Sändlista sida 5

ES

Ert tjänsteställe, handläggare
Säkerhetsskyddchef, IT-säkerhetschef, Signalskyddschef

Ert datum

Er beteckning

Vårt tjänsteställe, handläggare
Carina Martinsson,
carina.x.martinsson@mil.se

Vårt föregående datum
2022-08-31

Vår föregående beteckning
FM2021-6126:1

Instruktion rörande FM TEMPEST-krav för skydd mot röjande signaler.

(3 bilagor)

1. Inledning

1.1. Syfte och omfattning

Denna instruktion beskriver de krav som ställs på informationssystem för att uppnå en godtagbar säkerhetsnivå avseende skydd mot röjande signaler.

Instruktionen omfattar informationssystem som hanterar uppgifter i säkerhetsskyddsklass konfidentiell eller högre, för nationella säkerhetsskydds-klassificerade uppgifter, Nato sekretess samt EU sekretess.

Instruktionen hanterar skyddet mot röjande signaler av elektromagnetisk karaktär. Akustiska signaler omfattas inte av denna skrivelse.

Instruktionen består av ett missiv samt tre bilagor vilka tillsammans utgör TEMPEST- kraven för skydd mot röjande signaler.

Del	Innehåll
Missiv	Bakgrund, omfattning samt beslut (Öppen)
Bilaga 1	Krav på utrustning, lokaler och dokumentation (SK)
Bilaga 2	Mall för TEMPEST-deklaration (ES)
Bilaga 3	Installationskrav och anvisningar. (BH)

Tabell 1, Upplägg kravdokument

1.2. Lagkrav

Enligt förordningen med instruktion för Försvarsmakten, SFS 2024:1333 8§ ska Försvarsmakten fullgöra uppgiften som ”*nationell tempestmyndighet i enlighet med nationella och internationella åtaganden”.*

MUST SÄKK SÄKT har i Försvarsmakten uppgiften att agera i rollen som nationell tempestmyndighet, vilket i nationella och internationella sammanhang benämns som NTA (National Tempest Authority).

Enligt Säkerhetsskyddsförordningen SFS 2021:955, 3 kap. 4§ ska en verksamhetsutövare som ansvarar för ett informationssystem *”... beakta förekomsten av röjande signaler och vidta lämpliga skyddsåtgärder för systemet om informationssystemet avses behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre*.”

Enligt Försvarsmaktens föreskrifter om säkerhetsskydd FFS 2019:2, 4 kap. 25§ ska en myndighet *”... besluta om säkerhetskrav för skydd mot röjande signaler (RÖS). Beslutet ska dokumenteras."* Denna instruktion utgör Försvarsmaktens beslutade säkerhetskrav enligt ovan.

1.3. Bakgrund

TEMPEST var ett kodord för fenomenet ”Compromising Emanations” som upptäcktes i USA under början av 1940-talet och var omgärdat av mycket hög sekretess. Kodordet lever fortfarande kvar, främst som ett öppet namn på fenomenet och de internationella regelverken för skydd mot röjande signaler.

I Sverige gavs fenomenet namnet ”Röjande signaler”, vilket brukar förkortas som RÖS.

Sverige har haft ett nationellt regelverk för RÖS som gäller för att skydda säkerhetsskyddsklassificerade uppgifter, samt tillämpat Natos regelverk för TEMPEST för att skydda Nato-sekretess. Enligt strategisk inriktning från C Must ska det svenska regelverket harmoniseras med Natos regelverk, så att samma regler för skydd mot röjande signaler ska gälla oavsett om det syftar till att skydda säkerhetsskyddsklassificerade uppgifter eller Nato-sekretess.

Genom denna instruktion är det svenska RÖS-regelverket i linje med Nato och EU TEMPEST-regelverk.

1.4. Tillämpning

Inom Försvarsmakten är denna instruktion obligatorisk för informationssystem avsedda för svensk säkerhetsskyddsklass Konfidentiell (K), Nato Confidential (NC) samt EU Confidential (EUC) eller högre.

Övriga verksamhetsutövare kan tillämpa instruktionen i rådgivande syfte såväl för att visa kravuppfyllnad med avseende på TEMPEST för informationssystem avsedda för Nato och EU sekretess samt avseende hantering av skydd mot röjande signaler för nationell sekretess.

