



**Direktiv for
sikkerhetstjenesten**

Forsvarets militære organisasjon

Grunnlagsdokumentet

Forord

Direktiv for sikkerhetstjenesten i Forsvarets militære organisasjon (FMO) er FSJ's styringsdokument for sikkerhetstjenesten innenfor FMO. Direktivet beskriver ansvar og myndighet for ledelse og utøvelse av sikkerhetstjeneste i Forsvaret i - og utenfor Norge.

Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) med forskrifter ble iverksatt 1 juli 2001. Dette regelverket innebærer en fornyet og forsterket fokus på sikkerhetstjenesten i nasjonal sammenheng og gir klare føringer for organisering og vektlegging av sikkerhetstjenesten også i Forsvaret. Samtidig er det slik at sikkerhetsloven ikke omfatter all sikkerhetstjeneste i Forsvaret. Dette direktivet gir utfyllende bestemmelser innenfor militær sikkerhetstjeneste i FMO.

Operativ virksomhet er Forsvarets primære aktivitet, men begrepet anvendes i en videre forstand enn hva vi har vært vant til tidligere. Operativ virksomhet består av operasjoner, styrkeproduksjon og logistikk. Et tilstrekkelig sikkerhetsnivå er en forutsetning for gjennomføring av all virksomhet i Forsvaret. Sikkerhetstjenesten er en kapasitet som bidrar til å nå dette målet.

FSJ har det overordnede ansvaret for all operativ virksomhet, herunder også den militære sikkerhetstjenesten. Sjefen for Forsvarets sikkerhetsavdeling (SJ FSA) er delegert det utøvende ansvaret for forebyggende sikkerhetstjeneste. SJ FSA har fra FSJ delegert utøvende, koordinerende, kontrollerende og rådgivende ansvar i sikkerhetsspørsmål.

For bortsatt virksomhet som ikke er definert som kjernevirksomhet, men som omfatter drift, utvikling og vedlikehold av sikkerhetsgraderte informasjonssystemer som igjen er kritisk for understøttelse av operativ virksomhet har FSJ det sikkerhetsmessige ansvaret. SJ FSA har, på vegne av FSJ, det utøvende ansvaret for sikkerhetstjenesten i bortsatt virksomhet som påvirker den operative evnen.

Militære sjefer har et klart ansvar for vakthold og sikring definert i Kgl res av 10 juni 1949, pkt 13b, samt FSJ's direktiv for beskyttelse mot terrorisme, pkt 5.1. Alle må vise engasjement og tilstedeværelse i utøvelsen av militært vakthold/sikkerhetstjeneste.

Direktivet beskriver nå-situasjonen, men skal også være et levende dokument som gjennom årlige revisjoner skal fange opp endringer i Forsvarets struktur, kommandoforhold og oppgaver.

Det er FSJ's mål at direktivet skal bidra til øket fokus på sikkerhet, samt bidra til klarere ansvarslinjer. En målrettet sikkerhetstjeneste som understøtter operasjoner, skal støtte Forsvarets operative behov i fred, krise, væpnet konflikt og krig – både nasjonalt og internasjonalt.



Sigurd Frisvold
General
Forsvarssjef

Innhold

Innhold	3
1 Innledning	5
1.1 BAKGRUNN.....	5
1.2 HENSIKT.....	5
2 Definisjoner	6
2.1 KRITISKE VERDIER	6
2.2 KRITISK INFORMASJON	6
2.3 KRITISK MATERIELL	6
2.4 ATTRAKTIVT MATERIELL	6
2.5 VERDIVURDERING	6
2.6 TRUSSELVURDERING	6
2.7 SÅRBARHETSVURDERING	6
2.8 RISIKOVURDERING	6
3 Forsvarets militære organisasjon	7
3.1 ORGANISASJON	7
3.2 FORSVARETS OPPGAVER	7
3.2.1 Nasjonale oppgaver.....	7
3.2.2 Oppgaver som løses i samarbeid med allierte og eventuelt andre	7
3.2.3 Andre oppgaver for Forsvaret.....	7
4 Organisering av sikkerhetstjenesten i FMO	8
4.1 VIRKSOMHETENS LEDER.....	8
4.2 FORSVARETS SIKKERHETSAVDELING.....	8
4.3 FORESATT	8
4.4 AVDELINGENS SIKKERHETSORGANISASJON	8
4.5 AVDELINGENS SIKKERHETSLEDER.....	9
4.6 DEN ENKELTE	9
4.7 SAMARBEIDSAVTALE OM SIKKERHET	9
4.8 OPERASJONER I UTLANDET	9
4.9 BORTSETTING AV VIRKSOMHET	9
4.10 SIKKERHETSREVISJON.....	10
5 Personellsikkerhet	10
5.1 KLARERINGSMYNDIGHET	10
5.2 AUTORISASJON.....	10
5.3 UFORDELAKTIGE AUTORISASJONSAVGJØRELSE	10
5.4 PERSONELLSIKKERHETSKONVOLUTTEN.....	10
5.5 TILGANG TIL PERSONKONTROLLOPPLYSNINGER	10
5.6 ELEKTRONISK BEHANDLING	10
5.7 FORSENDELSE.....	10
5.8 KLARERINGS- OG AUTORISASJONSBEVIS	11
5.9 UTENLANDSKE STATSBORGERE	11
6 Fysisk sikring	11
6.1 BYGNINGSMESSIGE TILTAK	11
6.2 NØKLER, ADGANGSKORT OG KOMBINASJONER	11
6.3 VAKTHOLD.....	11
6.4 ELEKTRONISKE SIKRINGSTILTAK	12
6.5 KAMERA/VIDEO/MOBILTELEFON/PDA	12
7 Informasjonssikkerhet	12
7.1 OVERSIKT OVER SIKKERHETSGRADERTE INFORMASJONSSYSTEMER	12
7.2 RAPPORTERINGSPLIKT	12

7.3	SYSTEMEIER.....	12
7.4	GODKJENNINGSANSVARLIG.....	12
7.5	GRADERTE INFORMASJONSSYSTEMER.....	12
7.6	HÅNDTERING AV KRYPTOMATERIELL.....	13
7.7	GRADERTE DOKUMENTER.....	13
7.8	LEKKASJE AV SKJERMINGSVERDIG INFORMASJON.....	13
7.9	INTERNASJONALE OPERASJONER.....	14
7.10	NETTVERKSOVERVÅKING.....	14
7.11	INSIDENTHÅNTERING.....	14
8	Utførelse av sikkerhetstjenesten.....	14
8.1	RISIKOHÅNTERING.....	14
8.2	LOKALT GRUNNLAGSDOKUMENT FOR SIKKERHET.....	14
8.3	SIKKERHETSETTERRETNINGER.....	15
8.4	RAPPORTERING.....	15
8.5	REAKSJONSTILTAK.....	16
8.6	ADGANGSRETT.....	16
8.7	SIKKERHETSINSPEKSJONER.....	16
8.8	VEILEDNING.....	16
8.9	BESØKSKONTROLL.....	16
8.10	INDUSTRISIKKERHET.....	17
8.11	KURERPOSTTJENESTEN I FMO.....	17
8.12	DESTRUKSJONSPLAN.....	17
8.13	SPESIELLE SIKKERHETSTILTAK.....	17
8.13.1	Tekniske sikkerhetsundersøkelser.....	17
8.13.2	Monitoring.....	17
8.13.3	Inntrengningstesting.....	17
8.13.4	Militær kontraetterretning.....	17
8.13.5	Defensive informasjonsoperasjoner.....	18
9	Tiltak.....	18

1 Innledning

Forsvarets grunnlagsdokument for sikkerhet er Forsvarssjefens (FSJ) direktiv for forebyggende sikkerhetstjeneste i Forsvarets militære organisasjon (FMO). Dokumentets virkeområde er FMO og bortsatt virksomhet som er kritisk for understøttelse av operativ virksomhet..

