

FINLANDS NATIONELLA SÄKERHETSMYNDIGHET

**ANVISNING OM HANTERING
AV INTERNATIONELLT
SÄKERHETSKLASSIFICERAT
INFORMATIONSMATERIAL**

Uppdaterad

16.3.2016

Innehåll

1.	INLEDNING.....	4
2.	INTERNATIONELLT SÄKERHETSKLASSIFICERAT INFORMATIONSMATERIAL	5
2.1.	Sekretessplikt för informationsmaterial.....	5
2.2.	Överenskommelse om skydd och utbyte av säkerhetsklassificerad information	5
2.3.	Förpliktelserna gäller myndigheter och företag.....	6
3.	INFORMATIONSMATERIAL FRÅN EUROPEISKA UNIONEN OCH HANTERING AV DEN.....	7
3.1.	Allmänna principer	7
3.2.	Offentlig EU-information	7
3.3.	Dokument märkta LIMITE.....	7
3.4.	Säkerhetsklassificerad EU-information	8
3.4.1	RESTREINT UE / EU RESTRICTED	11
3.4.2	CONFIDENTIEL UE / EU CONFIDENTIAL	12
3.4.3	SECRET UE / EU SECRET	14
3.4.4	TRES SECRET UE / EU TOP SECRET.....	16
4.	INFORMATIONSMATERIAL FRÅN NATO OCH HANTERING AV DEN	17
4.1.	Offentlig Nato-information.....	17
4.2.	Icke-klassificerad Nato-information	17
4.3.	Säkerhetsklassificerad Nato-information	18
4.3.1	NATO RESTRICTED	21
4.3.2	NATO CONFIDENTIAL.....	22
4.3.3	NATO SECRET	24
4.3.4	NATO (COSMIC) TOP SECRET	26
5.	HANTERING AV INFORMATIONSMATERIAL FRÅN ANDRA STATER OCH INTERNATIONELLA ORGANISATIONER	27
	FÖRKORTNINGAR	28

MOTSVARIGHETER MELLAN SÄKERHETSKLASSER I EU OCH DESS MEDLEMSLÄNDER.....	29
---	----

1. INLEDNING

Den här anvisningen har som syfte att redogöra för och beskriva förpliktelserna i fråga om hantering av säkerhetsklassificerad information som hör till uppfyllandet av de internationella förpliktelserna som gäller informationssäkerhet. Finland har i fördrag förbundit sig att vidta åtgärder för informationssäkerhet för att skydda sådan säkerhetsklassificerad information som en fördragspart i enlighet med fördraget har överlåtit till Finland. Lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004 med ändringar) har stiftats för att uppfylla de här förpliktelserna på ett allmänt plan.

På hanteringen av internationellt säkerhetsklassificerat informationsmaterial tillämpas de allmänna förpliktelser som gäller god informationshantering i lagen om offentlighet i myndigheternas verksamhet (621/1999, nedan offentlighetslagen) samt förordningen om informationssäkerhet i statsförvaltningen (681/2010, nedan informationssäkerhetsförordningen), om inte annat följer av den internationella informationssäkerhetsförpliktelserna. För detaljerna i verkställigheten av informationssäkerhetsförordningen redogörs i finansministeriets anvisning (VAHTI 2/2010).

Den här anvisningen ersätter inte bestämmelser i fördrag eller andra internationella förpliktelser som gäller informationssäkerhet. Den som behöver exakt information om förpliktelserna ska som källa i första hand använda de bestämmelser och fördrag där förpliktelserna preciseras.

Utrikesministeriet (UM) är Finlands nationella säkerhetsmyndighet (*National Security Authority, NSA*) vid uppfyllande av internationella förpliktelser som gäller informationssäkerhet. Försvarsministeriet, huvudstaben, Skyddspolisen och Kommunikationsverket är sådana utsedda säkerhetsmyndigheter (*Designated Security Authority, DSA*) som utöver den nationella säkerhetsmyndigheten uppfyller internationella förpliktelser som gäller informationssäkerhet. Kommunikationsverket är dessutom ansvarig nationell myndighet för informationssäkerhet i fråga om informationssystem och datakommunikation (*National Communication Security Authority, NCSA*). Alla de här myndigheterna har sina egna ansvarsområden i den nationella säkerhetsmyndighetens arbetsfält.

Den som behöver råd och vägledning i enskilda fall ska vända sig till den nationella säkerhetsmyndighetsorganisationen. Allmänna frågor ska riktas till nationella säkerhetsmyndigheten vid UM (nsa@formin.fi) och specialfrågor som gäller elektronisk informationsöverföring till enheten NCSA-FI (ncsa@ficora.fi) vid Kommunikationsverket.

2. INTERNATIONELLT SÄKERHETSKLASSIFICERAT INFORMATIONSMATERIAL

Med internationellt säkerhetsklassificerat informationsmaterial avses sådant *särskilt känsligt informationsmaterial* enligt lagen om internationella förpliktelser som gäller informationssäkerhet som Finland ska skydda utifrån ett internationellt fördrag eller EU:s säkerhetsbestämmelser. Följaktligen är internationellt säkerhetsklassificerat informationsmaterial sådana handlingar och sådant material, samt uppgifter som ingår i dem, som har lämnats till Finland och som överlåtaren har försett med en säkerhetsklassmärkning enligt en internationell förpliktelse som gäller informationssäkerhet.

