Stödmaterial om säkerhetsskydd

Vägledning gällande samrådsplikten och signalskyddssystem MGS

Säkerhetspolisen

Innehåll

Inledning

KryptoPC, MGS, är ett signalskyddssystem som utgör ett informationssystem enligt säkerhetsskyddsförordningen, (SSF 2021:955)[1]. MGS utgör ett informationssystem eftersom det *"behandlar information"* i form av säkerhetsskyddsklassificerade uppgifter. Inför driftsättningen av systemet ska verksamhetsutövaren följaktligen uppfylla de krav som framgår av SSF 2021:955, Säkerhetspolisens föreskrifter om säkerhetsskydd, (PMFS 2022:1), samt eventuella egenidentifierade krav.

Innan MGS tas i drift ska verksamhetsutövaren genom en särskild säkerhetsskyddsbedömning ta ställning till vilka säkerhetskrav i systemet som är motiverade och se till att säkerhetsskyddet utformas så att dessa krav tillgodoses. Den särskilda säkerhetsskyddsbedömningen ska dokumenteras.[2]

Verksamhetsutövare som har tilldelats MGS av Försvarsmakten kan sakna uppgifter om systemets tekniska beskaffenheter eller vilka ställningstaganden om säkerhetsskyddsåtgärder som Försvarsmakten har gjort för systemet. Avsaknaden av dessa uppgifter kan försvåra för verksamhetsutövaren att ta ställning till vilka säkerhetskrav som är motiverade och se till att säkerhetsskyddet utformas så att dessa krav tillgodoses i enlighet med säkerhetsskyddsregelverket.

Syfte

Denna vägledning innehåller flertalet bedömningar avseende vilka tekniska säkerhetskrav i 4 kap. PMFS 2022:1 som MGS uppfyller. Observera att de säkerhetskrav som framgår av tabellen i bilagan endast kan anses vara uppfyllda om verksamhetsutövaren även uppfyller de administrativa säkerhetskrav som framgår av 4 kap. PMFS 2022:1 och har tillfredsställande administrativa åtgärder på plats för att säkerställa att eventuella uppdateringar eller säkerhetsmeddelanden från Försvarsmakten omhändertas. Utöver de säkerhetskrav som framgår av tabellen i bilagan ska den särskilda säkerhetsskyddsbedömningen redovisa att alla säkerhetskrav, som framgår av 4 kap. PMFS 2022:1, är omhändertagna eller, om kravet inte är applicerbart, att det motiveras varför.

Dessa bedömningar syftar till att utgöra ett stöd för verksamhetsutövare vid framtagandet av sin särskilda säkerhetsskyddsbedömning inför driftsättning av MGS i enlighet med 3 kap. 1 § SSF 2021:955. Vägledningens innehåll kan även användas som referensunderlag vid samråd med Säkerhetspolisen inför driftsättningen av MGS.

---

1 Jfr. 1 kap. 3 § tredje stycket säkerhetsskyddsförordningen, *"ett system av sammansatt mjuk- och hårdvara som behandlar information"*. Se även Säkerhetspolisens vägledning – Informationssäkerhet (2023), s. 6.