1.1 Bakgrunn

Sikkerhetsloven¹ trådte i kraft 1 juli 2001. Forskrift om sikkerhetsadministrasjon § 3-3 pålegger virksomheter med skjermingsverdig informasjon å ha et ajourført grunnlagsdokument for sikkerhet. I tillegg til skjermingsverdig informasjon har Forsvaret behov for å sikre kritiske verdier som kan skade Forsvaret eller det sivile samfunn hvis de faller i uriktige hender.

Et bredere og mer sammensatt risikobilde vil prege Norge i fremtiden. Utfordringene og de potensielle trusler er diffuse og kjennetegnes av glidende overganger mellom det nasjonale og det internasjonale, og mellom fred, krise, væpnet konflikt og krig. Dagens trusselaktører kan forårsake store skader ved bruk av begrensede ressurser. Intensjoner og kapasiteter kan forbli ukjent inntil sikkerhetstruende virksomhet² inntreffer. Dette aktualiserer behovet for en koordinert sikkerhetstjeneste i FMO.

Ny forsvarsstruktur med færre militære avdelinger og økt satsning på avansert teknologi for å oppnå informasjonsoverlegenhet i et fremtidig nettverksbasert forsvar, samt en stor satsing på sivil/militær samarbeid, vil stille høye krav til sikkerhetstjenesten. Sikkerhetstjenestens primære fokus er å beskytte Forsvarets kjernevirksomhet, det vil si den operative evnen.

Forsvarets operative evne vil alltid være avhengig av en rekke kritiske funksjoner. Disse kritiske funksjonene er det viktig å identifisere. Kritiske funksjoner for å kunne opprettholde operativ evne kan for eksempel utkrystallisere seg i spesielle objekter, personell, informasjon, materiell, infrastruktur, osv.

Utfordringen er å avdekke sikkerhetsmessige svakheter eller sårbarheter, se disse i forhold til en aktuell trussel og iverksette tilpassede sikkerhetstiltak i forhold til dette. Fremtidig operativ evne er avhengig av at egne sårbarheter blir identifisert og tatt hensyn til før en motstander evner å utnytte dem til sin fordel.

1.2 Hensikt

Forsvarets grunnlagsdokument for sikkerhet skal bidra til en enhetlig og effektiv sikkerhetstjeneste i FMO. Dokumentet skal ivareta sikkerhetslovens krav til forebyggende sikkerhetstjeneste, samt Forsvarets behov for beskyttelse av attraktivt materiell mot kriminalitet. Dokumentet gjelder i fred, krise og krig, samt for militære avdelinger i utlandet.

Sjefsforankring og samordning av sikkerhetstjenesten i FMO skal gjøre avdelingssjefer bedre rustet til å møte et dynamisk trusselbilde. Kunnskap om risikohåndtering og en klargjøring av gjeldende regelverk, skal sette FMO i stand til å beskytte sine kritiske verdier på en trygg og forsvarlig måte.

Etterretningstjenestens (E-tjenesten) spesielle karakter og sensitive virksomhet gjør at E-tjenesten er unntatt fra bestemmelsene i pkt 4.10, 5.8, 7.4, 8.9 og 8.10.

E-tjenesten er også unntatt fra bestemmelsene i punkt 4.8, 4.9, 7.1, 7.2, 7.10, 8.7, 8.13.1, 8.13.2 og 8.13.3 når det er krav om nøkkelordautorisasjon for tilgang eller adgang, samt for informasjon og fysiske områder som gjelder samarbeidende tjenester og annen særlig sensitiv virksomhet.

Det faktum at E-tjenesten er unntatt disse bestemmelsen frigjør ikke FSJ behov for kontroll med E-tjenesten. FSJ eller den FSJ bemyndiger (normalt personell ved Forsvarets sikkerhetsavdeling) kan kontrollere E-tjenesten på de punktene de er unntatt i dette dokument.

¹ Lov av 20 mars 1998 nr 10 om forebyggende sikkerhetstjeneste

² Sikkerhetsloven § 3

2 Definisjoner

2.1 Kritiske verdier

Med kritiske verdier forstås kritisk informasjon, kritisk materiell og objekter. Tap av kritiske verdier vil skade Forsvarets virksomhet, omdømme og samfunnet for øvrig.

2.2 Kritisk informasjon

Med kritisk informasjon forstås skjermingsverdig informasjon og opplysninger om rutiner og andre indikatorer som kan utnyttes av en motstander for å få tilgang til eller skade kritiske verdier. Kritisk informasjon omfatter også informasjonsbærere som dokumenter, personell og informasjonssystemer.

2.3 Kritisk materiell

Med kritisk materiell forstås operativt materiell, særlig farlig materiell³, farlig materiell og attraktivt materiell.

2.4 Attraktivt materiell

Med attraktivt materiell forstås ettertraktet eller lettomsettelig materiell som kan være mål for vinningskriminalitet eller organisert kriminalitet.

2.5 Verdivurdering

Med verdivurdering forstås prosessen med å utlede en oversikt over hvilke verdier som skal beskyttes. Prosessen med å bestemme hva som er beskyttelsesverdig i forhold til operativ evne og hensynet til rikets sikkerhet er grunnleggende.

2.6 Trusselvurdering

Med trusselvurdering forstås prosessen med å kartlegge trusselaktører, deres intensjoner og kapasiteter.

2.7 Sårbarhetsvurdering

Med sårbarhetsvurdering forstås prosessen med å avdekke egne sårbarheter som en trusselaktør kan utnytte for å få tilgang til kritiske verdier.