2.1. Sekretessplikt för informationsmaterial

På internationellt säkerhetsklassificerat material tillämpas specialbestämmelsen om ovillkorlig sekretessplikt i lagen om internationella förpliktelser som gäller informationssäkerhet och för sådant material gäller inte offentlighetslagens fallspecifika sekretessbedömning. Internationellt säkerhetsklassificerat material är följaktligen sekretessbelagt, om inte annat följer av fördrag eller bestämmelser som gäller materialet i fråga.

I lagen om internationella förpliktelser som gäller informationssäkerhet ingår straffbestämmelser för brott mot skyldigheten att sekretessbelägga handlingar. Enligt strafflagen (39/1889) utdöms straff för brott mot sekretessskyldigheten antingen som brott mot tjänsthemlighet eller brott mot tjänsthemlighet av oaktsamhet, sekretessbrott eller sekretessförseelse.

I förordningen om tillgång till EU-organs handlingar, den så kallade öppenhetsförordningen (1049/2001), ingår allmänna bestämmelser om hanteringen av känsliga EU-handlingar. I öppenhetsförordningen fastställs grunderna för säkerhetsklassificeringen. I säkerhetsbestämmelserna för Europeiska unionens organ föreskrivs närmare om förfaranden och arrangemang för att skydda säkerhetsklassificerade EU-uppgifter.

2.2. Överenskommelse om skydd och utbyte av säkerhetsklassificerad information

En överenskommelse om skydd av säkerhetsklassificerad information mellan Finland och en främmande stat eller Finland och en internationell organisation förutsätter ett fördrag. I överenskommelserna om informationssäkerhet förpliktas parterna att se till att den andra partens säkerhetsklassificerade information hanteras på ett korrekt sätt.

Det är NSA vid utrikesministeriet som ansvarar för beredningen av överenskommelser mellan Finland och främmande stater. Alla de förvaltningsgrenar vars sakkunskap anses vara behövlig deltar i beredningen.

2.3. Förpliktelserna gäller myndigheter och företag

Bestämmelserna om internationellt säkerhetsklassificerat informationsmaterial tillämpas förutom på myndigheter också på näringsidkare och deras anställda när de deltar i ett säkerhetsklassificerat projekt. Statsförvaltningens behöriga säkerhetsmyndigheter ansvarar för att Finlands näringsliv förmår hantera internationell säkerhetsklassificerad information när det tar emot säkerhetsklassificerade uppgifter från ett främmande land eller en internationell organisation. Finlands nationella kriteriesamling för säkerhetsauditering (KATAKRI), som används som verktyg när finska myndigheter ser över säkerhetsnivån i inhemska företag och andra organisationer, har strävat efter att beakta de allmänna internationella kraven.

3. INFORMATIONSMATERIAL FRÅN EUROPEISKA UNIONEN OCH HANTERING AV DEN

Rådets säkerhetsbestämmelser (488/2013) är medlemsstaternas viktigaste regelverk för skydd av säkerhetsklassificerade EU-uppgifter. Även andra EU-organ har egna säkerhetsregler där de förbinder sig att följa motsvarande säkerhetskrav. Rådets beslut om säkerhetsbestämmelser har ett omfattande tillämpningsområde. I beslutet föreskrivs det bland annat om säkerhetsklassificering av EU-handlingar, informationshantering, fysisk säkerhet, förfarandet för säkerhetsutredning av anställda, informationssäkerheten i informationssystemen samt överlåtande av information till tredje stater och internationella organisationer.

3.1. Allmänna principer

EU:s säkerhetsklassificerade uppgifter ska skyddas under hela deras livscykel för att förhindra att uppgifter äventyras eller går förlorade och för att sådant ska upptäckas. Dessa skyddsåtgärder gäller särskilt upprättande, registrering, kopiering, befordran, lagring och förstöring av säkerhetsklassificerad EU-information.

Säkerhetsklassificerad EU-information skyddas i enlighet med deras säkerhetsklass. Ju högre säkerhetsklassificering materialet har, desto striktare säkerhetsåtgärder krävs det. Merparten av den säkerhetsklassificerade informationen hör till den lägsta säkerhetsklassen RESTREINT UE/EU RESTRICTED. Material i säkerhetsklass CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET förekommer mer sällan och för detta gäller betydligt striktare säkerhetsåtgärder.

3.2. Offentlig EU-information

Informationen i Europeiska unionen är offentlig, om inga begränsningar av tillgången till information enligt öppenhetsförordningen gäller för den. Vilka av kommissionens och rådets handlingar som är offentliga framgår bland annat av organens offentliga register över handlingar.

3.3. Dokument märkta LIMITE

LIMITE-märkningen är inte en säkerhetsklassificering utan handlar om distribution. Märkningen betyder att dokumentet är avsett för intern distribution till rådet, dess medlemmar, kommissionen och vissa andra EU-institutioner och -organ.

Eventuell sekretess nationellt måste grunda sig på offentlighetslagen, till exempel 24 § 1 mom. 2 punkt.

LIMITE

En intern distributionsbegränsning inom EU.