Skyddet mot avlyssning av röjande signaler ska dimensioneras mot externa angripare, med andra ord aktörer utanför kontrollerat- eller inspekterbart område.

Informationssystem som hanterar information av svensk säkerhetsskyddsklass Begränsat hemlig, Nato Restricted samt EU Restricted berörs inte av kraven för skydd mot röjande signaler.

1.5. Ansvar

Ansvaret för skyddet mot röjande signaler ligger hos verksamhetsansvarig chef/ chefen för Organisationsenheten som en del av det generella säkerhetsskyddet. Ansvaret omfattar anskaffning av TEMPEST-verifierad utrustning, placering, installation, användning samt utbildning i enlighet med denna instruktion.

Som stöd för ansvarig chef ska en befattningshavare tilldelas rollen som ansvarig inom verksamheten med avseende på skyddet mot röjande signaler (exempelvis IT-säkerhetschef).

Den instans som TEMPEST-verifierar utrustning är ansvarig för att utrustningen har de angivna egenskaperna med avseende på röjande signaler som följer enligt denna instruktion.

Vid behov av avsteg från denna instruktion ansvarar MUST för att besluta om dessa.

2. Övergångsregler och undantag

2.1. Befintliga ackrediterade och driftsatta informationssystem

Befintliga informationssystem som är ackrediterade och driftsatta kan tills vidare omfattas av tidigare regelverk FM2021-6126:1, Försvarsmaktens säkerhetskrav för skydd mot röjande signaler (RÖS).

Vid förändringar som medför att systemet måste godkännas på nytt ur säkerhetskyddssynpunkt i enlighet med 4 kap 14§ FFS 2019:2 ska denna instruktion tillämpas för skydd mot röjande signaler istället för tidigare regelverk FM2021-6126:1.

Ett exempel på sådan förändring är när säkerhetsskyddsklassificeringen för ett system ändras.

2.2. Nyanskaffning av informationssystem

Nyanskaffning av informationssystem ska följa denna instruktion.

Fortsatt tillämpning av tidigare regelverk kan medges för system som närmar sig färdigställande och som endast hanterar svenska säkerhetsskyddsklassificerade uppgifter i klass konfidentiell eller högre. Avdömning enligt ovan ska ske av ansvarig MOAC i samråd med NTA. För att ges undantag ska tillämpning av nya regelverket orsaka omfattande åtgärder i form av kostnader och tid.

System som beviljas undantag ska tillämpa reglerna enligt kap 2.1. ovan.

Anskaffning av utrustning som uppfyller utrustningsklasserna U1 och U2 enligt det tidigare regelverket FM2021-6126:1, kan ske under en övergångsperiod på fem (5) år efter fastställandet av denna instruktion.

Installationen av utrustningen ska följa kraven i denna instruktion genom att:
- Utrustningsklass U1 ska följa kraven för utrustningsklass A_{plus}.
- Utrustningsklass U2 ska följa kraven för utrustningsklass B.

Anskaffning av U3 utrustning är inte tillåtet, utrustningen ska klassificeras om till någon av utrustningsklasserna definierade i denna instruktion.

2.3. Kontakt

Vid frågor eller avdömningsbehov kontakta NTA på Must SäkK SäkT.
Kontaktuppgifter: swe-nta@mil.se

3. Beslut

Denna instruktion börjar gälla vid fastställandedatum med övergångsregler enligt kapitel 2 i detta dokument och ersätter då tidigare beslut FM2021-6126:1.

I beredning av detta ärende har Teknisk chef Ledningssystem överstelöjtnant Christer Sandholm, chefsingenjör IT-säkerhet Ulrik Söderblom och Daniel Vikström deltagit.

Denna instruktion har beslutats av avdelningschef Erik Lyttkens**.** I den slutliga handläggningen har senior rådgivare Ove Friman deltagit och som föredragande Carina Martinsson.

Lyttkens, Erik

Chef Avdelningen för krypto- och IT-säkerhet

Handlingen är fastställd i Försvarsmaktens elektroniska dokument- och ärendehanteringssystem.

Sändlista

AST
MS
FS

Inom HKV
HKV stab
HKV FST CIO
HKV FST STÖD LOG
HKV FST RHS
HKV FST GEN UTB
HKV Operationsledningen
MUST
LedR TVK Ledsyst
FMTIS

För kännedom
Regeringskansliet, FOI, FMV, Fortifikationsverket