2 3 kap. 1 § säkerhetsskyddsförordningen

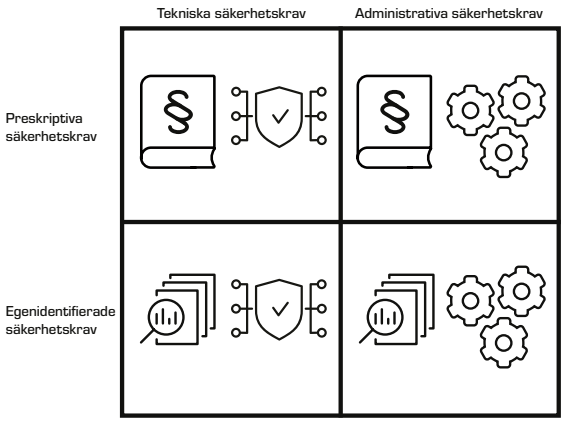
1 Säkerhetskrav i informationssystem

Notera
Denna vägledning är endast avsedd att användas för bedömningar om säkerhetskrav för MGS. Användning av MGS som går utöver signalskyddsinstruktionen omhändertas inte i tabellen i bilagan. Om verksamhetsutövaren identifierar användningsområden som går utanför det som beskrivs i signalskyddsinstruktionen behöver denna användning analyseras och bedömas i den särskilda säkerhetsskyddsbedömningen samt eventuella kompletterande åtgärder vidtas.
För mer information om säkerhetskrav för informationssystem, läs Säkerhetspolisens vägledning – Informationssäkerhet (2023).

För att tydliggöra och visualisera vilka säkerhetskrav en verksamhetsutövare ställer på sitt informationssystem kan dessa illustreras med hjälp av en så kallad fyrfältare. Säkerhetskraven kan antingen vara av teknisk eller administrativ karaktär samt preskriptiva eller egenidentifierade. Med tekniska säkerhetskrav avses sådana säkerhetskrav som tekniken omhändertar medan administrativa krav är sådana som omhändertas genom processer, rutiner, uppföljningar och kontroller.

Preskriptiva säkerhetskrav är sådana som återfinns i 4 kap. PMFS 2022:1. Egenidentifierade säkerhetskrav är sådana som verksamhetsutövaren själv identifierat som motiverade för att informationssystemets säkerhetsskydd ska kunna vidmakthållas. Denna typ av säkerhetskrav handlar typiskt sett om att säkerställa riktighet eller tillgänglighet.

Säkerhetskrav i informationssystem



Notera
Om verksamhetsutövaren har identifierat att MGS är skyddsvärt utifrån riktighets- eller tillgänglighetsperspektivet kan vägledningens bilaga användas som ett stöd även i dessa fall. Här är det viktigt att verksamhetsutövaren analyserar och bedömer hur säkerhetsskyddet ska utformas för att omhänderta de egenidentifierade säkerhetskraven som har bäring på riktighet eller tillgänglighet.

2 Samråd av signalskyddssystem

Om verksamhetsutövaren bedömer att MGS kan komma att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre ska verksamhetsutövaren skriftligen samråda med Säkerhetspolisen innan systemet tas i drift. Samrådsskyldigheten gäller även i fråga om obehörig åtkomst till systemet kan medföra en skada för Sveriges säkerhet som inte är obetydlig[3]

Notera
Även framtida signalskyddssystem som är ett informationssystem enligt 1 kap. 3 § SSF 2021:955 omfattas av kraven i säkerhetsskyddslagen och de föreskrifter som meddelats i anslutning till lagen. Det innebär att kraven i 4 kap. PMFS 2022:1 även gäller för sådana informationssystem som inte är samrådspliktiga. Informationssystem som inte är samrådspliktiga är informationssystem som hanterar säkerhetsskyddsklassificerade uppgifter i nivån begränsat hemlig eller motsvarande konsekvensnivå D.

3 3 kap. 1 och 2 §§ första och andra stycket SSF 2021:955.

3 Bilaga: Säkerhetspolisens bedömning av vilka säkerhetskrav för MGS som är omhändertagna av Försvarsmakten i enlighet med 4 kap. PMFS 2022:1

