. Kolumnen ”Nr” nedan anger löpnummer för respektive säkerhetsmål medan ”Tekniskt säkerhetsmål”/ ”Administrativt säkerhetsmål”/ ”Fysiskt säkerhetsmål”/ ”Organisatoriskt säkerhetsmål” anger säkerhetsmål. I kolumnen ”Krav” anges spårbarhet till ursprungskravet i avsnitt kapitel 4 och 5 ovan.

## Tekniska säkerhetsmål

| Nr | Tekniskt säkerhetsmål | Krav |
| --- | --- | --- |
|  | *Systemnamn* ska vara försett med av Försvarsmakten godkänt krypto. | V1 |
|  | Användare ska autentiseras vid användning av *Systemnamn*. | V2 |
|  | Dataöverföring för anslutna informationssystem och/eller sensorer skall kunna fortsätta samtidigt som radiokanal används. | V3 |
|  | Kvaliteten på det överförda talet skall vara så bra att det medger röstigenkänning och sinnesstämning/nyanser i röst ska förmedlas. | V4 |
|  |  |  |

## Administrativa och organisatoriska säkerhetsmål

| Nr | Administrativt säkerhetsmål | Krav |
| --- | --- | --- |
|  | Samtliga användare av *Systemnamn* ska ha genomgått användarutbildning. |  |
|  | Det skall finnas organisation och rutiner för tilldelning av behörighet till *Systemnamn*. |  |
|  | Installation av ny programvara ska utföras av administratör och får ej ske under skarpt uppdrag. | V5, V6 |
|  |  |  |

## Fysiska säkerhetsmål

| Nr | Fysiskt säkerhetsmål | Krav |
| --- | --- | --- |
|  |  |  |
|  |  |  |