- inga krav ställs på **lokalerna**
- inga krav ställs på **informationssystemen**
- inga krav ställs på **informationsöverföringen**
- okrypterad information får överföras över **internet**
- får **kopieras** med vanlig kopieringsmaskin
- får **sändas** per post
- får **förstöras** med dokumentförstörare eller genom att anlita en förstöringstjänst

3.4. Säkerhetsklassificerad EU-information

Säkerhetsklassificerad EU-information som betecknas med den internationella förkortningen EUCI (*European Union Classified Information*) avser vilka uppgifter eller material som helst som har EU-säkerhetsklassificerats och som, om de röjs utan grund, kan åsamka unionens eller medlemsstaternas intressen skada av varierande grad.

Ansvar för säkerhetsklassificeringen ligger hos det EU-organ vars information det gäller.

Klassificeringen av EU-uppgifter får inte ändras eller avlägnas utan tillstånd av den som är upphov till informationen.

Säkerhetsklassmärkningarnas motsvarigheter i EU och Finland:

Europeiska unionens säkerhetsklass	EU-förkortning	Finlands motsvarande säkerhetsklass (informationssäkerhetsförordningen)
TRES SECRET UE / EU TOP SECRET	TS-UE/ EU-TS	ERITTÄIN SALAINEN / YTTERST HEMLIG
SECRET UE / EU SECRET	S-UE/EU-S	SALAINEN / HEMLIG
CONFIDENTIEL UE / EU CONFIDENTIAL	C-UE/EU-C	LUOTTAMUKSELLINEN / KONFIDENTIELL
RESTREINT UE / EU RESTRICTED	R-UE/EU-R	KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG

EU-handlingar ska alltid klassificeras minst enligt den säkerhetsklass som gäller för uppgifter med den högsta klassificeringsnivån i dokumentet. Olika delar av handlingen kan ha olika säkerhetsklasser och ska märkas i enlighet med det. I fråga om stora informationsmaterial

bör det särskilt övervägas om helheten ska klassificeras högre än de enskilda uppgifterna (s.k. aggregationseffekt).

PERSONAL **Säkerhetsklassificerad EU-information får endast lämnas ut till personer som har ett arbetsrelaterat behov av informationen i fråga, godkänt av myndigheterna.** Dessa personer ska sätta sig in i de förpliktelser som gäller för skydd av säkerhetsklassificerad EU-information, innan informationen i fråga kan lämnas ut till dem.

Den som hanterar säkerhetsklassificerad EU-information av klass CONFIDENTIAL UE / EU CONFIDENTIAL eller högre, ska ha ett intyg över säkerhetsutredning av person (personnel security clearance, PSC) utfärdat av den nationella säkerhetsmyndigheten. Arbetsgivaren ska definiera vilka uppgifter som kräver ett PSC-intyg och upprätthålla en uppdaterad förteckning över dem. PSC-intyget grundar sig på en säkerhetsutredning gjord av Skyddspolisen i enlighet med lagen om säkerhetsutredning (726/2014). Det krävs dock varken PSC-intyg eller säkerhetsutredning för behovsbaserad överlåtelse av information av högst klass RESTREINT UE / EU RESTRICTED.

Länk till NSA:s webbplats med anvisning för ansökan om PSC-intyg

LOKALER **Den fysiska säkerheten** ska utformas så att den hindrar obehörig tillgång till säkerhetsklassificerad EU-information. Kravet rör alla lokaler där säkerhetsklassificerad EU-information hanteras eller förvaras. Beroende på säkerhetsklassnivå förutsätts det att lokalen godkänns av den behöriga myndigheten. Beroende på säkerhetsklass kan säkerhetsklassificerad EU-information hanteras i utrymmen på tre olika nivåer:

- **administrativa utrymmen**,
- egentliga **säkrade utrymmen** som omfattas av åtkomstkontroll och
- **tekniskt skyddade säkrade utrymmen**, som förhindrar avlyssning.

SYSTEM De **informationssystem** där säkerhetsklassificerad EU-information överförs eller hanteras ska godkännas separat av en behörig säkerhetsmyndighet (ackreditering) (SAA). I informationssystem där det hanteras information av säkerhetsklass CONFIDENTIAL UE / EU CONFIDENTIAL eller högre ska dessutom riskerna med elektromagnetisk diffus strålning beaktas och åtgärder för att minimera riskerna vidtas (s.k. TEMPEST-motåtgärder).

När säkerhetsklassificerad EU-information överförs i och mellan informationssystem ska den krypteras med metoder som är godkända av Finlands nationella godkännandemyndighet för informationssäkerhetsprodukter (CAA). Innan information av klassen SECRET UE / EU SECRET kan överföras i eller mellan informationssystem ska den krypteringsmetod eller informationssäkerhetsprodukt som används vara godkänd

av EU-rådets godkännandemyndighet för informationssäkerhetsprodukter. Det här gäller också de finska informationssystem som står i förbindelse med ett system klassificerat som SECRET UE / EU SECRET.