2.8 Risikovurdering

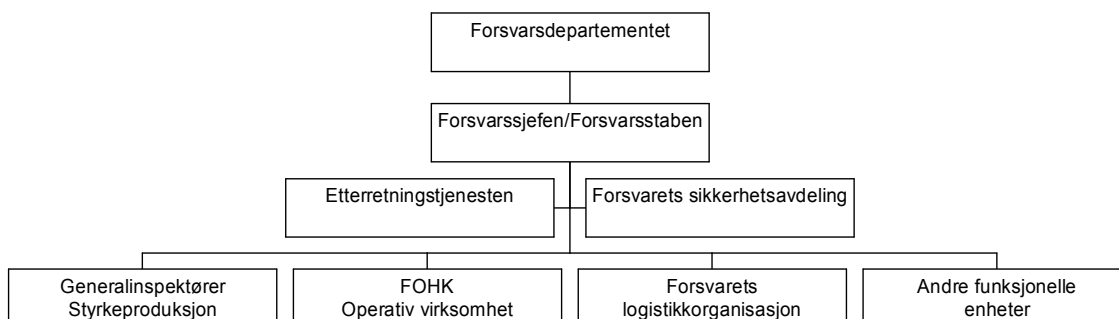
Med risikovurdering forstås prosessen som ligger til grunn for å fastslå områder hvor trusler kan utnytte sårbarheter for å få tilgang til kritiske verdier. Fastsetting av risiko er en delvis rasjonell beslutning siden ikke all relevant informasjon er kjent i beslutningsøyeblikket. Følgelig er en risikovurdering en kontinuerlig prosess der nye forutsetninger vil endre risikobildet.

³ Forsvarssjefens direktiv for sikring av Forsvarets materiell, Forsvarets overkommando, 14. des 1990

3 Forsvarets militære organisasjon

3.1 Organisasjon

FSJ er etatssjef for Forsvarets militære organisasjon (FMO) som vist i figur 1.



Figur 1: Forsvarets militære organisasjon

FSJ er delegert alminnelig kommando over all militær virksomhet i Forsvaret. Sjef Fellesoperativt hovedkvarter (FOHK) delegeres operativ kommando/kontroll over tildelte styrker. Ansvar for alliert trening i Norge tilligger FOHK.

FSJ organiserer styrkeproduksjon under Generalinspektører og logistikkvirksomhet under Forsvarets logistikkorganisasjon.

3.2 Forsvarets oppgaver

Forsvaret skal fremstå som en relevant og troverdig aktør i det samlede samfunnssikkerhetsarbeidet. Forsvaret skal kunne bidra til å forebygge og bekjempe anslag og angrep mot landets befolkning, infrastruktur og ledelseskapasitet, herunder anslag og angrep av asymmetrisk karakter.

Bekjempelse og forebygging av terror på norsk territorium er en politioppgave. Forsvaret bistår etter anmodning om støtte. Forsvaret skal støtte det sivile samfunn med grunnlag i gjeldende lover og forskrifter.

3.2.1 Nasjonale oppgaver

- å sikre et nasjonalt beslutningsgrunnlag gjennom tidsmessig overvåkning og etterretning
- å håndheve norsk suverenitet
- å ivareta norske myndighetsutøvelse på avgrensede områder
- å forebygge og håndtere episoder og sikkerhetspolitiske kriser i Norge og norske områder

3.2.2 Oppgaver som løses i samarbeid med allierte og eventuelt andre

- å bidra til kollektivt forsvar av Norge og øvrige deler av NATO mot trusler, anslag og angrep, inkludert bruk av masseødeleggelsesvåpen.
- å bidra til flernasjonalt krisehåndtering, herunder flernasjonale fredsoperasjoner

3.2.3 Andre oppgaver for Forsvaret

- å bidra med militær støtte til diplomati og til å forhindre spredning av masseødeleggelsesvåpen.
- å bidra til ivaretagelse av samfunnssikkerhet og andre sentrale samfunnsoppgaver.

Strukturen i det reviderte nasjonale beredskapssystemet⁴ er tilpasset NATO's krisehåndteringssystem (NATO Crisis Response System – NCRS) for å gi økt evne til samvirke med våre allierte og andre nasjoner ved en krise.

4 Organisering av sikkerhetstjenesten i FMO

I henhold til Sikkerhetsloven § 5 plikter forvaltningsorganer å utøve forebyggende sikkerhetstjeneste. Ansvar påhviler lederen for virksomheten. Dersom utøvende funksjoner delegeres internt i virksomheten, skal dette gjøres skriftlig.

4.1 Virksomhetens leder

FSJ er virksomhetens leder for FMO. Ansvar og oppgaver som fremgår av Sikkerhetsloven faller dermed på ham.

4.2 Forsvarets sikkerhetsavdeling

Utøvende ansvar for forebyggende sikkerhetstjeneste er delegert av FSJ til SJ FSA⁵. SJ FSA er sikkerhetsleder i henhold til Forskrift om sikkerhetsadministrasjon § 2-5 i FMO. Han skal utøve sikkerhetstjeneste i FMO, samt koordinere, gi råd og kontrollere sikkerheten som foresatte og den enkelte er ansvarlig for. FSA skal være dimensjonert for å løse FSJ sikkerhetsbehov.

På bakgrunn av innrapporterte sikkerhetstruende hendelser, skal FSA utarbeide et oppdatert situasjonsbilde på sikkerhetstilstanden i FMO. Endringer i situasjonsbildet skal rapporteres til avdelingene slik at disse har et best mulig grunnlag for å møte endringer i trusselbildet.

SJ FSA er fagmyndighet for sikkerhetsutdanning i FMO. FSA skal holde oversikt over den sikkerhetsfaglige kompetansen i FMO og sørge for at opplæring blir gjennomført slik at kompetanse innen sikkerhetstjeneste utvikles og vedlikeholdes.

SJ FSA skal representere FSJ i Forsvarets samarbeid med Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM) i sikkerhetssaker og sørge for at forholdene fra Forsvarets side blir tilrettelagt for et effektivt og godt samarbeid sentralt, regionalt og lokalt.

I sikkerhetssaker innen Forsvaret hvor Politiet er ansvarlig for etterforskningen, skal SJ FSA sørge for nødvendig bistand. I sikkerhetssaker utenfor Forsvaret hvor Politiets sikkerhetstjeneste (PST) ønsker militær bistand, skal SJ FSA bidra til at nødvendig støtte blir gitt, og at arbeidet innen Forsvaret blir koordinert.

FSA skal koordinere all virksomhet som retter seg mot NSM's virkeområde.

4.3 Foresatt

Enhver sjef i Forsvaret er foresatt⁶ i sikkerhetslovens betydning.

4.4 Avdelingens sikkerhetsorganisasjon

Avdelingssjefer ved Driftsenhet i Forsvaret (DIF), bataljon, fartøy, distrikt og baser⁷ skal etablere sikkerhetsfunksjoner i henhold til Forskrift om sikkerhetsadministrasjon og dette direktiv. Øvrige avdelinger som disponerer kritiske verdier skal også etablere sikkerhetsfunksjoner i egen avdeling.

Avdelingens sikkerhetsorganisasjons faglige og antallsmessige omfang skal dimensjoneres i forhold til avdelingens behov for sikring av kritiske verdier. Sikkerhetsorganisasjonen skal ha oversikt over den totale sikkerhetstilstanden ved avdelingen, være i stand til å gjennomføre

⁴ Nasjonalt beredskapssystem(NBS) består av sivilt beredskapssystem(SBS) og beredskapssystem for Forsvaret(BFF)

⁵ Instruks for sjefen for Forsvarets sikkerhetsavdeling, fastsatt av FSJ 15 oktober 2004

⁶ Forskrift om sikkerhetsadministrasjon § 2-2

⁷ IVB 2005-2008, skisserer baser i FMO

verdivurdering, avdekke sårbarheter og forestå tilfredsstillende sikkerhetstiltak. All sikkerhetstjeneste ved avdelingen må derfor koordineres.

