COUNCIL OF THE EUROPEAN UNION

Brussels, 27 November 2009 (OR. en)

13885/1/09 REV 1

LIMITE

CSC 33

LEGISLATIVE ACTS AND OTHER INSTRUMENTS

Subject: COUNCIL DECISION on the security rules for protecting EU classified information

COUNCIL DECISION

of

on the security rules for protecting EU classified information

(…/…/...)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 240(3) thereof,

Having regard to Council Decision …/…/… of … adopting the Council's Rules of Procedure[1*], and in particular Article 24 thereof,

---

[1] OJ L … .

[*] OJ: Please insert the number, the date of adoption and the publication reference of doc. 16525/09.

Whereas:

(1) In order to develop Council activities in all areas which require handling classified information, it is appropriate to establish a comprehensive security system for protecting classified information covering the Council, its General Secretariat and the Member States.

(2) This Decision should apply where the Council, its preparatory bodies and the General Secretariat of the Council (GSC) handle EU classified information (EUCI).

(3) In accordance with national laws and regulations and to the extent required for the functioning of the Council, the Member States should respect this Decision where their competent authorities, personnel or contractors handle EUCI, in order that each may be assured that an equivalent level of protection is afforded to EUCI.

(4) The Council and the Commission are committed to applying equivalent security standards for protecting EUCI.

(5) The Council underlines the importance of associating, where appropriate, the European Parliament and other EU institutions, agencies, bodies or offices with the principles, standards and rules for protecting classified information which are necessary in order to protect the interests of the Union and its Member States.

(6) EU agencies and bodies established under TitleV, Chapter 2, of the Treaty on European Union, Europol and Eurojust apply, in the context of their internal organisation, the basic principles and minimum standards laid down in this Decision for protecting EUCI, as provided for in their respective founding acts.

(7) Crisis management operations established under Title V, Chapter 2, of the TEU and their personnel apply the security rules adopted by the Council for protecting EUCI.

(8) EU Special Representatives and the members of their teams apply the security rules adopted by the Council for protecting EUCI.

(9) This Decision is taken without prejudice to Articles 15 and 16 of the Treaty on the Functioning of the European Union (TFEU) and to instruments implementing them.

(10) This Decision is taken without prejudice to existing practices in Member States with regard to informing their national Parliaments about the activities of the Union,

HAS ADOPTED THIS DECISION:

Article 1

Purpose, scope and definitions

1. This Decision lays down the basic principles and minimum standards of security for protecting EUCI.

2. These basic principles and minimum standards shall apply to the Council and the GSC and be respected by the Member States in accordance with their respective national laws and regulations, in order that each may be assured that an equivalent level of protection is afforded to EUCI.

3. For the purposes of this Decision, the definitions set out in Appendix A shall apply.

Article 2

Definition of EUCI, security classifications and markings

1. "EU classified information" (EUCI) means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.

2. EUCI shall be classified at one of the following levels:

   (a) TRES SECRET UE/EU TOP SECRET: information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States.

   (b) SECRET UE/EU SECRET: information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States.

   (c) CONFIDENTIEL UE/EU CONFIDENTIAL: information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States.

   (d) RESTREINT UE/EU RESTRICTED: information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.

3. EUCI shall bear a security classification marking in accordance with paragraph 2. It may bear additional markings to designate the field of activity to which it relates, identify the originator, limit distribution, restrict use or indicate releasability.

Article 3

Classification management

1. The competent authorities shall ensure that EUCI is appropriately classified, clearly identified as classified information and retains its classification level for only as long as necessary.

2. EUCI shall not be downgraded or declassified nor shall any of the markings referred to in Article 2(3) be modified or removed without the prior written consent of the originator.

3. The Council shall approve a security policy on creating EUCI which shall include a practical classification guide.

Article 4

Protection of classified information

1. EUCI shall be protected in accordance with this Decision.

2. The holder of any item of EUCI shall be responsible for protecting it in accordance with this Decision.

3. Where Member States introduce classified information bearing a national security classification marking into the structures or networks of the European Union, the Council and the GSC shall protect that information in accordance with the requirements applicable to EUCI at the equivalent level as set out in the table of equivalence of security classifications contained in Appendix B.

4. Large quantities or a compilation of EUCI may warrant a level of protection corresponding to a higher classification.

Article 5

Security risk management

1. Risk to EUCI shall be managed as a process. This process shall be aimed at determining known security risks, defining security measures to reduce such risks to an acceptable level in accordance with the basic principles and minimum standards set out in this Decision and at applying these measures in line with the concept of defence in depth as defined in Appendix A. The effectiveness of such measures shall be continuously evaluated.

2. Security measures for protecting EUCI throughout its life-cycle shall be commensurate in particular with its security classification, the form and the volume of the information or material, the location and construction of facilities housing EUCI and the locally assessed threat of malicious and/or criminal activities, including espionage, sabotage and terrorism.

3. Contingency plans shall take account of the need to protect EUCI during emergency situations in order to prevent unauthorised access, disclosure or loss of integrity or availability.

4. Preventive and recovery measures to minimise the impact of major failures or incidents on the handling and storage of EUCI shall be included in business continuity plans.

Article 6

Implementation of this Decision

1. Where necessary, the Council, on recommendation by the Security Committee, shall approve security policies setting out measures for implementing this Decision.

2. The Security Committee may agree at its level security guidelines to supplement or support this Decision and any security policies approved by the Council.

Article 7

Personnel security

1. Personnel security is the application of measures to ensure that access to EUCI is granted only to individuals who have:

   – a need-to-know;

   – been security cleared to the relevant level, where appropriate; and

   – been briefed on their responsibilities.

2. Personnel security clearance procedures shall be designed to determine whether an individual, taking into account his loyalty, trustworthiness and reliability, may be authorised to access EUCI.

3. All individuals in the GSC whose duties may require them to have access to EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be security cleared to the relevant level before being granted access to such EUCI. The personnel security clearance procedure for GSC officials and other servants is set out in Annex I.

4. Member States' personnel referred to in Article 14(3) whose duties may require access to EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be security cleared to the relevant level or otherwise duly authorised by virtue of their functions, in accordance with national laws and regulations, before being granted access to such EUCI.

5. Before being granted access to EUCI and at regular intervals thereafter, all individuals shall be briefed on and acknowledge their responsibilities to protect EUCI in accordance with this Decision.

6. Provisions for implementing this Article are set out in Annex I.

Article 8

Physical security

1. Physical security is the application of physical and technical protective measures to prevent unauthorised access to EUCI.

2. Physical security measures shall be designed to deny surreptitious or forced entry by an intruder, to deter, impede and detect unauthorised actions and to allow for segregation of personnel in their access to EUCI on a need-to-know basis. Such measures shall be determined based on a risk management process.