3.4.1 RESTREINT UE / EU RESTRICTED

En säkerhetsklass, enligt vilken

- **personen i fråga** ska ha ett arbetsrelaterat **behov** av den säkerhetsklassificerade informationen, godkänt av myndigheterna (need-to-know) och **sätta sig in** i de förpliktelser som gäller för säkerhetsklassen
- inga specialkrav ställs på **lokalen**, men en lokal där material av klass RESTREINT UE / EU RESTRICTED hanteras ska hållas låst då man lämnar den. Materialet i fråga ska förvaras på en låst plats, och utomstående får inte komma åt att bekanta sig med det
- **informationssystemet** ska godkännas separat av en behörig myndighet (NCSA-FI).
- krypteringsmetoden ska vara godkänd av EU:s säkerhetsmyndighet eller en nationell behörig myndighet (CAA) vid **elektronisk överföring av information**
- information inte **får överföras över internet**, om den inte har krypterats med en krypteringsmetod godkänd särskilt för ändamålet
- informationen får **kopieras** med vanlig kopieringsmaskin
- informationen får **sändas** per post i ett ogenomskinligt kuvert
- informationen får **transporteras**, men ska skyddas
- informationen får **förstöras** med dokumentförstörare eller genom att anlita en förstöringstjänst som har godkänts av en myndighet.

3.4.2 CONFIDENTIEL UE / EU CONFIDENTIAL

En säkerhetsklass, enligt vilken

- **personen i fråga** ska ha ett arbetsrelaterat **behov** av den säkerhetsklassificerade informationen, godkänd av myndigheterna (need-to-know)
- **personen** ska ha ett intyg över säkerhetsutredning av person på tillräckligt hög nivå (**PSC**)
- personen ska **sätta sig in** i de förpliktelser som gäller för säkerhetsklassen
- arbetsgivaren ska skriftligen **berättiga** personen att hantera information klassificerad CONFIDENTIEL UE / EU CONFIDENTIAL
- information klassificerad CONFIDENTIEL UE / EU CONFIDENTIAL får hanteras i administrativa utrymmen, om informationen har skyddats så att utomstående inte har tillgång till den. Insyn utifrån måste förhindras
- information klassificerad CONFIDENTIEL UE / EU CONFIDENTIAL ska förvaras i ett nationellt godkänt säkerhetsskåp alltid när man lämnar rummet, om det inte är fråga om ett larmförsatt valv som har godkänts för ändamålet
- **informationssystemet** ska godkännas separat av en behörig myndighet (NCSA-FI)
- anslutning av nationella informationsnät till EU:s klassificerade informationsnät ska godkännas av en nationell behörig myndighet (SAA)
- elektromagnetisk diffus strålning ska förhindras tillräckligt effektivt (s.k. TEMPEST-motåtgärder), om information av klass CONFIDENTIEL UE / EU CONFIDENTIAL behandlas elektroniskt,
- krypteringsmetoden ska vara godkänd av EU:s säkerhetsmyndighet eller en nationell behörig myndighet (CAA) vid **elektronisk överföring av information**
- informationen **inte får överföras över internet**, om den inte har krypterats med en krypteringsmetod godkänd särskilt för ändamålet
- **registrering** krävs före sändning, vid mottagning och förstöring
- informationen inte får **kopieras** med vanlig kopieringsmaskin. Kopieringsmaskinen får inte ha nätkontakt och dess massminne bör administreras av den säkerhetsansvariga vid arbetsenheten (servicemannen får inte lämnas ensam vid maskinen)
- informationen får **sändas** inom EU i enlighet med de krav som gäller för kommersiell kurirservice, rekommenderat i två ogenomskinliga kuvert eller i en låst och/eller förseglad transportpåse. Det yttre kuvertet får inte ha någon anteckning om säkerhetsklass. Information från unionens område till tredje stater får sändas endast per kurir

- informationen får **sändas** i slutet kuvert med den egna organisationen som mottagare. Transportmedlet (portfölj el.dyl.) får inte lämnas utan övervakning
- informationen får **förstöras** med dokumentförstörare med säkerhetsnivå DIN 4 (registerförare på registratorskontor)

3.4.3 SECRET UE / EU SECRET

En säkerhetsklass, enligt vilken

- **personen i fråga** ska ha ett arbetsrelaterat **behov** av den säkerhetsklassificerade informationen, godkänd av myndigheterna (need-to-know)
- **personen** ska ha ett intyg över säkerhetsutredning av person på tillräckligt hög nivå (**PSC**)
- personen ska **sätta sig in** i de förpliktelser som gäller för säkerhetsklassen
- arbetsgivaren ska skriftligen **berättiga** personen att hantera information klassificerad som SECRET UE / EU SECRET
- information klassificerad som SECRET UE / EU SECRET får hanteras i administrativa utrymmen, om den har skyddats så att utomstående inte har tillgång till den. Insyn utifrån måste förhindras
- information klassificerad som SECRET UE / EU SECRET ska förvaras i ett nationellt godkänt säkerhetsskåp alltid då man lämnar rummet, om det inte är ett larmförsatt valv som har godkänts för ändamålet.
- **informationssystemet** ska godkännas separat av en behörig myndighet (NCSA-FI)
- anslutning av de nationella informationsnäten till EU:s klassificerade informationsnät ska godkännas av en nationell behörig myndighet (SAA)
- elektromagnetisk diffus strålning ska förhindras tillräckligt effektivt (s.k. TEMPEST-motåtgärder), om information av klass SECRET UE / EU SECRET behandlas elektroniskt
- den krypteringsmetod eller informationssäkerhetsprodukt som används i eller mellan informationssystem som **för över information** av klassen SECRET UE / EU SECRET ska vara godkända av EU-rådets godkännandemyndighet för informationssäkerhetsprodukter. Det här gäller också de finska informationssystem som står i förbindelse till ett system klassificerat som SECRET UE / EU SECRET
- informationen inte får överföras över **internet**, om den inte har krypterats med en krypteringsmetod som EU:s säkerhetsmyndighet särskilt har godkänt för ändamålet
- **registrering** krävs före sändning och vid mottagning
- informationen inte får **kopieras** med vanlig kopieringsmaskin. Kopieringsmaskinen får inte ha nätkontakt och dess massminne bör administreras av den säkerhetsansvariga vid arbetsenheten (servicemannen får inte lämnas ensam vid maskinen)
- informationen får **sändas** endast med kurir