4.5 Avdelingens sikkerhetsleder

Sikkerhetsleder utpekes av avdelingssjef. Sikkerhetslederen skal være faglig kvalifisert⁸, og ha nødvendig myndighet i avdelingen. Det anses som avgjørende at alder og grad gjenspeiler krav til myndighet og kvalifisering. Relativt ungt og uerfarent personell skal som hovedregel ikke benyttes i rollene.

Med ”faglig kvalifisert” menes fagutdanning og erfaring innen forebyggende sikkerhetstjeneste.

Med ”nødvendig myndighet” menes at vedkommende har autoritet gjennom alder, gradsnivå og personlige egenskaper, samt være tillagt formell myndighet knyttet til utøvelse av sikkerhetstjenesten.

Sikkerhetsleder skal gjennomføre praktisk tilrettelegging i forbindelse med klarering og autorisasjon.

Sikkerhetsleder skal utarbeide kompetanseplan som viser hvordan nøkkelpersonell skal få nødvendig opplæring for å fylle roller i egen sikkerhetsorganisasjon.

4.6 Den enkelte

Faste og midlertidig ansatte, vernepliktige mannskaper samt innleid personell i FMO skal gis opplæring og i sitt daglige virke medvirke til en effektiv sikkerhetstjeneste.

4.7 Samarbeidsavtale om sikkerhet

Der hvor flere avdelinger er lokalisert til en felles base, påhviler det alle stedlige avdelingssjefer å inngå en gjensidig samarbeidsavtale om sikkerhet. Samarbeidsavtalen⁹ skal fastsette en avdelingssjef som er ansvarlig for å lede sikkerhetstjeneste ved basen. Hensikten med samarbeidsavtalen er å sikre en helhetlig og koordinert sikkerhetstjeneste.

Dersom det ikke oppnås enighet lokalt løftes saken til FSA som på vegne av FSJ utpeker ansvarlig avdelingssjef for sikkerhetstjenesten ved basen.

4.8 Operasjoner i utlandet

Personell til sikkerhetsrelaterte stillinger til direkte støtte for norsk kontingentsjef (NCC), senior norsk representativ eller norske sjefer på brigadenivå og høyere skal godkjennes av SJ FSA før beordring.

Personell i feltsikkerhetslag eller tilsvarende, som kan benyttes til innhenting av sikkerhetsetterretninger for norske sjefer nevnt overfor skal godkjennes av SJ FSA før beordring.

4.9 Bortsetting av virksomhet

Virksomheter i Forsvaret som ikke er definert som kjernevirksomhet kan bli konkurranseutsatt og bortsatt til private aktører eller andre deler av offentlig sektor

Dersom bortsatt virksomhet faller inn under virkeområdet for Sikkerhetsloven med Forskrifter eller andre gjeldende sikkerhetsbestemmelser for FMO, skal leverandøren etablere en sikkerhetsorganisasjon som tilfredstiller FMO's krav til sikkerhet. Slike krav til sikkerhet skal spesifiseres i kontrakten og være en del av kontraktsforhandlingene før underskrift.

FSA eller den SJ FSA bemyndiger skal stille krav til sammensettingen av en slik sikkerhetsorganisasjon og at sikkerhetskrav spesifisert i kontrakter tilfredstiller FMO's krav til sikkerhet. Unntak fra dette krav kan kun avgjøres av FSA.

⁸ Forskrift om sikkerhetsadministrasjon § 3-2 tredje ledd

⁹ Vedlegg C

4.10 Sikkerhetsrevisjon

Avdelingssjefer som nevnt i pkt 4.4 skal som ledd i egenkontroll foreta en årlig gjennomgang av egen sikkerhetstjeneste. Rapport etter egenkontroll (bør inneholde registrerte sikkerhetstruende hendelser, status egen sikkerhetstjeneste og sjefens vurdering av egne sikkerhetsutfordringer) skal sendes FSA innen januar¹⁰.

5 Personellsikkerhet

5.1 Klareringsmyndighet

FSA er klareringsmyndighet for FMO opp til og med nivå STRENGT HEMMELIG, unntatt for Etterretningstjenesten.

5.2 Autorisasjon

Tilgang til gradert informasjon gradert BEGRENSET kan gis etter utfylling av taushetserklæring og autorisasjon. Tilgang til informasjon gradert KONFIDENSIELT eller høyere kan gis etter forutgående klarering og autorisasjon. Avdelingssjefer gis autorisasjonsmyndighet for eget personell. Avdelingssjefer med autorisasjonsmyndighet er ansvarlig for at det gjennomføres autorisasjonssamtale før personell gis tilgang til gradert informasjon. Avdelingssjefer kan delegere autorisasjonsmyndighet videre innenfor egen organisasjon, dette skal gjøres skriftlig. Avdelingssjef skal forvise seg om at medarbeidere som er betrodd tilgang til gradert informasjon er skikket til å håndtere disse på en troverdig og forsvarlig måte.

5.3 Ufordelaktige autorisasjonsavgjørelser

Ved ufordelaktig autorisasjonsavgjørelse vedrørende tilgang til skjermingsverdig informasjon skal klareringsmyndigheten underrettes skriftlig med begrunnelse for avgjørelse. Klareringsmyndigheten vil på bakgrunn av dette foreta en ny vurdering av personens sikkerhetsmessige skikkethet. Dersom klareringsmyndigheten opprettholder klareringsavgjørelsen, kan ikke autoriserende myndighet tilbakekalle eller nedsette autorisasjonen på bakgrunn av de forhold som har vært vurdert av klareringsmyndigheten.

5.4 Personellsikkerhetskvolutten

Følgende dokumenter skal oppbevares i personellsikkerhetskvolutten (X-0136/2)¹¹:

- Original personopplysningsblankett (X-0136/1 B/N Godkj. 10-00)
- Taushetserklæring (X-0138 B/N Godkj. 06-01)
- Klareringsbevis (X-0139 B/N Godkj. 12-96 eller X-0139 B/N Godkj. 08-02)
- Annen sikkerhetsmessig relevant informasjon

5.5 Tilgang til personkontrollopplysninger

Tilgang til personkontrollopplysninger skal BARE gis til personell med tjenstlig behov som er særskilt utpekt til dette¹². Opplysningene SKAL oppbevares og journalføres separat fra andre arkivdokumenter, og sikres fysisk i samsvar med Forskrift om Informasjonssikkerhet Kap. 6.

5.6 Elektronisk behandling

Doculive eller FISBasis skal IKKE benyttes ved anmodning om sikkerhetsklarering/personkontroll eller ved oversendelse av særskilte personopplysninger som faller inn under den særskilte graderingen: "BEGRENSET-PERSONKONTROLL".