3. Physical security measures shall be put in place for all premises, buildings, offices, rooms and other areas in which EUCI is handled or stored, including areas housing communication and information systems as defined in Article 10(2).

4. Areas in which EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is stored shall be established as Secured Areas in accordance with Annex II and approved by the competent security authority.

5. Only approved equipment or devices shall be used for protecting EUCI at the level CONFIDENTIEL UE/EU CONFIDENTIAL or above.

6. Provisions for implementing this Article are set out in Annex II.

Article 9

Management of classified information

1. The management of classified information is the application of administrative measures for controlling EUCI throughout its life-cycle to supplement the measures provided for in Articles 7, 8 and 10 and thereby help deter, detect and recover from deliberate or accidental compromise or loss of such information. Such measures relate in particular to the creation, registration, copying, translation, carriage and destruction of EUCI.

2. Information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be registered for security purposes prior to distribution and on receipt. The competent authorities in the GSC and in the Member States shall establish a registry system for this purpose. Information classified TRES SECRET UE/EU TOP SECRET shall be registered in designated registries.

3. Services and premises where EUCI is handled or stored shall be subject to regular inspection by the competent security authority.

4. EUCI shall be conveyed between services and premises outside physically protected areas as follows:

   (a) as a general rule, EUCI shall be transmitted by electronic means protected by cryptographic products approved in accordance with Article 10(6);

   (b) when the means referred to in point (a) are not used, EUCI shall be carried either:

      (i) on electronic media (e.g. USB sticks, CDs, hard drives) protected by cryptographic products approved in accordance with Article 10(6); or

      (ii) in all other cases, as prescribed by the competent security authority in accordance with the relevant protective measures laid down in Annex III.

5. Provisions for implementing this Article are set out in Annex III.

Article 10

Protection of EUCI handled

in communication and information systems

1. Information Assurance (IA) in the field of communication and information systems is the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Effective IA shall ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity. IA shall be based on a risk management process.

2. "Communication and Information System" means any system enabling the handling of information in electronic form. A communication and information system shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources. This Decision shall apply to Communication and Information Systems handling EUCI (CIS).

3. CIS shall handle EUCI in accordance with the concept of IA.

4. All CIS shall undergo an accreditation process. Accreditation shall aim at obtaining assurance that all appropriate security measures have been implemented and that a sufficient level of protection of the EUCI and of the CIS has been achieved in accordance with this Decision. The accreditation statement shall determine the maximum classification level of the information that may be handled in a CIS as well as the corresponding terms and conditions.

5. CIS handling information classified CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be protected in such a way that the information cannot be compromised by unintentional electromagnetic emanations ("TEMPEST security measures").

6. Where the protection of EUCI is provided by cryptographic products, such products shall be approved as follows:

   (a) the confidentiality of information classified SECRET UE/EU SECRET and above shall be protected by cryptographic products approved by the Council as Crypto Approval Authority (CAA), upon recommendation by the Security Committee;

   (b) the confidentiality of information classified CONFIDENTIEL UE/EU CONFIDENTIAL or RESTREINT UE/EU RESTRICTED shall be protected by cryptographic products approved by the Secretary-General of the Council (hereinafter referred to as "the Secretary-General") as CAA, upon recommendation by the Security Committee.

   Notwithstanding point (b), within Member States' national systems, the confidentiality of EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or RESTREINT UE/EU RESTRICTED may be protected by cryptographic products approved by a Member State's CAA.

7. During transmission of EUCI by electronic means, approved cryptographic products shall be used. Notwithstanding this requirement, specific procedures may be applied under emergency circumstances or specific technical configurations as specified in Annex IV.

8. The competent authorities of the GSC and of the Member States respectively shall establish the following IA functions:

(a) an IA Authority (IAA);

(b) a TEMPEST Authority (TA);

(c) a Crypto Approval Authority (CAA);

(d) a Crypto Distribution Authority (CDA).

9. For each system, the competent authorities of the GSC and of the Member States respectively shall establish:

(a) a Security Accreditation Authority (SAA);

(b) an IA Operational Authority.

10. Provisions for implementing this Article are set out in Annex IV.

Article 11

Industrial security

1. Industrial security is the application of measures to ensure the protection of EUCI by contractors or subcontractors in pre-contract negotiations and throughout the life-cycle of classified contracts. Such contracts shall not involve access to information classified TRES SECRET UE/EU TOP SECRET.

2. The GSC may entrust by contract tasks involving or entailing access to or the handling or storage of EUCI by industrial or other entities registered in a Member State or in a third State which has concluded an agreement or an administrative arrangement in accordance with Article 12(2)(a) or (b).

3. The GSC, as contracting authority, shall ensure that the minimum standards on industrial security set out in this Decision, and referred to in the contract, are complied with when awarding classified contracts to industrial or other entities.

4. The National Security Authority (NSA), the Designated Security Authority (DSA) or any other competent authority of each Member State shall ensure, to the extent possible under national laws and regulations, that contractors and subcontractors registered in their territory take all appropriate measures to protect EUCI in pre-contract negotiations and when performing a classified contract.

5. The NSA, DSA or any other competent security authority of each Member State shall ensure, in accordance with national laws and regulations, that contractors or subcontractors registered in the said Member State participating in classified contracts or sub-contracts which require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET within their facilities, either in the performance of such contracts or during the pre-contractual stage, hold a Facility Security Clearance (FSC) at the relevant classification level.

6. Contractor or subcontractor personnel who, for the performance of a classified contract, require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be granted a Personnel Security Clearance (PSC) by the respective NSA, DSA or any other competent security authority in accordance with national laws and regulations and the minimum standards laid down in Annex I.

7. Provisions for implementing this Article are set out in Annex V.

Article 12

Exchange of classified information

with third States and international organisations

1. Where the Council determines that there is a need to exchange EUCI with a third State or international organisation, an appropriate framework shall be put in place to that effect.

2. In order to establish such a framework and define reciprocal rules on the protection of classified information exchanged,

   (a) the Council shall conclude agreements on security procedures for exchanging and protecting classified information (hereinafter referred to as "security of information agreements"); or

   (b) the Secretary-General may enter into administrative arrangements in accordance with paragraph 17 of Annex VI where the classification level of EUCI to be released is as a general rule no higher than RESTREINT UE/EU RESTRICTED.

3. Security of information agreements or administrative arrangements referred to in paragraph 2 shall contain provisions to ensure that when third States or international organisations receive EUCI, such information is given protection appropriate to its classification level and according to minimum standards which are no less stringent than those laid down in this Decision.

4. The decision to release EUCI originating in the Council to a third State or international organisation shall be taken by the Council on a case-by-case basis, according to the nature and content of such information, the recipient's need-to-know and the measure of advantage to the EU. If the originator of the classified information for which release is desired is not the Council, the GSC shall first seek the originator's written consent to release. If the originator cannot be established, the Council shall assume the former's responsibility.