- får **sändas** i slutet kuvert beaktande kraven på kurirförfarande (kuririntyg osv.) och med den egna organisationen som mottagare. Öppnas officiellt i mottagarändan. Transportmedlet (portfölj el.dyl.) får inte lämnas utan övervakning.
- informationen får **förstöras** med dokumentförstörare med säkerhetsnivå DIN 4 (registerförare på registratorskontor).

3.4.4 TRES SECRET UE / EU TOP SECRET

Handlingar av klass TRES SECRET UE / EU TOP SECRET förekommer eller hanteras mycket sällan i EU och dess medlemsländer. För hanteringen förutsätts kraven enligt klass SECRET UE / EU SECRET, men dessutom är personvalet av hanteraren ofta förknippat med särskilda specialåtgärder som ska lösas (hanteringsrättigheter och bestämning av nivå för säkerhetsutredning). Vidare skiljer sig registreringen och förstöringen av handlingar i den här klassen från de lägre säkerhetsklasserna (bl.a. registrering i specialregister), och ett informationssystem av den här klassen får inte heller ha förbindelser till oskyddade nät.

4. INFORMATIONSMATERIAL FRÅN NATO OCH HANTERING AV DEN

Enligt överenskommelsen om informationssäkerhet mellan Nato och Finland (FördrS 7 och 8/2013) ska parterna skydda varandras säkerhetsklassificerade information. Nato har ett separat, internt godkänt regelverk för hantering av säkerhetsklassificerad information. I överenskommelsen om informationssäkerhet mellan Finland och Nato har Finland förbundit sig att genom tillräckliga nationella åtgärder respektera kraven i Natos säkerhetsregelverk.

På finska myndigheters handlingar tillämpas offentlighetsprincipen. På Natos handlingar tillämpas sekretessprincipen. Natos gällande säkerhetsregelverk bygger på dokumentationshelheten *Nato Security Policy* (NSP). Det praktiska uppdateringsarbetet med säkerhetsregelverket sköts av Natos säkerhetsenhet NOS (*Nato Office of Security*).

Om information som överlåtit till Nato är säkerhetsklassificerad, kvarstår bestämmanderätten till informationen hos det utlämnande landet och informationen kan inte klassificeras på nytt av Nato utan skriftligt tillstånd av landet.

Nato förutsätter av sina medlemsländer och sina avtalspartnerländer en centraliserad administration av säkerhetsklassificerad information. Det här innebär att ett centralregister (högst två per land) och underregister måste inrättas. Finlands Nato-centralregister finns vid utrikesministeriet.

4.1. Offentlig Nato-information

Sådan Nato-information är offentlig som inte är säkerhetsklassificerad och som ett Nato-organ eller en Nato-myndighet med ansvar för ärendet offentliggör.

4.2. Icke-klassificerad Nato-information

Icke-säkerhetsklassificerad information, som är avsedd för internt bruk i Nato, märks med distributionsbegränsningen NATO UNCLASSIFIED (NU) i stället för med anteckning om säkerhetsklass. Informationen i fråga kan enligt prövning lämnas till mottagare utanför Natoländers myndigheter utan de villkor som ställs på hanteringen av säkerhetsklassificerad information.

En distributionsbegränsning.

- **personen i fråga** ska ha ett arbetsrelaterat **behov** av informationen, godkänt av myndigheterna, och ska förstå betydelsen av distributionsbegränsningen
- inga krav ställs på **lokalen**
- inga krav ställs på **informationssystemen**
- inga krav ställs på **informationsöverföringen**
- kan överföras okrypterad över **internet**
- får **kopieras** med vanlig kopieringsmaskin
- får **sändas** per post
- får **förstöras** med dokumentförstörare eller genom att anlita en förstöringstjänst

4.3. Säkerhetsklassificerad Nato-information

Med säkerhetsklassificerad Nato-information avses vilken information eller vilket material som helst som har säkerhetsklassificerats av Nato och som, om den röjs utan grund, kan orsaka skada av varierande grad för Natos eller något av dess medlemsländers intressen.