5.7 Forsendelse

Personkontrollopplysninger skal sendes i dobbel konvolutt. Den ytre skal adresseres til den respektive virksomhet, og den indre merkes: "BEGRENSET-PERSONKONTROLL"¹³

¹⁰ Direktiv for sikkerhetsrapportering pkt 8.10

¹¹ Forskrift om Personellsikkerhet § 6-3

¹² Forskrift om Personellsikkerhet § 6-4

¹³ Forskrift om Personellsikkerhet § 6-7

5.8 Klarerings- og autorisasjonsbevis

Klareringsbevis, herunder NATO SECURITY CLEARANCE CERTIFICATE (blanket X-0140/1 E, Appendix 1 to AC/35 – D/2000), kan kun utstedes av klareringsmyndigheten.

Autorisasjonsbevis, herunder CERTIFICATE OF SECURITY CLEARANCE (Appendix 2 to Annex to AC/35 - D/2000), kan utstedes av lokal sikkerhetsoffiser etter forutgående verifisering av gyldig sikkerhetsklarering og autorisasjon.

5.9 Utenlandske statsborgere

Anmodning om klarering av utenlandske statsborgere skal begrunnes særskilt i eget skriv til Forsvarsdepartementet (FD). Dette gjelder også for personer med dobbelt statsborgerskap.¹⁴

FSA skal kun behandle anmodninger der personen har dobbelt statsborgerskap og ikke kan si fra seg det andre statsborgerskapet.¹⁵

Avdelinger, leverandører og bortsatt virksomhet skal fremlegge en særskilt begrunnelse for at sikkerhetsklarering av utenlandsk personell skal finne sted.

Først når klarering foreligger kan personen autoriseres for skjermingsverdig informasjon.

6 Fysisk sikring

Det påligger avdelingssjef å sørge for tilfredsstillende fysiske sikringstiltak for å beskytte avdelingens kritiske verdier mot uautorisert tilgang, kompromittering, tyveri og sabotasje. Tiltakene skal være basert på en lokal risikovurdering ut over minimumskrav gitt i gjeldende bestemmelser¹⁶. Hensikten med tiltakene skal være å forhindre, detektere og iverksette reaksjonstiltak.

Fysisk sikring omfatter bygningsmessige tiltak, vakthold og elektroniske sikringstiltak.

6.1 Bygningsmessige tiltak

Objekter for oppbevaring og behandling av kritiske verdier skal ha en fysisk styrkegrad mot inntrengning som tilfredsstillende kravene i gjeldende bestemmelser¹⁷.

6.2 Nøkler, adgangskort og kombinasjoner

Nøkler, adgangskort og kombinasjoner skal gis samme grad av beskyttelse som kreves for verdiene de gir tilgang til.

All utlevering av nøkler, adgangskort og kombinasjoner samt skifte av kombinasjoner til kritiske verdier skal registreres. Opptelling av nøkler, adgangskort og kombinasjoner samt skifte av kombinasjoner skal gjennomføres regelmessig og minimum hver sjette måned¹⁸.

6.3 Vakthold

Det skal normalt være militær vakt¹⁹ ved Forsvarets baser. Militær vakt er bevæpnet iht instruks. Militær vakt skal være under ledelse av militær befalingsmann. Skriftlig vaktinstruks skal foreligge og være gjort kjent for vaktmannskapene. Militær vakt skal være i stand til å utføre adgangskontroll, patruljering, rapportering og anvende tildelte maktmidler.

I de tilfeller der militær virksomhet ikke blir sikret av militær vakt, men av en annen type vakt, skal SJ FSA underrettes om dette. SJ FSA skal vurdere om kvaliteten/kompetansen på denne type vakt er i overensstemmelse med sikkerhetskravene i FMO.

¹⁴ Forskrift om personellsikkerhet § 3-3.

¹⁵ Forskrift om personellsikkerhet § 2-2

¹⁶ Vedlegg A: Gjeldende bestemmelser

¹⁷ Forsvarssjefens direktiv for sikring av Forsvarets materiell, Forsvarets overkommando, 14. des 1990, samt Retningslinjer for tjenestefeltet eiendommer, bygg og anlegg, FD 6 september 2004 og Norsk Standar 3454

¹⁸ Sikkerhetsloven, Forskrift om informasjonssikkerhet, § 6-16.

¹⁹ Forskrift om utøvelse av politimyndighet i det militære Forsvar, pkt 4.

6.4 Elektroniske sikringstiltak

Elektroniske sikringstiltak skal benyttes til sikring av særlig farlig materiell²⁰, og for å forsterke sikringen av øvrige kritiske verdier hvor vaktstyrken ikke er dimensjonert for umiddelbar deteksjon av anslag og forsøk på anslag. Elektroniske sikringssystemer i tilknytning til en Driftsenhet i Forsvaret (DIF), bataljon, fartøy, distrikt eller base skal termineres hos lokal vakt.

Sjef FSA er fagmyndighet²¹ for elektronisk sikring i FMO.

6.5 Kamera/Video/Mobiltelefon/PDA

Avanserte informasjons- og kommunikasjonssystemer er blitt hver manns eie. For å hindre at gradert informasjon blir kompromittert og at liv og helse settes i fare, er det nødvendig å regulere bruken av slikt utstyr. Utstyr er her definert som alt kommersielt utstyr med sender/mottakermuligheter, samt utstyr som behandler lyd og bilde.

All bruk av kommersielt utstyr innebærer en sikkerhetsrisiko og skal begrenses til et minimum. Bruk av slikt utstyr skal reguleres og inngå i avdelingenes grunnlagsdokument for sikkerhet.

Bruk av privat utstyr til formidling av gradert informasjon er ikke tillatt.²²

7 Informasjonssikkerhet

7.1 Oversikt over sikkerhetsgraderte informasjonssystemer

FSA skal holde à jour en oversikt over alle sikkerhetsgraderte informasjonssystemer i FMO. Oversikten skal omfatte systemnavn, systemeier, sikkerhetsgradering, operasjonsmåte og kryptoforbindelser.

7.2 Rapporteringsplikt

Systemeier er rapporteringspliktig til FSA ved anskaffelse, endring av systemeierskap, sikkerhetsgradering, operasjonsmåte og ved avhending.

7.3 Systemeier

Ved anskaffelse av sikkerhetsgraderte informasjonssystemer skal den enhet som iverksetter anskaffelse utpeke systemeier.

FSA skal godkjenne systemeiere for sikkerhetsgraderte informasjonssystemer.

7.4 Godkjenningsansvarlig

Godkjenningsansvarlig for sikkerhetsgraderte informasjonssystemer er Nasjonal Sikkerhetsmyndighet (NSM) eller virksomhetens leder²³.

FSA eller den SJ FSA bemyndiger sikkerhetsgodkjenner informasjonssystemer i FMO hvor virksomhetens leder er godkjenningsansvarlig²⁴ og iht myndighet delegert fra NSM .

FSA fastsetter krav til dokumentasjon av sikkerhetstiltak i de tilfeller hvor virksomhetens leder er godkjenningsansvarlig.