5. Assessment visits shall be arranged to ascertain the effectiveness of the security measures in place in a third State or international organisation for protecting EUCI provided or exchanged.

6. Provisions for implementing this Article are set out in Annex VI.

Article 13

Breaches of security and compromise of EUCI

1. A breach of security occurs as the result of an act or omission by an individual which is contrary to the security rules laid down in this Decision.

2. Compromise of EUCI occurs when, as a result of a breach of security, it has wholly or in part been disclosed to unauthorised persons.

3. Any breach or suspected breach of security shall be reported immediately to the competent security authority.

4. Where it is known or where there are reasonable grounds to assume that EUCI has been compromised or lost, the competent security authority shall take all appropriate measures in accordance with the relevant laws and regulations to:

   (a) inform the originator;

   (b) ensure that the case is investigated by personnel not immediately concerned with the breach in order to establish the facts;

   (c) assess the potential damage caused to the interests of the EU or of the Member States;

   (d) take appropriate measures to prevent a recurrence; and

   (e) notify the appropriate authorities of the action taken.

5. Any individual who is responsible for a breach of the security rules laid down in this Decision may be liable to disciplinary action in accordance with the applicable rules and regulations. Any individual who is responsible for compromising or losing EUCI shall be liable to disciplinary and/or legal action in accordance with the applicable laws, rules and regulations.

Article 14

Responsibility for implementation

1. The Council shall take all necessary measures to ensure overall consistency in the application of this Decision.

2. The Secretary-General shall take all necessary measures to ensure that, when handling or storing EUCI or any other classified information, this Decision is applied in premises used by the Council and within the GSC, including in its liaison offices in third States, by GSC officials and other servants, by personnel seconded to the GSC and by GSC contractors.

3. Member States shall take all appropriate measures, in accordance with their respective national laws and regulations, to ensure that when EUCI is handled or stored, this Decision is respected by:

   (a) personnel of Member States' Permanent Representations to the European Union, and national delegates attending meetings of the Council or of its preparatory bodies, or participating in other Council activities;

   (b) other personnel in Member States' national administrations, including personnel seconded to those administrations, whether they serve on the territory of the Member States or abroad;

   (c) other persons in the Member States duly authorised by virtue of their functions to have access to EUCI; and

   (d) Member States' contractors, whether on the territory of the Member States or abroad.

Article 15

The organisation of security in the Council

1. As part of its role in ensuring overall consistency in the application of this Decision, the Council shall approve:

   (a) agreements referred to in Article 12(2)(a);

   (b) decisions authorising the release of EUCI to third States and international organisations;

   (c) an annual inspection programme proposed by the Secretary-General and recommended by the Security Committee for inspections of Member States' services and premises and of EU agencies and bodies established under Title V, Chapter 2 of the TEU as well as of Europol and Eurojust, and assessment visits to third States and international organisations in order to ascertain the effectiveness of measures implemented for protecting EUCI; and

   (d) security policies as foreseen in Article 6(1).

2. The Secretary-General shall be the GSC's Security Authority. In that capacity, the Secretary-General shall:

   (a) implement the Council's security policy and keep it under review;

   (b) coordinate with Member States' NSAs on all security matters relating to the protection of classified information relevant for the Council's activities;

   (c) grant EU PSCs to GSC officials and other servants in accordance with Article 7(3) before they may be granted access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above;

(d) as appropriate, order investigations into any actual or suspected compromise or loss of classified information held by or originating in the Council and request the relevant security authorities to assist in such investigations;

(e) undertake periodic inspections of the security arrangements for protecting classified information on GSC premises;

(f) undertake periodic inspections of the security arrangements for protecting EUCI in EU agencies and bodies established under Title V, Chapter 2, of the TEU, Europol, Eurojust, as well as in crisis management operations established under Title V, Chapter 2, of the TEU and by EU Special Representatives (EUSR) and the members of their teams;

(g) undertake, jointly and in agreement with the NSA concerned, periodic inspections of the security arrangements for protecting EUCI in Member States' services and premises;

(h) coordinate security measures with the competent authorities of the Member States which are responsible for protecting classified information and, as appropriate, third States or international organisations, including on the nature of threats to the security of EUCI and the means of protection against them;

(i) enter into the administrative arrangements referred to in Article 12(2)(b); and

(j) undertake initial and periodic assessment visits to third States or international organisations in order to ascertain the effectiveness of measures implemented for protecting EUCI provided to or exchanged with them.

The Security Office of the GSC shall be at the disposal of the Secretary-General to assist in these responsibilities.

3. For the purposes of implementing Article 14(3), Member States should:

(a) designate an NSA responsible for security arrangements for protecting EUCI in order that:

(i) EUCI held by any national department, body or agency, public or private, at home or abroad, is protected in accordance with this Decision;

(ii) security arrangements for protecting EUCI are periodically inspected;

(iii) all individuals employed within a national administration or by a contractor who may be granted access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above are appropriately security cleared or are otherwise duly authorised by virtue of their functions in accordance with national laws and regulations;

(iv) security programmes are set up as necessary in order to minimise the risk of EUCI being compromised or lost;

(v) security matters related to protecting EUCI are coordinated with other competent national authorities, including those referred to in this Decision; and

(vi) responses are given to appropriate security clearance requests from EU agencies and bodies established under Title V, Chapter 2 of the TEU, Europol, Eurojust, as well as crisis management operations established under Title V, Chapter 2, of the TEU and EUSRs and their teams.

NSAs are listed in Appendix C;

(b) ensure that their competent authorities provide information and advice to their governments, and through them to the Council, on the nature of threats to the security of EUCI and the means of protection against them.

Article 16

Security Committee

1. A Security Committee is hereby established. It shall examine and assess any security matter within the scope of this Decision and make recommendations to the Council as appropriate.

2. The Security Committee shall be composed of representatives of the Member States' NSAs and be attended by a representative of the Commission. It shall be chaired by the Secretary-General or by the Secretary-General's designated delegate. It shall meet as instructed by the Council, or at the request of the Secretary-General or of an NSA.

   Representatives of EU agencies and bodies established under Title V, Chapter 2, of the TEU, as well Europol and Eurojust, may be invited to attend when questions concerning them are discussed.

3. The Security Committee shall organise its activities in such a way that it can make recommendations on specific areas of security. It shall establish an expert sub-area for IA issues and other expert sub-areas as necessary. It shall draw up terms of reference for such expert sub-areas and receive reports from them on their activities including, as appropriate, any recommendations for the Council.

Article 17

Replacement of previous decision

1. This Decision shall repeal and replace Council Decision 2001/264/EC of 19 March 2001 adopting the Council's security regulations[1].