4 kap. PMFS - Informationssäkerhet i och kring informationssystem	Säkerhetspolisens bedömning av säkerhetskrav för MGS
Granskning vid utveckling och anskaffning	
1 § Verksamhetsutövaren ska se till att egenutvecklad programvara i informationssystem som har betydelse för säkerhetskänslig verksamhet granskas för att upptäcka och åtgärda säkerhetsbrister och sårbarheter.	MGS är en produkt bestående av fördefinierad hård- och mjukvara där mjukvaran inte har utvecklats av verksamhetsutövaren. Följaktligen gäller inte kravet för systemet. Verksamhetsutövaren kan hänvisa till denna vägledning i sin särskilda säkerhetsskyddsbedömning.
2 § Verksamhetsutövaren ska se till att hårdvara och tredjepartsprogramvara i informationssystem som har betydelse för säkerhetskänslig verksamhet granskas för att upptäcka och åtgärda säkerhetsbrister och sårbarheter, eller att hårdvaran och programvaran på annat sätt bedöms vara tillförlitlig från säkerhetsskyddssynpunkt.	Baserat på den tekniska dokumentationen[4] för MGS som tillgängliggjorts för Säkerhetspolisen bedömer Säkerhetspolisen att hårdvaran och tredjepartsprogramvaran är tillförlitliga ur säkerhetsskyddssynpunkt. Verksamhetsutövaren kan hänvisa till denna vägledning i sin särskilda säkerhetsskyddsbedömning.
Åtgärder inför driftsättning eller förändring	
3 § Verksamhetsutövaren ska, innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift, genomföra tester av skyddsåtgärderna. Resultatet ska jämföras med de säkerhetskrav som gäller för informationssystemet. Den särskilda säkerhetsskyddsbedömningen ska uppdateras med eventuella avvikelser och de kompensatoriska åtgärder som måste vidtas.	I den tekniska testdokumentationen för MGS som tillgängliggjorts för Säkerhetspolisen beskrivs testerna av de tekniska säkerhetsskyddsåtgärderna på ett sådant sätt att det framgår att testerna genomförts med godkänt resultat för att uppfylla kravet enligt bestämmelsen. Verksamhetsutövaren kan hänvisa till denna vägledning i sin särskilda säkerhetsskyddsbedömning avseende de tekniska säkerhetskraven. Tester av de administrativa skyddsåtgärderna enligt bestämmelsen behöver däremot genomföras av verksamhetsutövaren.

4 L1-H-07:0129, Bilaga 10 till 19 621:79821, Bilaga 2 09 621:79821, 60212/2007, L1-H-07:0130, 60213/2007, Bilaga 9 till 19 621:79821, 10 750:79837, L1-H-07:0139, 09 621:79821