Den kontraktmessige delen av anskaffelsen av sikkerhetsgraderte informasjonssystemer ivaretas av merkantilt personell og jurister. Sikkerhetskrav og spesifisering av disse i kontraktene skal kontrolleres/godkjennes av FSA eller den SJ FSA bemyndiger.

7.5 Graderte informasjonssystemer

FISBasis er gitt, iht midlertidig godkjenning av Nasjonal Sikkerhetsmyndighet (NSM), sikkerhetsgodkjenning for behandling av informasjon til og med BEGRENSET / NATO

²⁰ Forsvarssjefens direktiv for sikring av Forsvarets materiell, Forsvarets overkommando, 14. des 1990

²¹ Forsvarets strategiske direktiv for operativ virksomhet, vedlegg A.

²² Forskrift om informasjonssikkerhet § 5-18.

²³ Forskrift om informasjonssikkerhet § 5-16

²⁴ Forskrift om informasjonssikkerhet § 5-16

RESTRICTED. Informasjon som er gradert skal merkes²⁵ (topptekst/bunntekst) av usteder og gjentas under hele mailrekken.

FISBasis INTRANETT er basert på NEED TO KNOW – prinsippet. Dette vil si at gradert informasjon nevnt overfor skal bare kunne leses av de som har behov (ansatte ved en base).

DOCULIVE, en applikasjon på FISBasis, skal forholde seg som nevnt overfor. Journalføring av dokumenter opp til og med HEMMELIG utføres i Doculive. Dokumenter (selve dokumentet) gradert KONFIDENSIELT og høyere skal ikke legges inn i Doculive.

NORCCIS II er gitt, iht Sikkerhetsloven, sikkerhetsgodkjenning for behandling av informasjon gradert opp til og med HEMMELIG / NATO SECRET. All informasjon som lagres og behandles på systemet skal kunne frigis til NATO.

NORDIS-S (FISBasis HEMMELIG/NATO SECRET) er et partisjonert informasjonssystem som kan behandle gradert informasjon opp til og med HEMMELIG / NATO SECRET separat. Informasjon som lagres og behandles på systemet skal forholde seg til et skille mellom nasjonal gradering og NATO gradering. Nasjonal gradering på informasjon som ikke kan deles med NATO vil tilsi at informasjonen ikke kan lagres eller behandles på NATO delen av systemet.

7.6 Håndtering av kryptomateriell

FSA fastsetter krav til håndtering av kryptomateriell i FMO i samsvar med gjeldende regelverk²⁶.

7.7 Graderte dokumenter

Graderte dokumenter på nivå KONFIDENSIELT eller høyere i form av papirkopi, disketter, CD, minnebrikke etc stiller avdelingene overfor sikkerhetsmessige utfordringer.

Avdelingssjefer som definert i pkt 4.4 skal utpeke en informasjonsforvalter i egen avdeling som holder kontroll med avdelingens graderte dokumenter på dette nivået.

7.8 Lekkasje av skjermingsverdig informasjon

Forsvaret er avhengig av at forsvarets personell evner å unngå lekkasjer av skjermingsverdig informasjon. Derfor er Forsvaret helt avhengige av medarbeidere med personlig integritet og lojalitet.²⁷

Når informasjon²⁸ må beskyttes av sikkerhetsmessige grunner (skjermingsverdig informasjon) skal den sikkerhetsgraderes.²⁹

Enhver som får tilgang til sikkerhetsgradert informasjon som ledd i arbeid, oppdrag eller verv plikter å hindre at uvedkommende får kjennskap til informasjonen.³⁰

Enhver plikter å hindre at andre får adgang eller kjennskap til opplysninger om tekniske innretninger og fremgangsmåter, samt drifts- og forretningsforhold, som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den opplysningen angår.³¹ Med drifts- og forretningsforhold menes her interne prosesser og saksbehandling i Forsvaret.

Taushetsplikten gjelder også etter at vedkommende har avsluttet tjenesten, arbeidet, oppdraget eller vervet.³²

²⁵ Forskrift om informasjonssikkerhet § 4-1 til 4-6

²⁶ AMSG 293 og Forskrift om informasjonssikkerhet kapittel 7

²⁷ Forsvarets verdigrunnlag s 15

²⁸ Sikkerhetsloven § 8 nr 7

²⁹ Sikkerhetsloven § 11

³⁰ Sikkerhetsloven §12.

³¹ Forvaltningsloven §13 og Forskrift om offentlige anskaffelser § 3-3.

³² Sikkerhetsloven § 12.

Lekkasjer skal rapporteres som sikkerhetstruende hendelser iht til dette direktiv . Etterforskning av lekkasjen skal vurderes i hvert enkelt tilfelle.

7.9 Internasjonale operasjoner

FSA skal utføre kontroll og veiledning før avdelinger deployerer til internasjonale operasjoner. Normalt utøves dette ved den siste øvelsen der avdelingens kommandoplass er fullt oppsatt.

Kontroll- og veiledningen skal omfatte operasjonssikkerhet (OPSEC), informasjonssikkerhet (INFOSEC) og emisjonssikkerhet (EMSEC).

OPSEC omhandler verdivurdering, trusselvurdering, sårbarhetsvurdering og risikofastsettelse. INFOSEC omhandler sårbarhetsundersøkelser av informasjonssystemer, konfigurasjonskontroll, overvåking og insidenthåndtering. EMSEC som omhandle kartlegging av kompromitterende elektromagnetisk stråling.

Denne kontroll og veiledning i regi av FSA skal lede frem til konkrete anbefalinger og pålegg om endringer av operative og tekniske sikkerhetsprosedyrer. Dette danner grunnlaget for avdelingens sikkerhetsdokumentasjon før utreise og er en del av nødvendig sikkerhetsgodkjenning før utreise fra Norge.

7.10 Nettverksovervåking

FSA eller den SJ FSA bemyndiger kan iverksette undersøkelser av militære nettverk i forbindelse med en sikkerhetstruende hendelse. Konkret omfatter overvåkingen innsamling og analyse av data fra brannmurer, IDS`er, systemlogger, antivirusprogrammer og andre sensorer.

Hensikten med denne virksomheten er å beskytte Forsvarets kritiske informasjonsinfrastruktur mot angrep som innfiltrasjon, manipulering, kompromittering og tjenestenekning.

7.11 Insidenthåndtering

FSA eller den SJ FSA bemyndiger skal lede oppdrag der kartlegging av omstendighetene rundt sikkerhetstruende hendelser og annet uhjemlet bruk av forsvarets informasjonssystemer har forekommet.

8 Utførelse av sikkerhetstjenesten

8.1 Risikohåndtering

Avdelingssjef skal utøve kontinuerlig risikohåndtering. Risikohåndtering er å fastsette, iverksette, gjennomføre og kontrollere sikkerhetstiltak etter en risikovurdering. Risikovurderingen skal gjennomføres med utgangspunkt i en verdivurdering og omfatte trusselvurdering og sårbarhetsvurdering som grunnlag for å fastsette risiko. Fastsatte sikkerhetstiltak skal dokumenteres og uttrykkes i avdelingens grunnlagsdokument for sikkerhet.