2. All EUCI classified in accordance with Council Decision 2001/264/EC shall continue to be protected in accordance with the relevant provisions of this Decision.

Article 18

Entry into force

This Decision shall apply from the date of its publication *in the Official Journal of the European Union*.

Done at Brussels,

For the Council

The President

---

1 OJ L 101, 11.4.2001, p. 1.

ANNEXES

ANNEX I

Personnel security

ANNEX II

Physical security

ANNEX III

Management of classified information

ANNEX IV

Protection of EUCI handled in CIS

ANNEX V

Industrial security

ANNEX VI

Exchange of classified information with third States and international organisations

ANNEX I

PERSONNEL SECURITY

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 7. It lays down in particular the criteria for determining whether an individual, taking into account his loyalty, trustworthiness and reliability, may be authorised to have access to EUCI and the investigative and administrative procedures to be followed to that effect.

2. Throughout this Annex, except where the distinction is relevant, the term "Personnel Security Clearance" shall refer to a national Personnel Security Clearance (national PSC) and/or an EU Personnel Security Clearance (EU PSC) as defined in Appendix A.

II. AUTHORISING ACCESS TO EUCI

3. An individual shall only be authorised to access information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above after:

   (a) his need-to-know has been determined;

   (b) he has been granted a PSC to the relevant level or is otherwise duly authorised by virtue of his functions in accordance with national laws and regulations; and

   (c) he has been briefed on the security rules and procedures for protecting EUCI and has acknowledged his responsibilities with regard to protecting such information.

4. Each Member State and the GSC shall identify the positions in their structures which require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above and therefore require a PSC to the relevant level.

III. PERSONNEL SECURITY CLEARANCE REQUIREMENTS

5. After having received a duly authorised request, NSAs or other competent national authorities shall be responsible for ensuring that security investigations are carried out on their nationals who require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above. Standards of investigation shall be in accordance with national laws and regulations.

6. Should the individual concerned reside in the territory of another Member State or of a third State, the competent national authorities shall seek assistance from the competent authority of the State of residence in accordance with national laws and regulations. Member States shall assist one another in carrying out security investigations in accordance with national laws and regulations.

7. Where permissible under national laws and regulations, NSAs or other competent national authorities may conduct investigations on non-nationals who require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above. Standards of investigation shall be in accordance with national laws and regulations.

Security investigation criteria

8. The loyalty, trustworthiness and reliability of an individual for the purposes of being granted a PSC for access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be determined by means of a security investigation. The competent national authority shall make an overall assessment based on the findings of such a security investigation. No single adverse finding shall necessarily constitute a reason to deny a PSC. The principal criteria used for that purpose should include, to the extent possible under national laws and regulations, an examination of whether the individual:

(a) has committed or attempted to commit, conspired with or aided and abetted another to commit any act of espionage, terrorism, sabotage, treason or sedition;

(b) is, or has been, an associate of spies, terrorists, saboteurs, or of individuals reasonably suspected of being such or an associate of representatives of organisations or foreign states, including foreign intelligence services, which may threaten the security of the EU and/or Member States unless these associations were authorised in the course of official duty;

(c) is, or has been, a member of any organisation which by violent, subversive or other unlawful means seeks, *inter alia*, to overthrow the government of a Member State, to change the constitutional order of a Member State or to change the form or the policies of its government;

(d) is, or has been, a supporter of any organisation described in point (c), or who is, or who has been closely associated with members of such organisations;

(e) has deliberately withheld, misrepresented or falsified information of significance, particularly of a security nature, or has deliberately lied in completing a personnel security questionnaire or during the course of a security interview;

(f) has been convicted of a criminal offence or offences;

(g) has a history of alcohol dependence, use of illegal drugs and/or misuse of legal drugs;

(h) is or has been involved in conduct which may give rise to the risk of vulnerability to blackmail or pressure;

(i) by act or through speech, has demonstrated dishonesty, disloyalty, unreliability or untrustworthiness;

(j) has seriously or repeatedly infringed security regulations; or has attempted, or succeeded in, unauthorised activity in respect of communication and information systems;

(k) may be liable to pressure (e.g. through holding one or more non-EU nationalities or through relatives or close associates who could be vulnerable to foreign intelligence services, terrorist groups or other subversive organisations, or individuals whose aims may threaten the security interests of the EU and/or Member States).

9. Where appropriate and in accordance with national laws and regulations, an individual's financial and medical background may also be considered relevant during the security investigation.

10. Where appropriate and in accordance with national laws and regulations, a spouse's, cohabitant's or close family member's character, conduct and circumstances may also be considered relevant during the security investigation.

Investigative requirements for access to EUCI

Initial granting of a PSC

11. The initial PSC for access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET shall be based on a security investigation covering at least the last five years, or from age 18 to the present, whichever is the shorter, which shall include the following:

(a) the completion of a national personnel security questionnaire for the level of EUCI to which the individual may require access; once completed, this questionnaire shall be forwarded to the competent security authority;

(b) identity check/citizenship/nationality status – the individual's date and place of birth shall be verified and his identity checked. Citizenship status and/or nationality, past and present, of the individual shall be established; this shall include an assessment of any vulnerability to pressure from foreign sources, for example, due to former residence or past associations; and

(c) national and local records check – a check shall be made of national security and central criminal records, where the latter exist, and/or other comparable governmental and police records. The records of law enforcement agencies with legal jurisdiction where the individual has resided or been employed shall be checked.

12. The initial PSC for access to information classified TRES SECRET UE/EU TOP SECRET shall be based on a security investigation covering at least the last ten years, or from age 18 to the present, whichever is the shorter. If interviews are conducted as stated in point (e), investigations shall cover at least the last seven years, or from age 18 to the present, whichever is the shorter. In addition to the criteria indicated in paragraph 8 above, the following elements shall be investigated, to the extent possible under national laws and regulations, before granting a TRES SECRET UE/EU TOP SECRET PSC; they may also be investigated before granting a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET PSC, where required by national laws and regulations:

(a) financial status – information shall be sought on the individual's finances in order to assess any vulnerability to foreign or domestic pressure due to serious financial difficulties, or to discover any unexplained affluence;

(b) education – information shall be sought to verify the individual's educational background at schools, universities and other education establishments attended since his 18th birthday, or during a period judged appropriate by the investigating authority;

(c) employment – information covering present and former employment shall be sought, reference being made to sources such as employment records, performance or efficiency reports and to employers or supervisors;

(d) military service – where applicable, the service of the individual in the armed forces and type of discharge shall be verified; and

(e) interviews – where provided for and admissible under national law, an interview or interviews shall be conducted with the individual. Interviews shall also be conducted with other individuals who are in a position to give an unbiased assessment of the individual's background, activities, loyalty, trustworthiness and reliability. When it is national practice to ask the subject of the investigation for referrals, referees shall be interviewed unless there are good reasons for not doing so.

