



Europeiska
unionens råd

Bryssel den 29 mars 2022
(OR. en)

**Interinstitutionellt ärende:
2022/0084(COD)**

**7670/22
ADD 1**

**CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34**

FÖRSLAG

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	22 mars 2022
till:	Jeppe TRANHOLM-MIKKELSEN, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	COM(2022) 119 final - Annex 1
Ärende:	BILAGA till förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om informationssäkerhet i unionens institutioner, organ och byråer

För delegationerna bifogas dokument – COM(2022) 119 final - Annex 1.

Bilaga: COM(2022) 119 final - Annex 1



EUROPEISKA
KOMMISSIONEN

Bryssel den 22.3.2022
COM(2022) 119 final

ANNEX 1

BILAGA

till

förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om informationssäkerhet i unionens institutioner, organ och byråer

{SWD(2022) 65 final} - {SWD(2022) 66 final}

BILAGA I

Skyddsåtgärder för hantering av känsliga icke-säkerhetsskyddsklassificerade uppgifter

Märkning och hantering av känsliga icke-säkerhetsskyddsklassificerade uppgifter

1. Handlingar som innehåller känsliga icke-säkerhetsskyddsklassificerade uppgifter ska märkas med en säkerhetsmärkning och, vid behov, en eller flera distributionsmärkningar eller märkningar som anger målgruppen, beroende på vad som är lämpligt. Standardsäkerhetsmärkningen ska vara ordet SENSITIVE med versaler, utom i de fall som avses i artikel 15.2.
2. Handlingar som innehåller känsliga icke-säkerhetsskyddsklassificerade uppgifter får endast vara tillgängliga för mottagare med behovsenlig behörighet för officiella ändamål. Om distributionsmärkningar används måste tillstånd begäras från den EU-institution eller det EU-organ som utfärdat handlingen för att utöka distributionen av en handling.
3. Alla personer som hanterar känsliga icke-säkerhetsskyddsklassificerade uppgifter måste göras medvetna om hanteringsanvisningarna.
4. Handlingar märkta med SENSITIVE sänks till EU NORMAL eller PUBLIC USE genom att märkningarna tas bort eller stryks över.
5. När unionens institutioner och organ förstör handlingar som innehåller känsliga icke-säkerhetsskyddsklassificerade uppgifter måste detta göras på ett sådant sätt att de inte kan rekonstrueras på ett enkelt sätt. Papperskopior ska köras genom dokumentförstörare och elektroniska kopior måste på ett säkert sätt överskrivas, fysiskt förstöras eller på annat sätt göras omöjliga att återskapa.

Skydd av känsliga icke-säkerhetsskyddsklassificerade uppgifter vid arbete utanför EU-institutioners och EU-organs anläggningar

6. Känsliga icke-säkerhetsskyddsklassificerade uppgifter måste skyddas från avlyssning och observation vid distansarbete och uppdrag utanför kontoret och får inte hanteras eller lagras offentligt.
7. Handlingar som innehåller känsliga icke-säkerhetsskyddsklassificerade uppgifter får endast hanteras och lagras på utrustning eller applikationer som på lämpligt sätt har säkrats under EU-institutionernas och EU-organens ansvar.
8. Unionens institutioner och organ måste tillhandahålla medel för att hindra obehöriga personer, inbegripet släktingar, från att få tillgång till känsliga icke-säkerhetsskyddsklassificerade uppgifter som hanteras eller lagras på en EU-institutions eller ett EU-organs utrustning vid arbete utanför anställningsplatsen.
9. Unionens institutioner och organ måste instruera sin personal att
 - a) skydda EU-institutionernas eller EU-organens utrustning som hanterar känsliga icke-säkerhetsskyddsklassificerade uppgifter från stöld, förlust och skada och omedelbart rapportera alla negativa säkerhetshändelser som påverkar deras enheter eller uppgifter på enheterna,
 - b) inte dela sina enheter med obehöriga personer,
 - c) inte använda utrustningen för verksamhet som inte är arbetsrelaterad.

10. Unionens institutioner och organ måste säkerställa att deras utrustning eller på lämpligt sätt skyddade applikationer så långt det är möjligt används för att hantera och lagra känsliga icke-säkerhetsskyddsklassificerade handlingar i elektroniskt format utanför deras anläggningar. Hantering av fysiska kopior av känsliga icke-säkerhetsskyddsklassificerade handlingar utanför kontoret bör undvikas.
11. Om verktyg för telefonkonferenser eller videokonferenser används måste unionens institutioner och organ minimera risken för att obehöriga personer ser eller hör diskussionerna genom att på lämpligt sätt autentisera deltagarna och använda krypterade kommunikationsverktyg som är kompatibla med den behovsenliga behörigheten.
12. Unionens institutioner och organ ska tillhandahålla utbildning för all personal som arbetar på distans med hantering av känsliga icke-säkerhetsskyddsklassificerade uppgifter när de arbetar utanför kontoret.

Utbyte av känsliga icke-säkerhetsskyddsklassificerade uppgifter

13. Handlingar som innehåller känsliga icke-säkerhetsskyddsklassificerade uppgifter får delas mellan unionens institutioner och organ utan ytterligare formaliteter.
14. Unionens institutioner och organ får endast utbyta handlingar som innehåller känsliga icke-säkerhetsskyddsklassificerade uppgifter utanför unionens samtliga institutioner och organ på grundval av ett åtagande som binder parterna att följa hanteringsanvisningarna.
15. Unionens institutioner och organ måste underrätta mottagarna av känsliga icke-säkerhetsskyddsklassificerade uppgifter om skyldigheten att inte dela uppgifterna med någon part utöver den målgrupp som anges genom distributionsmärkningarna, såvida inte upphovsmannen tillåter det.
16. Unionens institutioner och organ måste skydda känsliga icke-säkerhetsskyddsklassificerade uppgifter som tillhandahålls eller delas elektroniskt genom lämpliga säkerhetsåtgärder, inbegripet kryptering vid överföring med hjälp av lämpliga kryptografiska mekanismer.