MÄRKNINGAR Säkerhetsklassmärkningarnas motsvarigheter i Nato och Finland

Natos säkerhetsklass	Förkortning	Finlands motsvarande säkerhetsklass (informationssäkerhetsförordningen)
COSMIC TOP SECRET	CTS	ERITTÄIN SALAINEN / YTTERST HEMLIG
NATO SECRET	NS	SALAINEN / HEMLIG
NATO CONFIDENTIAL	NC	LUOTTAMUKSELLINEN / KONFIDENTIELL
NATO RESTRICTED	NR	KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG

I Nato-handlingar ska anteckning om säkerhetsklass göras på varje sida och både upptill och nedtill på sidan. Dessutom ska sista sidans baksida förses med anteckningen. Nato-handlingar ska alltid klassificeras minst enligt den säkerhetsklass som motsvarar uppgifterna i handlingen med den högsta klassificeringsnivån. I fråga om stora informationsmaterial bör det särskilt övervägas om helheten ska klassificeras högre än de enskilda uppgifterna (s.k. aggregationseffekt).

När det gäller Nato-information ansvarar den som upprättat handlingen för säkerhetsklassificeringen. **Klassificeringen av säkerhetsklassificerad Nato-information kan sänkas eller informationen offentliggöras endast med skriftligt förhandstillstånd av den som har upprättat handlingen.**

Distributionen av säkerhetsklassificerad Nato-information kan administreras och begränsas med anteckning om distribution intill anteckningen om säkerhetsklass. Detta blir aktuellt särskilt när handlingen eller materialet distribueras till en så kallad tredje part. Nedan ges tre exempel på hur anteckningar om säkerhetsklass och om distribution kan göras:

1. Målorganisation eller insats och säkerhetsklass, t.ex.

ISAF CONFIDENTIAL

2. Om tillgången till materialet i fråga har begränsats till enbart vissa fredspartnerländer, är anteckningen t.ex.

NATO / PfP RESTRICTED

FINLAND AND SWEDEN ONLY

3. Om t.ex. alla stater som deltar i en viss krishanteringsinsats ges tillgång till materialet i fråga, är anteckningen t.ex.

NATO / CONFIDENTIAL

RELEASABLE to KFOR

PERSONAL

Säkerhetsklassificerad Nato-information får endast överlåtas till personer som har behov av informationen i fråga, godkänt av en nationell myndighet. Innan informationen överlåts ska den personen sätta sig in i de förpliktelser som gäller för skydd av säkerhetsklassificerad Nato-information.

Den som hanterar säkerhetsklassificerad Nato-information av klass NATO CONFIDENTIAL eller högre, ska ha ett intyg över säkerhetsutredning av person (personnel security clearance, PSC) utfärdat av den nationella säkerhetsmyndigheten. Arbetsgivaren ska definiera vilka uppgifter som kräver ett PSC-intyg och upprätthålla en uppdaterad förteckning över dem. PSC-intyget grundar sig på en säkerhetsutredning gjord av Skyddspolisen i enlighet med lagen om säkerhetsutredning (726/2014). Varken PSC-intyg eller säkerhetsutredning krävs för behovsbaserad överlåtelse av information av högst klass NATO RESTRICTED.

Länk till NSA:s webbplats med anvisning om ansökan om PSC-intyg

LOKALER

Den fysiska säkerheten ska dimensioneras så att det inte är möjligt att få obehörig tillgång till säkerhetsklassificerad Nato-information. Kravet gäller alla de lokaler där säkerhetsklassificerad Nato-information hanteras eller förvaras. Om informationen som ska behandlas har säkerhetsklass NATO SECRET eller högre, ska säkerhetsnivån i lokalen där informationen förvaras vara godkänd av en ansvarig myndighet.

SYSTEM

Alla **informationssystem** där det överförs säkerhetsklassificerad Nato-information ska godkännas separat av en behörig säkerhetsmyndighet (ackreditering). Informationssystem där det överförs information av säkerhetsklass NATO SECRET eller högre ska vara godkända av Natos militärkommitté. Det här gäller även informationssystem i Finland som står i förbindelse med NATO SECRET-systemet och där det överförs säkerhetsklassificerad Nato-information. I informationssystem där det hanteras information av klass NATO CONFIDENTIAL eller högre ska dessutom riskerna med elektromagnetisk diffus strålning beaktas och metoder för att minimera riskerna tas fram (s.k. TEMPEST-motåtgärder).

När säkerhetsklassificerad Nato-information förs över mellan Natos informationssystem och ett inhemskt informationssystem ska informationen krypteras med en metod som är godkänd av Natos militärkommitté. När säkerhetsklassificerad Nato-information förs över i nationella system ska de krypteringssystem som används vara godkända av Natos militärkommitté alltid då informationen som överförs har klassen NATO SECRET. För krypteringssystem för överföring av Nato-information med lägre säkerhetsklass räcker ett godkännande av Finlands behöriga myndighet (NCSA-FI), förutsatt att Nato godkänner det i varje enskilt fall.