13. Where necessary and in accordance with national laws and regulations, additional investigations may be conducted to develop all relevant information available on an individual and to substantiate or disprove adverse information.

Renewal of a PSC

14. After the initial granting of a PSC and provided that the individual has had uninterrupted service with a national administration or the GSC and has a continuing need for access to EUCI, the PSC shall be reviewed for renewal at intervals not exceeding five years for a TRES SECRET UE/EU TOP SECRET clearance and ten years for SECRET UE/EU SECRET and CONFIDENTIEL UE/EU CONFIDENTIAL clearances, with effect from the date of notification of the outcome of the last security investigation on which they were based. All security investigations for the renewal of a PSC shall cover the period since the previous such investigation.

15. For the renewal of PSCs, the elements outlined in paragraphs 11 and 12 shall be investigated.

16. Requests for renewal shall be made in a timely manner taking account of the time required for security investigations. Nevertheless, where the relevant NSA or other competent national authority has received the relevant request for renewal and the corresponding personnel security questionnaire before a PSC expires, and the necessary security investigation has not been completed, the competent national authority may, where admissible under national laws and regulations, extend the validity of the existing PSC for a period of up to 12 months. If, at the end of this 12-month period, the security investigation has still not been completed, the individual shall be assigned to duties which do not require a PSC.

PSC procedures in the GSC

17. For officials and other servants in the GSC, the GSC Security Authority shall forward the completed personnel security questionnaire to the NSA of the Member State of which the individual is a national requesting that a security investigation be undertaken for the level of EUCI to which the individual will require access.

18. Where information relevant for a security investigation becomes known to the GSC concerning an individual who has applied for an EU PSC, the GSC, acting in accordance with the relevant rules and regulations, shall notify the relevant NSA thereof.

19. Following completion of the security investigation, the relevant NSA shall notify the GSC Security Authority of the outcome of such an investigation, using the standard format for the correspondence prescribed by the Security Committee.

(a) Where the security investigation results in an assurance that nothing adverse is known which would call into question the loyalty, trustworthiness and reliability of the individual, the GSC Appointing Authority may grant an EU PSC to the individual concerned and authorise access to EUCI up to the relevant level until a specified date;

(b) Where the security investigation does not result in such an assurance, the GSC Appointing Authority shall notify the individual concerned, who may ask to be heard by the Appointing Authority. The Appointing Authority may ask the competent NSA for any further clarification it can provide according to its national laws and regulations. If the outcome is confirmed, an EU PSC shall not be granted.

20. The security investigation together with the results obtained shall be subject to the relevant laws and regulations in force in the Member State concerned, including those concerning appeals. Decisions by the GSC Appointing Authority shall be subject to appeals in accordance with the Staff Regulations of Officials of the European Communities and the Conditions of employment of other servants of the European Communities, laid down in Regulation (EEC, Euratom, ECSC) No 259/68[1] (hereinafter referred to as "the Staff Regulations and Conditions of employment").

21. The assurance on which an EU PSC is based, provided it remains valid, shall cover any assignment by the individual concerned within the GSC or the Commission.

22. If an individual's period of service does not commence within 12 months of the notification of the outcome of the security investigation to the GSC Appointing Authority, or if there is a break of 12 months in an individual's service, during which time he has not been employed in the GSC or in a position with a national administration of a Member State, this outcome shall be referred to the relevant NSA for confirmation that it remains valid and appropriate.

23. Where information becomes known to the GSC concerning a security risk posed by an individual who holds a valid EU PSC, the GSC, acting in accordance with the relevant rules and regulations, shall notify the relevant NSA thereof. Where an NSA notifies the GSC of withdrawal of an assurance given in accordance with paragraph 19(a) for an individual who holds a valid EU PSC, the GSC Appointing Authority may ask for any clarification the NSA can provide according to its national laws and regulations. If the adverse information is confirmed, the EU PSC shall be withdrawn and the individual shall be excluded from access to EUCI and from positions where such access is possible or where he might endanger security.

---

[1] OJ L 56, 4.3.1968, p.1

24. Any decision to withdraw an EU PSC from a GSC official or other servant and, where appropriate, the reasons for doing so shall be notified to the individual concerned, who may ask to be heard by the Appointing Authority. Information provided by an NSA shall be subject to the relevant laws and regulations in force in the Member State concerned, including those concerning appeals. Decisions by the GSC Appointing Authority shall be subject to appeals in accordance with the Staff Regulations and Conditions of employment.

25. National experts seconded to the GSC for a position requiring an EU PSC shall present a valid national PSC for access to EUCI to the GSC Security Authority prior to taking up their assignment.

Records of PSCs

26. Records of national PSCs and EU PSCs granted for access to EUCI shall be maintained respectively by each Member State and by the GSC. These records shall contain as a minimum the level of EUCI to which the individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the date the PSC was granted and its period of validity.

27. The competent security authority may issue a Personnel Security Clearance Certificate (PSCC) showing the level of EUCI to which the individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the date of validity of the relevant national PSC for access to EUCI or EU PSC and the date of expiry of the certificate itself.

Exemptions from the PSC requirement

28. Access to EUCI by individuals in Member States duly authorised by virtue of their functions shall be determined in accordance with national laws and regulations; such individuals shall be briefed on their security obligations in respect of protecting EUCI.

IV. SECURITY EDUCATION AND AWARENESS

29. All individuals who have been granted a PSC shall acknowledge in writing that they have understood their obligations in respect of protecting EUCI and the consequences if EUCI is compromised. A record of such a written acknowledgement shall be kept by the Member State and by the GSC, as appropriate.

30. All individuals who are authorised to have access to, or required to handle EUCI, shall initially be made aware, and periodically briefed on the threats to security and must report immediately to the appropriate security authorities any approach or activity that they consider suspicious or unusual.

31. All individuals who cease to be employed in duties requiring access to EUCI shall be made aware of, and where appropriate acknowledge in writing, their obligations in respect of the continued protection of EUCI.

V. EXCEPTIONAL CIRCUMSTANCES

32. Where permissible under national laws and regulations, a personnel security clearance granted by a competent national authority of a Member State for access to national classified information may, for a temporary period pending the granting of a national PSC for access to EUCI, allow access by national officials to EUCI up to the equivalent level specified in the table of equivalence in Appendix B where such temporary access is required in the interests of the EU. NSAs shall inform the Security Committee where national laws and regulations do not permit such temporary access to EUCI.