Granskning av säkerheten	
6 § Verksamhetsutövaren ska årligen granska säkerheten i ett informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig eller i informationssystem som är av motsvarande betydelse för Sveriges säkerhet.	I den tekniska dokumentationen för MGS som tillgängliggjorts för Säkerhetspolisen beskrivs att granskning av säkerheten i informationssystemet sker på ett sådant sätt att det framgår att den tekniska komponenten av kravet enligt bestämmelsen uppfylls. Verksamhetsutövaren kan hänvisa till denna vägledning i sin särskilda säkerhetsskyddsbedömning avseende de tekniska säkerhetskraven. Granskning av de administrativa skyddsåtgärderna enligt bestämmelsen behöver däremot genomföras av verksamhetsutövaren.
Unika identiteter och spårbarhet	
7 § Alla utställda identiteter i ett informationssystem som har betydelse för säkerhetskänslig verksamhet ska vara unika över tid. Åtkomsten ska vara spårbar till individ, system eller resurs.	I den tekniska dokumentationen för MGS som tillgängliggjorts för Säkerhetspolisen beskrivs de tekniska säkerhetsskyddsåtgärderna på ett sådant sätt att det framgår att informationssystemet har stöd för att uppfylla kravet enligt bestämmelsen. Verksamhetsutövaren kan hänvisa till denna vägledning i sin särskilda säkerhetsskyddsbedömning avseende de tekniska säkerhetskraven. Administrativa åtgärder för att säkerställa spårbarhet enligt bestämmelsen behöver verksamhetsutövaren själv ta fram.
Autentisering m.m.	
9 § Verksamhetsutövaren ska se till att autentisering vid åtkomst till informationssystem som har betydelse för säkerhetskänslig verksamhet baseras på flera faktorer, om det inte är uppenbart obehövligt.	I den tekniska dokumentationen för MGS som tillgängliggjorts för Säkerhetspolisen beskrivs autentiseringslösningen är baserad på flerfaktorsautentisering på ett sådant sätt att Säkerhetspolisen anser att kravet enligt bestämmelsen uppfylls. Verksamhetsutövaren kan hänvisa till denna vägledning i sin särskilda säkerhetsskyddsbedömning.
Kommunikationssäkerhet	
14 § Verksamhetsutövaren ska se till att informationssystem som har betydelse för säkerhetskänslig verksamhet 1. kommunicerar på ett kontrollerat sätt med komponenter eller delsystem inom samma informationssystem, och 2. kommunicerar på ett kontrollerat sätt med informationssystem eller nätverk som inte omfattas av krav på säkerhetsskydd.	I den tekniska dokumentationen för MGS som tillgängliggjorts för Säkerhetspolisen beskrivs kommunikationssäkerheten på ett sådant sätt att Säkerhetspolisen anser att kravet enligt bestämmelsen uppfylls. Verksamhetsutövaren kan hänvisa till denna vägledning i sin särskilda säkerhetsskyddsbedömning.
15 § Verksamhetsutövaren ska se till att informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen begränsat hemlig eller konfidentiell, logiskt separeras från informationssystem eller nätverk som inte omfattas av motsvarande krav på säkerhetsskydd.	I den tekniska dokumentationen för MGS som tillgängliggjorts för Säkerhetspolisen beskrivs kommunikationssäkerheten på ett sådant sätt att Säkerhetspolisen anser att kravet enligt bestämmelsen uppfylls. Verksamhetsutövaren kan hänvisa till denna vägledning i sin särskilda säkerhetsskyddsbedömning.

16 § Verksamhetsutövaren ska se till att informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig, fysiskt separeras från informationssystem eller nätverk som inte omfattas av motsvarande krav på säkerhetsskydd.	I den tekniska dokumentationen för MGS som tillgängliggjorts för Säkerhetspolisen beskrivs kommunikationssäkerheten på ett sådant sätt att Säkerhetspolisen anser att kravet enligt bestämmelsen uppfylls. Verksamhetsutövaren kan hänvisa till denna vägledning i sin särskilda säkerhetsskyddsbedömning.
17 § Informationssystem som är separerade från andra informationssystem enligt 15 eller 16 § får genom envägskommunikation överföra data för export till eller import från andra informationssystem.	I den tekniska dokumentationen för MGS som tillgängliggjorts för Säkerhetspolisen beskrivs kommunikationssäkerheten på ett sådant sätt att Säkerhetspolisen anser att kravet enligt bestämmelsen uppfylls. Verksamhetsutövaren kan hänvisa till denna vägledning i sin särskilda säkerhetsskyddsbedömning.
Konfiguration, uppdatering och dokumentering	
18 § Verksamhetsutövaren ska för informationssystem som har betydelse för säkerhetskänslig verksamhet tillämpa konfiguration som använder lämpliga säkerhetsfunktioner, stänger av funktioner som inte används och även i övrigt reducerar sårbarheter.	I den tekniska dokumentationen för MGS som tillgängliggjorts för Säkerhetspolisen beskrivs de tekniska säkerhetsskyddsåtgärderna på ett sådant sätt att Säkerhetspolisen anser att kravet enligt bestämmelsen uppfylls. Verksamhetsutövaren kan hänvisa till denna vägledning i sin särskilda säkerhetsskyddsbedömning.
20 § Verksamhetsutövaren ska ha dokumentation som visar logiska samband och inbördes beroenden mellan komponenter som används i informationssystem som har betydelse för säkerhetskänslig verksamhet.	I systemdokumentationen för MGS som tillgängliggjorts för Säkerhetspolisen beskrivs logiska samband och inbördes beroenden mellan komponenter som används i informationssystemet på ett sådant sätt att Säkerhetspolisen anser att kravet uppfylls. Verksamhetsutövaren kan hänvisa till denna vägledning i sin särskilda säkerhetsskyddsbedömning.
Skydd mot skadlig kod	
22 § Verksamhetsutövaren ska för informationssystem som har betydelse för säkerhetskänslig verksamhet analysera behovet av och i förekommande fall besluta att använda de funktioner för skydd mot skadlig kod som är nödvändiga från säkerhetsskyddssynpunkt.	I den tekniska dokumentationen för MGS som tillgängliggjorts för Säkerhetspolisen beskrivs de tekniska säkerhetsskyddsåtgärderna på ett sådant sätt att det framgår att informationssystemet har stöd för att uppfylla kravet enligt bestämmelsen. Verksamhetsutövaren kan hänvisa till denna vägledning i sin särskilda säkerhetsskyddsbedömning.