4.3.1 NATO RESTRICTED

En säkerhetsklass, enligt vilken

- **personen i fråga** ska ha ett arbetsrelaterat **behov** av den säkerhetsklassificerade informationen, godkänt av myndigheterna, (need-to-know) och **sätta sig in** i de förpliktelser som gäller för säkerhetsklassen
- inga specialkrav ställs på **lokalen**, men en lokal där material av klass NATO RESTRICTED hanteras ska hållas låst då man lämnar den. Materialet i fråga ska förvaras på en låst plats, och utomstående får inte komma åt att bekanta sig med det
- **informationssystemet** ska godkännas separat av en behörig myndighet
- vid **elektronisk överföring** av information ska krypteringsmetoden vara godkänd av Nato eller av en behörig myndighet
- information inte får överföras över **internet**, om den inte har krypterats med en krypteringsmetod godkänd särskilt för ändamålet
- informationen får **kopieras** med vanlig kopieringsmaskin
- informationen får **sändas** per post i ett ogenomskinligt kuvert
- informationen får **transporteras**, men ska skyddas
- informationen får **förstöras** med dokumentförstörare eller genom att anlita en förstöringstjänst, om denna är godkänd av en myndighet.

4.3.2 NATO CONFIDENTIAL

En säkerhetsklass, enligt vilken

- **personen i fråga** ska ha ett arbetsrelaterat **behov** av den säkerhetsklassificerade informationen, godkänt av myndigheterna, (need-to-know)
- personen ska ha ett intyg över säkerhetsutredning av person på tillräckligt hög nivå (**PSC**)
- personen ska **sätta sig in** i de förpliktelser som gäller för säkerhetsklassen
- arbetsgivaren ska skriftligen **berättiga** personen att hantera information klassificerad som NATO CONFIDENTIAL
- tillträdet till **lokalen** ska vara övervakat och vid hantering av material klassificerat som NATO CONFIDENTIAL ska tillgången till informationen skyddas för utomstående. Insyn utifrån måste förhindras
- information klassificerad som NATO CONFIDENTIAL ska förvaras i ett nationellt godkänt säkerhetsskåp alltid då man lämnar rummet, om det inte är ett larmförsett valv som har godkänts för ändamålet.
- **informationssystemet** ska godkännas separat av en behörig myndighet
- om information av klass NATO CONFIDENTIAL behandlas elektroniskt ska elektromagnetisk diffus strålning förhindras tillräckligt effektivt (s.k. TEMPEST-motåtgärder)

- krypteringsmetoden ska vara godkänd av Nato eller av en behörig myndighet vid **elektronisk överföring** av informationen
- informationen inte får överföras över **internet**, om den inte är krypterad med en krypteringsmetod godkänd särskilt för ändamålet
- **registrering** krävs före sändning och vid mottagning
- informationen inte får **kopieras** med vanlig kopieringsmaskin. Kopieringsmaskinen får inte ha nätkontakt och dess massminne bör administreras av den säkerhetsansvariga vid arbetsenheten (servicemannen får inte lämnas ensam vid maskinen)
- informationen får **sändas** endast med kurir
- informationen får **transporteras** i slutet kuvert, med den egna organisationen som mottagare. Transportmedlet (portfölj el.dyl.) får inte lämnas utan övervakning
- informationen får **förstöras** med dokumentförstörare med säkerhetsnivå DIN 4

4.3.3 NATO SECRET

En säkerhetsklass, enligt vilken

- **personen** ska ha ett arbetsrelaterat **behov** av den säkerhetsklassificerade informationen, godkänt av myndigheterna (need-to-know)
- personen ska ha ett intyg över säkerhetsutredning av person på tillräckligt hög nivå (**PSC**)
- personen ska **sätta sig in** i de förpliktelser som gäller för säkerhetsklassen
- arbetsgivaren skriftligen ska **berättiga** personen att hantera information klassificerad som NATO SECRET
- tillträdet till **lokalen** måste övervakas så att arrangemanget hindrar andra än personer med rätt att hantera NATO SECRET-klassificerat material från att oövervakat komma in. Lokalen ska vara särskilt godkänd för hantering av NATO SECRET-klassificerat material och utrustad med ett system för passerkontroll
- NATO SECRET-klassificerad information ska förvaras i ett nationellt godkänt säkerhetsskåp alltid då man lämnar rummet, om det inte är ett larmförsett valv som har godkänts för ändamålet.
- insyn utifrån måste förhindras närmaterial klassificerat som NATO SECRET hanteras
- **informationssystemet** ska godkännas separat av Natos militärkommitté
- elektromagnetisk diffus strålning måste förhindras tillräckligt effektivt (s.k. TEMPEST-motåtgärder), om information av klass NATO SECRET behandlas elektroniskt

- krypteringsmetoden ska godkännas separat av Natos militärkommitté vid **elektronisk överföring** av information
- informationen inte får överföras över **internet**, om den inte är krypterad med en krypteringsmetod som Natos militärkommitté särskilt har godkänt för det här uttryckliga ändamålet
- **registrering** krävs före sändning, vid mottagning och vid förstöring
- informationen inte får **kopieras** med vanlig kopieringsmaskin. Kopieringsmaskinen får inte ha nätkontakt och dess massminne bör administreras av den säkerhetsansvariga vid arbetsenheten (servicemannen får inte lämnas ensam vid maskinen). Varje kopia ska numreras och registreras
- informationen får **sändas** endast med kurir
- informationen får **transporteras** med kurirförpliktelser och försedd med kurirdokumentation i slutet kuvert med den egna organisationen som mottagare. Transportmedlet (portfölj el.dyl.) får under inga omständigheter lämnas utan övervakning. Försändelsen ska öppnas dokumenterat
- informationen ska **förstöras** med dokumentförstörare med minimisäkerhetsnivå DIN 4 med arkivhanteringsåtgärder (registerförare)

4.3.4 NATO (COSMIC) TOP SECRET

Det är mycket sällsynt att NATO COSMIC TOP SECRET-handlingar överläts till mottagare utanför Natos medlemsländer och det kräver en separat godkännandeprocess.