33. For reasons of urgency, where duly justified in the interests of the service and pending completion of a full security investigation, the GSC Appointing Authority may, after consulting the NSA of the Member State of whom the individual is a national and subject to the outcome of preliminary checks to verify that no adverse information is known, grant a temporary authorisation for GSC officials and other servants to access EUCI for a specific function. Such temporary authorisations shall be valid for a period not exceeding six months and shall not permit access to information classified TRES SECRET UE/EU TOP SECRET. All individuals who have been granted a temporary authorisation shall acknowledge in writing that they have understood their obligations in respect of protecting EUCI and the consequences if EUCI is compromised. A record of such a written acknowledgement shall be kept by the GSC.

34. When an individual is to be assigned to a position that requires a PSC at one level higher than that currently possessed by the individual, the assignment may be made on a provisional basis, provided that:

(a) the compelling need for access to EUCI at a higher level shall be justified, in writing, by the individual's superior;

(b) access shall be limited to specific items of EUCI in support of the assignment;

(c) the individual holds a valid national PSC or EU PSC;

(d) action has been initiated to obtain authorisation for the level of access required for the position;

(e) satisfactory checks have been made by the competent authority that the individual has not seriously or repeatedly infringed security regulations;

(f) the assignment of the individual is approved by the competent authority; and

(g) a record of the exception, including a description of the information to which access was approved, shall be kept by the registry or subordinate registry responsible.

35. The above procedure shall be used for one-time access to EUCI at one level higher than that to which the individual has been security cleared. Recourse to this procedure shall not be made on a recurring basis.

36. In very exceptional circumstances, such as missions in hostile environments or during periods of mounting international tension when emergency measures require it, in particular for the purposes of saving lives, Member States and the Secretary-General may grant, where possible in writing, access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET to individuals who do not possess the requisite PSC, provided that such permission is absolutely necessary and there are no reasonable doubts as to the loyalty, trustworthiness and reliability of the individual concerned. A record shall be kept of this permission describing the information to which access was approved.

37. In the case of information classified TRES SECRET UE/EU TOP SECRET, this emergency access shall be confined to EU nationals who have been authorised access to either the national equivalent of TRES SECRET UE/EU TOP SECRET or information classified SECRET UE/EU SECRET.

38. The Security Committee shall be informed of cases when recourse is made to the procedure set out in paragraphs 36 and 37.

39. Where national laws and regulations of a Member State stipulate more stringent rules with respect to temporary authorisations, provisional assignments, one-time access or emergency access by individuals to classified information, the procedures foreseen in this Section shall be implemented only within any limitations set forth in the relevant national laws and regulations.

40. The Security Committee shall receive an annual report on recourse to the procedures set out in this section.

VI. ATTENDANCE AT MEETINGS IN THE COUNCIL

41. Subject to paragraph 28, individuals assigned to participate in meetings of the Council or of Council preparatory bodies at which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is discussed may only do so upon confirmation of the individual's PSC status. For delegates, a PSCC or other proof of PSC shall be forwarded by the appropriate authorities to the GSC Security Office, or exceptionally be presented by the delegate concerned. Where applicable, a consolidated list of names may be used, giving the relevant proof of PSC.

42. Where a national PSC for access to EUCI is withdrawn for security reasons from an individual whose duties require attendance at meetings of the Council or of Council preparatory bodies, the competent authority shall inform the GSC thereof.

VII. POTENTIAL ACCESS TO EUCI

43. When individuals are to be employed in circumstances in which they may potentially have access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, they shall be appropriately security cleared or escorted at all times.

44. Couriers, guards and escorts shall be security cleared to the relevant level or otherwise appropriately investigated in accordance with national laws and regulations, be briefed on security procedures for protecting EUCI and be instructed on their duties for protecting such information entrusted to them.

ANNEX II

PHYSICAL SECURITY

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 8. It lays down minimum requirements for the physical protection of premises, buildings, offices, rooms and other areas where EUCI is handled and stored, including areas housing CIS.

2. Physical security measures shall be designed to prevent unauthorised access to EUCI by:

   (a) ensuring that EUCI is handled and stored in an appropriate manner;

   (b) allowing for segregation of personnel in terms of access to EUCI on the basis of their need-to-know and, where appropriate, their security clearance;

   (c) deterring, impeding and detecting unauthorised actions; and

   (d) denying or delaying surreptitious or forced entry by intruders.

II. PHYSICAL SECURITY REQUIREMENTS AND MEASURES

3. Physical security measures shall be selected on the basis of a threat assessment made by the competent authorities. The GSC and Member States shall each apply a risk management process for protecting EUCI on their premises to ensure that a commensurate level of physical protection is afforded against the assessed risk. The risk management process shall take account of all relevant factors, in particular:

(a) the classification level of EUCI;

(b) the form and volume of EUCI, bearing in mind that large quantities or a compilation of EUCI may require more stringent protective measures to be applied;

(c) the surrounding environment and structure of the buildings or areas housing EUCI; and

(d) the assessed threat from intelligence services which target the EU or Member States and from sabotage, terrorist, subversive or other criminal activities.

4. The competent security authority, applying the concept of defence in depth, shall determine the appropriate combination of physical security measures to be implemented. These can include one or more of the following:

(a) a perimeter barrier: a physical barrier which defends the boundary of an area requiring protection;

(b) intrusion detection systems (IDS): an IDS may be used to enhance the level of security offered by a perimeter barrier, or in rooms and buildings in place of, or to assist, security staff;

(c) access control: access control may be exercised over a site, a building or buildings on a site or to areas or rooms within a building. Control may be exercised by electronic or electro-mechanical means, by security personnel and/or a receptionist, or by any other physical means;

(d) security personnel: trained, supervised and, where necessary, appropriately security-cleared security personnel may be employed, *inter alia,* in order to deter individuals planning covert intrusion;

(e) closed circuit television (CCTV): CCTV may be used by security personnel in order to verify incidents and IDS alarms on large sites or at perimeters;

(f) security lighting: security lighting may be used to deter a potential intruder, as well as to provide the illumination necessary for effective surveillance directly by security personnel or indirectly through a CCTV system; and

(g) any other appropriate physical measures designed to deter or detect unauthorised access or prevent loss of or damage to EUCI.

5. The competent authority can be authorised to conduct entry and exit searches to act as a deterrent to the unauthorised introduction of material or the unauthorised removal of EUCI from premises or buildings.

6. When EUCI is at risk from overlooking, even accidentally, appropriate measures shall be taken to counter this risk.

7. For new facilities, physical security requirements and their functional specifications shall be defined as part of the planning and design of the facilities. For existing facilities, physical security requirements shall be implemented to the maximum extent possible.

III. EQUIPMENT FOR THE PHYSICAL PROTECTION OF EUCI

8. When acquiring equipment (such as security containers, shredding machines, door locks, electronic access control systems, IDS, alarm systems) for the physical protection of EUCI, the competent security authority shall ensure that the equipment meets approved technical standards and minimum requirements.