8.2 Lokalt grunnlagsdokument for sikkerhet

Avdelinger med plikt til å etablere lokal sikkerhetsorganisasjon jf pkt 4.4 skal utarbeide eget grunnlagsdokument for sikkerhet.

Grunnlagsdokument for sikkerhet³³ skal omfatte:

- Organisasjon
- Operasjonskonsept
- Sikkerhetsorganisasjon
- Personellsikkerhet
- Kritiske verdier
- Fysisk sikring

³³ Vedlegg B: Mal for avdelingens grunnlagsdokument for sikkerhet

- Tilgangskontroll
- Sikkerhetsdokumentasjon
- Kryptoforvaltningsorganisasjon når avdelingen disponerer kryptomateriell

8.3 Sikkerhetsetterretninger

FSA skal med utgangspunkt i innrapporterte sikkerhetstruende hendelser fra avdelinger i FMO samt informasjon fra samarbeidende tjenester utarbeide sikkerhetsetterretninger og sikkerhetsvurderinger. Sikkerhetsetterretninger forstås i denne sammenheng som informasjon om potensielle trusselaktører.

Sikkerhetsetterretninger skal tilføres lokale sikkerhetsorganisasjoner og benyttes som grunnlag for den lokale risikovurderingen.

Gjennom samarbeid, bedret informasjonsflyt og et felles situasjonsbilde, skal den totale sikkerheten i FMO styrkes.

8.4 Rapportering

Rapportering³⁴ er en forutsetning for en effektiv forebyggende sikkerhetstjeneste. Det påhviler derfor den enkelte sjef for avdeling, fartøy og base et særskilt ansvar for å rapportere sikkerhetstruende hendelser³⁵ samt forsøk på og gjennomføring av tyveri og annen kriminell virksomhet rettet mot kritiske verdier.

Lokal sikkerhetsleder skal rapportere sikkerhetstruende hendelser, samt forsøk på og gjennomføring av tyveri og annen kriminell virksomhet rettet mot kritiske verdier, tjenestevei og med kopi til FSA innen 24 timer.

Ved kompromittering eller mistanke om kompromittering av nasjonalt kryptomateriell skal lokal kryptosikkerhetsleder rapportere hendelsen til Nasjonal sikkerhetsmyndighet (NSM)³⁶ med kopi til FSA.

Ved kompromittering eller mistanke om kompromittering av NATO kryptomateriell skal lokal kryptosikkerhetsleder rapportere hendelsen i henhold til NATO's publikasjon AMMSG 600 med kopi til Nasjonal sikkerhetsmyndighet (NSM)³⁷ og FSA.

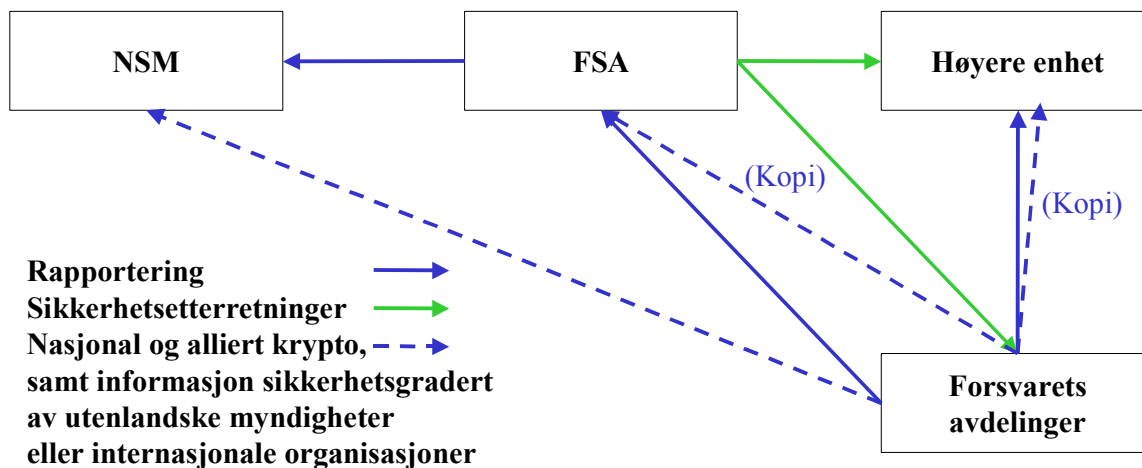
FSA skal rutinemessig orientere NSM om sikkerhetstruende hendelser i FMO.

³⁴ FSJ rapporteringsdirektiv av 1 mars 2004 samt Direktiv om sikkerhetsrapportering av 1 april 2004

³⁵ Sikkerhetsloven, Forskrift om sikkerhetsadministrasjon, §1-2, pkt 2.

³⁶ Forskrift om informasjonssikkerhet §7-45

³⁷ Forskrift om informasjonssikkerhet §7-45



Figur 2: Rapportering og sikkerhetsetterretning

8.5 Reaksjonstiltak

Reaksjonstiltak omfatter utrykning, observasjon, pågrepelse, rapportering, samt reetablering og forsterkning av sikkerhetstiltak. Avdelingene skal forberede reaksjonstiltak gjennom å utarbeide reaksjonsplaner for potensielle sikkerhetstruende hendelser og anslag mot andre kritiske verdier identifisert gjennom lokal risikovurdering. Tiltakene skal øves regelmessig.

Avdelingssjef med sikkerhetsansvaret pålegges å utarbeide lokalt planverk for anti-terroriltak.³⁸

8.6 Adgangsrett

NSM skal gis uhindret adgang til ethvert område i FMO hvor skjermingsverdig informasjon eller objekt befinner seg³⁹.

FSA skal gis uhindret adgang til ethvert område i FMO hvor kritiske verdier befinner seg.

8.7 Sikkerhetsinspeksjoner

NSM fører tilsyn med den forebyggende sikkerhetstjenesten.⁴⁰

FSA, eller den FSA bemyndiger, skal kontrollere sikkerhetstjenesten i FMO gjennom sikkerhetsinspeksjoner. Inspeksjonsteamet skal verifisere at sikkerhetstjenesten er i henhold til sikkerhetsloven, grunnlagsdokumentet og lokal risikohåndtering.

8.8 Veiledning

FSA, eller den FSA bemyndiger, skal gjennomføre veiledning innen sikkerhetstjeneste. Veiledningsteam skal støtte avdelingene i risikohåndtering.

Anmodning om støtte rettes til FSA.

8.9 Besøkskontroll

Besøk kan bli iverksatt etter invitasjon fra ulike ledd i FMO eller etter initiativ fra den som ønsker å komme på besøk.

FSA fører besøksprotokoll over personell som ikke er norske statsborgere og ajourfører oversikter over alle besøk som krever FSJ approbasjon.

³⁸ BFF, kap 6

³⁹ Sikkerhetsloven § 10

⁴⁰ Sikkerhetsloven § 9

Alle besøk til avdelinger i FMO og til norsk forsvarsindustribedrifter skal klareres på forhånd⁴¹. Besøkanmodningen rettes til FSA gjennom vedkommende lands forsvarsattache. Besøkanmodning fra land som er uten militær akkreditering til Norge, skal rettes til Utenriksdepartementet.