Skydd mot obehörig förändring av informationssystem	
23 § Verksamhetsutövaren ska för informationssystem som har betydelse för säkerhetskänslig verksamhet vidta skyddsåtgärder som ger förmåga att försvåra och upptäcka obehörig förändring av informationssystemet och dess säkerhetsskydd.	I den tekniska dokumentationen för MGS som tillgängliggjorts för Säkerhetspolisen beskrivs de tekniska säkerhetsskyddsåtgärderna på ett sådant sätt att det framgår att informationssystemet är tillförlitligt ur säkerhetssynpunkt. Verksamhetsutövaren kan hänvisa till denna vägledning i sin särskilda säkerhetsskyddsbedömning.
Säkerhetsloggning	
25 § Verksamhetsutövaren ska logga händelser som kan påverka säkerheten i informationssystem som har betydelse för säkerhetskänslig verksamhet.	I den tekniska dokumentationen för MGS som tillgängliggjorts för Säkerhetspolisen beskrivs att loggning av händelser som kan påverka säkerheten i systemet sker på ett sådant sätt att Säkerhetspolisen anser att kravet enligt bestämmelsen uppfylls. Verksamhetsutövaren kan hänvisa till denna vägledning i sin särskilda säkerhetsskyddsbedömning.
27 § För informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter ska loggningen omfatta användning och ändring av behörigheter med systemadministrativ åtkomst och av roller med särskild behörighet till informationssystemet.	I den tekniska dokumentationen för MGS som tillgängliggjorts för Säkerhetspolisen beskrivs att loggningen omfattar användning och ändring av behörigheter med systemadministrativ åtkomst och av roller med särskild behörighet till informationssystemet sker på ett sådant sätt att Säkerhetspolisen anser att de tekniska aspekterna av kravet enligt bestämmelsen uppfylls. Verksamhetsutövaren kan hänvisa till denna vägledning i sin särskilda säkerhetsskyddsbedömning.
29 § Verksamhetsutövaren ska vidta åtgärder för att skydda säkerhetsloggar mot obehörig åtkomst, ändring eller förstöring.	I den tekniska dokumentationen för MGS som tillgängliggjorts för Säkerhetspolisen beskrivs att åtgärder för att skydda säkerhetsloggar mot obehörig åtkomst, ändring eller förstöring i informationssystemet sker på ett sådant sätt att det framgår att kravet enligt bestämmelsen uppfylls. Verksamhetsutövaren kan hänvisa till denna vägledning i sin särskilda säkerhetsskyddsbedömning avseende de tekniska säkerhetskraven. Administrativa åtgärder för att skydda säkerhetsloggar enligt bestämmelsen behöver verksamhetsutövaren själv ta fram.

Säkerhetspolisen

Box 12312, 102 28 Stockholm
010-568 70 00 | säkerhetspolisen@säkerhetspolisen.se
www.säkerhetspolisen.se