9. The technical specifications of equipment to be used for the physical protection of EUCI shall be set out in security guidelines to be approved by the Security Committee.

10. Security systems shall be inspected at regular intervals and equipment shall be maintained regularly. Maintenance work shall take account of the outcome of inspections to ensure that equipment continues to operate at optimum performance.

11. The effectiveness of individual security measures and of the overall security system shall be re-evaluated during each inspection.

IV. PHYSICALLY PROTECTED AREAS

12. Two types of physically protected areas, or the national equivalents thereof, shall be established for the physical protection of EUCI:

(a) Administrative Areas; and

(b) Secured Areas (including technically Secured Areas).

In this Decision, all references to Administrative Areas and Secured Areas, including technically Secured Areas, shall be understood as also referring to the national equivalents thereof.

13. The competent security authority shall establish that an area meets the requirements to be designated as an Administrative Area, a Secured Area or a technically Secured Area.

14. For Administrative Areas:

(a) a visibly defined perimeter shall be established which allows individuals and, where possible, vehicles to be checked;

(b) unescorted access shall be granted only to individuals who are duly authorised by the competent authority; and

(c) all other individuals shall be escorted at all times or be subject to equivalent controls.

15. For Secured Areas:

(a) a visibly defined and protected perimeter shall be established through which all entry and exit are controlled by means of a pass or personal recognition system;

(b) unescorted access shall be granted only to individuals who are security-cleared and specifically authorised to enter the area on the basis of their need-to-know;

(c) all other individuals shall be escorted at all times or be subject to equivalent controls.

16. Where entry into a Secured Area constitutes, for all practical purposes, direct access to the classified information contained in it, the following additional requirements shall apply:

(a) the level of highest security classification of the information normally held in the area shall be clearly indicated;

(b) all visitors shall require specific authorisation to enter the area, shall be escorted at all times and shall be appropriately security cleared unless steps are taken to ensure that no access to EUCI is possible.

17. Secured Areas protected against eavesdropping shall be designated technically Secured Areas. The following additional requirements shall apply:

(a) such areas shall be IDS equipped, be locked when not occupied and be guarded when occupied. Any keys shall be controlled in accordance with section VI;

(b) all persons and material entering such areas shall be controlled;

(c) such areas shall be regularly physically and/or technically inspected as required by the competent security authority. Such inspections shall also be conducted following any unauthorised entry or suspicion of such entry; and

(d) such areas shall be free of unauthorised communication lines, unauthorised telephones or other unauthorised communication devices and electrical or electronic equipment.

18. Notwithstanding point (d) of paragraph 17, before being used in areas where meetings are held or work is being performed involving information classified SECRET UE/EU SECRET and above, and where the threat to EUCI is assessed as high, any communications devices and electrical or electronic equipment shall first be examined by the competent security authority to ensure that no intelligible information can be inadvertently or illicitly transmitted by such equipment beyond the perimeter of the Secured Area.

19. Secured Areas which are not occupied by duty personnel on a 24-hour basis shall, where appropriate, be inspected at the end of normal working hours and at random intervals outside normal working hours, unless an IDS is in place.

20. Secured Areas and technically Secured Areas may be set up temporarily within an Administrative Area for a classified meeting or any other similar purpose.

21. Security operating procedures shall be drawn up for each Secured Area stipulating:

(a) the level of EUCI which may be handled and stored in the area;

(b) the surveillance and protective measures to be maintained;

(c) the individuals authorised to have unescorted access to the area by virtue of their need-to-know and security clearance;

(d) where appropriate, the procedures for escorts or for protecting EUCI when authorising any other individuals to access the area;

(e) any other relevant measures and procedures.

22. Strong rooms shall be constructed within Secured Areas. The walls, floors, ceilings, windows and lockable doors shall be approved by the competent security authority and afford protection equivalent to a security container approved for the storage of EUCI of the same classification level.

V. PHYSICAL PROTECTIVE MEASURES FOR HANDLING AND STORING EUCI

23. EUCI which is classified RESTREINT UE/EU RESTRICTED may be handled:

(a) in a Secured Area,

(b) in an Administrative Area provided the EUCI is protected from access by unauthorised individuals, or

(c) outside a Secured Area or an Administrative Area provided the holder carries the EUCI in accordance with paragraphs 28 to 40 of Annex III and has undertaken to comply with compensatory measures laid down in security instructions issued by the competent security authority to ensure that EUCI is protected from access by unauthorised persons.

24. EUCI which is classified RESTREINT UE/EU RESTRICTED shall be stored in suitable locked office furniture in an Administrative Area or a Secured Area. It may temporarily be stored outside a Secured Area or an Administrative Area provided the holder has undertaken to comply with compensatory measures laid down in security instructions issued by the competent security authority.

25. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET may be handled:

(a) in a Secured Area;

(b) in an Administrative Area provided the EUCI is protected from access by unauthorised individuals; or

(c) outside a Secured Area or an Administrative Area provided the holder:

(i) carries the EUCI in accordance with paragraphs 28 to 40 of Annex III;

(ii) has undertaken to comply with compensatory measures laid down in security instructions issued by the competent security authority to ensure that EUCI is protected from access by unauthorised persons;

(iii) keeps the EUCI at all times under his personal control; and

(iv) in the case of documents in paper form, has notified the relevant registry of the fact.

26. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET shall be stored in a Secured Area in a security container or strong room.

27. EUCI which is classified TRES SECRET UE/EU TOP SECRET shall be handled in a Secured Area.

28. EUCI which is classified TRES SECRET UE/EU TOP SECRET shall be stored in a Secured Area under one of the following conditions:

(a) in a security container in line with paragraph 8 with one or more of the following supplementary controls:

(i) continuous protection or verification by cleared security staff or duty personnel;

(ii) an approved IDS in combination with response security personnel;

or

(b) in an IDS-equipped strong room in combination with response security personnel.

29. Rules governing the carriage of EUCI outside physically protected areas are set out in Annex III.

VI. CONTROL OF KEYS AND COMBINATIONS USED FOR PROTECTING EUCI

30. The competent security authority shall define procedures for managing keys and combination settings for offices, rooms, strong rooms and security containers. Such procedures shall protect against unauthorised access.

31. Combination settings shall be committed to memory by the smallest possible number of individuals needing to know them. Combination settings for security containers and strong rooms storing EUCI shall be changed:

(a) whenever there is a change in personnel knowing the combination;

(b) whenever a compromise has occurred or is suspected;

(c) when a lock has undergone maintenance or repair; and

(d) at least every 12 months.

ANNEX III

MANAGEMENT OF CLASSIFIED INFORMATION

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 9. It lays down the administrative measures for controlling EUCI throughout its life-cycle in order to help deter, detect and recover from deliberate or accidental compromise or loss of such information.