5. HANTERING AV INFORMATIONSMATERIAL FRÅN ANDRA STATER OCH INTERNATIONELLA ORGANISATIONER

I de internationella överenskommelserna om säkerhetsklassificerad information förbinder sig parterna till ett ömsesidigt skydd av säkerhetsklassificerad information: den andra partens säkerhetsklassificerade uppgifter skyddas på samma nivå som egen information i motsvarande säkerhetsklass. För det här ändamålet definieras säkerhetsklassernas motsvarigheter och de allmänna principerna för utbyte av säkerhetsklassificerad information. I överenskommelserna begränsas användningen av säkerhetsklassificerad information till angivet ändamål. Det definieras i vilka situationer hanteringen av säkerhetsklassificerad information kräver en säkerhetsutredning av företag, organisationer och personer inom fördragsparternas jurisdiktion. Intyget över säkerhetsutredning av person benämns PSC (*Personal Security Clearance*) eller PSCC (*Personal Security Clearance Certificate*). På motsvarande sätt kallas intyget över säkerhetsutredning av företag och andra organisationer FSC (*Facility Security Clearance*).

Länk till gällande överenskommelser om informationssäkerhet

FÖRKORTNINGAR

CAA	Crypto Approval Authority, i Finland NCSA-FI vid Kommunikationsverket
DSA	Designated Security Authority, utsedd säkerhetsmyndighet
FSC	Facility Security Clearance, säkerhetsutredning av företag
NSA	National Security Authority, nationell säkerhetsmyndighet
PSC	Personnel Security Clearance, intyg över säkerhetsutredning av person
PSCC	Personnel Security Clearance Certificate, se PSC
SAA	Security Accreditation Authority, i Finland NCSA-FI vid Kommunikationsverket

MOTSVARIGHETER MELLAN SÄKERHETSKLASSER I EU OCH DESS MEDLEMSLÄNDER

EU-SÄKERHETSKLASS	TRES SECRET UE / EU TOP SECRET	SECRET UE / EU SECRET	CONFIDENTIEL UE / EU CONFIDENTIAL	RESTREINT UE / EU RESTRICTED
Nederländerna	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Belgien	Très Secret (Loi 11.12.1998) Zeet Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	<i>se anmärkning 1</i>
Bulgarien	Строго секретно	Секретно	Поверително	За служебно ползване
Spanien	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Irland	Top Secret	Secret	Confidential	Restricted
Italien	Segretissimo	Segreto	Riservatissimo	Riservato
Österrike	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Grekland	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Cypern	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Kroatien	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Lettland	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litauen	Visiškai slapiai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
<i>se anmärkning 2</i>	Top Secret	Secret	Confidential	Restricted
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Polen	Ścisłe Tajne	Tajne	Poufne	Zastrzeżone
Frankrike	Très Secret Défense	Secret Défense	Confidentiel Défense	<i>se anmärkning 3</i>
Rumänien	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu

Sverige <i>se anmärkning 4</i>	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Tyskland	STRENG GEHEIM	GEHEIM	VS — VERTRAULICH <i>(se anmärkning 5)</i>	VS — NUR FÜR DEN DIENSTGEBRAUCH
Slovakien	Prísne tajné	Tajné	Dôverné	Vyhradené
Slovenien	STROGO TAJNO	TAJNO	ZAUPNO	INTERNO
Finland	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Danmark	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Republiken Tjeckien	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Ungern	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Estland	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Förenade kungariket	UK TOP SECRET	UK SECRET	UK CONFIDENTIAL <i>se anmärkning 6</i>	UK RESTRICTED

ANMÄRKNINGAR

1: Diffusion Restreinte / Beperkte Verspreiding är inte en säkerhetsklass i Belgien. Belgien hanterar och skyddar RESTREINT UE/EU RESTRICTED-uppgifter minst lika strikt som de i Europeiska unionens säkerhetsbestämmelser beskrivna kraven och förfarandena förutsätter.

2: I Malta kan man använda märkningar på både maltesiska och engelska.

3: Frankrike använder inte säkerhetsklassen RESTREINT i sitt nationella system. Frankrike hanterar och skyddar RESTREINT UE/EU RESTRICTED-uppgifter minst lika strikt som de i Europeiska unionens säkerhetsbestämmelser beskrivna kraven och förfarandena förutsätter.

4: Sverige: Märkningarna på den övre raden används inom försvaret medan andra myndigheter använder märkningarna på den nedre raden.

5: Tyskland: VS = Verschlusssache.

6: Förenade kungariket övergick 1.4.2014 till en säkerhetsklassificering i tre steg. Förenade kungariket avstår från säkerhetsklassen UK CONFIDENTIAL och hanterar information med klassen CONFIDENTIEL UE/EU CONFIDENTIAL i enlighet med säkerhetsåtgärderna i klassen UK SECRET. UK RESTRICTED omvandlas till den motsvarande säkerhetsklassen UK OFFICIAL-SENSITIVE.