Besøkanmodningen skal foreligge hos FSA i god tid, minimum 14 dager (10 virkedager) før besøket finner sted.

Besøksdirektivet regulerer også reiser til andre land.

8.10 Industrisikkerhet

Ved anskaffelse av varer og tjenester skal avdelingene i FMO vurdere behovet for å sikkerhetsgradere anskaffelsen⁴² eller deler av den.

Vurderingen av behovet for å sikkerhetsgradere anskaffelsen skal utføres under ledelse og kontroll av FSA eller den SJFSA bemyndiger. Anskaffelsesmyndigheten og bruker pålegges å støtte aktivt opp om denne prosessen.

8.11 Kurerposttjenesten i FMO

Sjef Forsvarets logistikkorganisasjon (FLO) er ansvarlig for samordning av all kurerforsendelse i regi av FMO, herunder innenlands og til/fra utlandet. Herunder følger ansvaret for utarbeidelse av bestemmelser for kurerposttjeneste i FMO.

Kurerposttjeneste⁴³ kan bare utføres av avdelinger godkjent av FSA for dette formål.

Kurerposttjeneste til nasjoner som ikke er medlem av NATO kan kun utføres av utenriktjenesten.

8.12 Destruksjonsplan

Avdelinger og personell som forvalter gradert utstyr/materiell og spesielt kryptomateriell skal utarbeide en plan for hvordan dette materiellet skal tilintetgjøres i krisesituasjoner/sikkerhetstruende situasjoner (nødmakulering).

8.13 Spesielle sikkerhetstiltak

8.13.1 Tekniske sikkerhetsundersøkelser

Avdelinger som har behov for tekniske sikkerhetsundersøkelser (TSU)⁴⁴ skal fremsende anmodning til FSA. FSA fremsender koordinert behov og avtaler gjennomføring med NSM.

8.13.2 Monitoring

Avdelinger som ønsker støtte til monitoring⁴⁵ skal fremsende anmodning til FSA. FSA fremsender koordinert behov og avtaler gjennomføring med NSM.

8.13.3 Inntrengningstesting

Avdelinger som ønsker støtte til inntrengningstesting⁴⁶ skal fremsende anmodning til FSA. FSA fremsender koordinert behov og avtaler gjennomføring med NSM.

8.13.4 Militær kontraetterretning

Sjef FSA er fagmyndighet og utøvende ansvarlig for militær kontraetterretning på alle nivåer i Forsvaret⁴⁷.

⁴¹ Forsvarets besøksdirektiv, FO/SEKR 3 mai 99

⁴² Forskrift om sikkerhetsgraderte anskaffelser

⁴³ Forskrift om informasjonssikkerhet kapittel 8

⁴⁴ Forskrift om informasjonssikkerhet kapittel 10

⁴⁵ Forskrift om informasjonssikkerhet kapittel 11

⁴⁶ Forskrift om informasjonssikkerhet kapittel 11

⁴⁷ Instruks for sjefen for Forsvarets sikkerhetsavdeling av 15 oktober 2004

8.13.5 Defensiv informasjonsoveroperasjoner

Sjef FSA er fagmyndighet og utøvende ansvarlig for defensive informasjonsoveroperasjoner i Forsvaret⁴⁸.

9 Tiltak

Oversikt over tiltak beskrevet i dette dokumentet.

Tiltak	Ansvar	Revisjon	Ref.
Holde à jour grunnlagsdokument for sikkerhet for FMO	FSA	Fortløpende ved endringer	
Utarbeid utdanningsprogram for sikkerhetspersonell	FSA	Årlig	4.2
Fastsette minimumskrav til kompetanse for sikkerhetsfunksjoner i FMO	FSA	Årlig	4.2
Etabler lokal sikkerhetsorganisasjon	Avdelingssjefer som forvalter kritiske verdier	Fortløpende ved endringer	4.4, 4.5,
Inngå samarbeidsavtale om sikkerhet	Avdelingssjefer med felles base	Årlig eller ved endringer	4.7
Gjennomfør sikkerhetsklarering av personell i FMO	FSA	Fortløpende	5.1
Autoriser eget personell	Avdelingssjefer	Fortløpende	5.2
Etabler fysiske sikringstiltak	Avdelingssjefer	Fortløpende	6
Før kontroll med nøkler, adgangskort og kombinasjoner	Avdelingssjefer	Regelmessig og ved frabeordring av personell	6.2
Etabler militær vakt	Avdelingssjefer	Fortløpende	6.3
Ivareta rollen som fagmyndighet for elektronisk sikring. Gi råd og koordiner virksomheten.	FSA	Fortløpende	6.4
Hold oversikt over sikkerhetsgraderte informasjonssystemer	FSA	Fortløpende	7.1
Rapporter sikkerhetsgraderte informasjonssystemer til FSA	Avdelingssjefer	Ved anskaffelse og endringer	7.2
Fastsette systemeierskap for graderte informasjonssystemer	Anskaffende avdeling	Ved anskaffelse og endringer	7.3
Godkjenne informasjonssystemer hvor virksomhetens leder er godkjenningsansvarlig	FSA	Ved anskaffelse og idriftsetting	7.4

⁴⁸ Instruks for sjefen for Forsvarets sikkerhetsavdeling av 15 oktober 2004

Tiltak	Ansvar	Revisjon	Ref.
Fastsette krav til sikkerhetsdokumentasjon	FSA	Fortløpende	7.4
Fastsette krav til håndtering av kryptomateriell	FSA	Fortløpende	7.6
Gjennomføre lokal risikohåndtering	Avdelingssjefer	Kontinuerlig	8
Gjennomføre strategisk risikohåndtering	FSA	Kontinuerlig	8
Utarbeid lokalt grunnlagsdokument for sikkerhet	Avdelingssjefer	Årlig og ved endringer	8.2
Produsere sikkerhetsetterretninger til avdelinger i FMO	FSA	Rutinemessig	8.3
Rapportere lokale sikkerhetstruende hendelser til FSA	Avdelingssjefer	Innen 24 timer	8.4
Utarbeide reaksjonsplaner, og øve disse	Avdelingssjefer	Årlig og ved endringer	8.5
Gjennomfør sikkerhetsinspeksjoner	FSA	Årlig	8.7
Gjennomfør kontroll og veiledning	FSA	På forespørsel	8.8
Bestemmelser for kurerposttjenesten	FLO	Rutinemessig	8.11
Fremsende anmodning om TSU eller monitoring til FSA	Avdelingssjefer	Ved behov	8.13.1, 8.13.2
Ivareta rollen som fagmyndighet for militær kontraetterretning. Gi råd og koordiner virksomheten.	FSA	Fortløpende	8.13.4
Ivareta rollen som fagmyndighet for defensive informasjonsoperasjoner. Gi råd og koordiner virksomheten.	FSA	Fortløpende	8.13.5