II. CLASSIFICATION MANAGEMENT

Classifications and markings

2. Information shall be classified where it requires protection with regard to its confidentiality.

3. The originator of EUCI shall be responsible for determining the security classification level, in accordance with the relevant classification guidelines, and for the initial dissemination of the information.

4. The classification level of EUCI shall be determined in accordance with Article 2(2) and by reference to the security policy to be approved in accordance with Article 3(3).

5. The security classification shall be clearly and correctly indicated, regardless of whether the EUCI is on paper, oral, electronic or in any other form.

6. Individual parts of a given document (i.e. pages, paragraphs, sections, annexes, appendices, attachments and enclosures) may require different classifications and shall be marked accordingly, including when stored in electronic form.

7. The overall classification level of a document or file shall be at least as high as that of its most highly classified component. When information from various sources is collated, the final product shall be reviewed to determine its overall security classification level, since it may warrant a higher classification than its component parts.

8. To the extent possible, documents containing parts with different classification levels shall be structured so that parts with a different classification level may be easily identified and detached if necessary.

9. The classification of a letter or note covering enclosures shall be as high as the highest classification of its enclosures. The originator shall indicate clearly at which level it is classified when detached from its enclosures by means of an appropriate marking, e.g.:

CONFIDENTIEL UE/EU CONFIDENTIAL
Without attachment(s) RESTREINT UE/EU RESTRICTED

Markings

10. In addition to one of the security classification markings set out in Article 2(2), EUCI may bear additional markings, such as:

(a) an identifier to designate the originator;

(b) any caveats, code-words or acronyms specifying the field of activity to which the document relates, a particular distribution on a need-to-know basis or restrictions on use;

(c) releasability markings;

(d) where applicable, the date or specific event after which it may be downgraded or declassified.

Abbreviated classification markings

11. Standardised abbreviated classification markings may be used to indicate the classification level of individual paragraphs of a text. Abbreviations shall not replace the full classification markings.

12. The following standard abbreviations may be used within EU classified documents to indicate the classification level of sections or blocks of text of less than a single page:

TRES SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Creation of EUCI

13. When creating an EU classified document:

(a) each page shall be marked clearly with the classification level;

(b) each page shall be numbered;

(c) the document shall bear a reference number and a subject, which is not itself classified information, unless it is marked as such;

(d) the document shall be dated;

(e) documents classified SECRET UE/EU SECRET or above shall bear a copy number on every page, if they are to be distributed in several copies.

14. Where it is not possible to apply paragraph 13 to EUCI, other appropriate measures shall be taken in accordance with security guidelines to be established pursuant to Article 6(2).

Downgrading and declassification of EUCI

15. At the time of its creation, the originator shall indicate, where possible, and in particular for information classified RESTREINT UE/EU RESTRICTED, whether EUCI can be downgraded or declassified on a given date or following a specific event.

16. The GSC shall regularly review EUCI held by it to ascertain whether the classification level still applies. The GSC shall establish a system to review the classification level of registered EUCI which it has originated no less frequently than every five years. Such a review shall not be necessary where the originator has indicated from the outset that the information will automatically be downgraded or declassified and the information has been marked accordingly.

III. REGISTRATION OF EUCI FOR SECURITY PURPOSES

17. For every organisational entity within the GSC and Member States' national administrations in which EUCI is handled, a responsible registry shall be identified to ensure that EUCI is handled in accordance with this Decision. Registries shall be established as Secured Areas as defined in Annex II.

18. For the purposes of this Decision, registration for security purposes (hereinafter referred to as "registration") means the application of procedures which record the life-cycle of material, including its dissemination and destruction.

19. All material classified CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be registered in designated registries when it arrives at or leaves an organisational entity.

20. The Central Registry within the GSC shall keep a record of all classified information released by the Council and the GSC to third States and international organisations, and of all classified information received from third States or international organisations.

21. In the case of a CIS, registration procedures may be performed by processes within the CIS itself.

22. The Council shall approve a security policy on the registration of EUCI for security purposes.

TRES SECRET UE/EU TOP SECRET registries

23. A registry shall be designated in the Member States and in the GSC to act as the central receiving and dispatching authority for information classified TRES SECRET UE/EU TOP SECRET. Where necessary, subordinate registries may be designated to handle such information for registration purposes.

24. Such subordinate registries may not transmit TRES SECRET UE/EU TOP SECRET documents directly to other subordinate registries of the same central TRES SECRET UE/EU TOP SECRET registry or externally without the express written approval of the latter.

IV. COPYING AND TRANSLATING EU CLASSIFIED DOCUMENTS

25. TRES SECRET UE/EU TOP SECRET documents shall not be copied or translated without the prior written consent of the originator.

26. Where the originator of documents classified SECRET UE/EU SECRET and below has not imposed caveats on their copying or translation, such documents may be copied or translated on instruction from the holder.

27. The security measures applicable to the original document shall apply to copies and translations thereof.

V. CARRIAGE OF EUCI

28. Carriage of EUCI shall be subject to the protective measures set out in paragraphs 30 to 40. When EUCI is carried on electronic media, and notwithstanding Article 9(4), the protective measures set out below may be supplemented by appropriate technical countermeasures prescribed by the competent security authority so as to minimise the risk of loss or compromise.

29. The competent security authorities in the GSC and in Member States shall issue instructions on the carriage of EUCI in accordance with this Decision.

Within a building or self-contained group of buildings

30. EUCI carried within a building or self-contained group of buildings shall be covered in order to prevent observation of its contents.

31. Within a building or self-contained group of buildings, information classified TRES SECRET UE/EU TOP SECRET shall be carried in a secured envelope bearing only the addressee's name.

Within the EU

32. EUCI carried between buildings or premises within the EU shall be packaged so that it is protected from unauthorised disclosure.

33. The carriage of information classified up to SECRET UE/EU SECRET within the EU shall be by one of the following means:

(a) military, government or diplomatic courier, as appropriate;

(b) hand carriage, provided that:

(i) EUCI does not leave the possession of the bearer, unless it is stored in accordance with the requirements set out in Annex II;

(ii) EUCI is not opened *en route* or read in public places;

(iii) individuals are briefed on their security responsibilities;

(iv) individuals are provided with a courier certificate where necessary;

(c) postal services or commercial courier services, provided that:

(i) they are approved by the relevant NSA in accordance with national laws and regulations;

(ii) they apply appropriate protective measures in accordance with minimum requirements to be laid down in security guidelines pursuant to Article 6(2).

In the case of carriage from one Member State to another, the provisions of point (c) shall be limited to information classified up to CONFIDENTIEL UE/EU CONFIDENTIAL.

34. Material classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET (e.g. equipment or machinery) which cannot be carried by the means referred to in paragraph 33 shall be transported as freight by commercial carrier companies in accordance with Annex V.

35. The carriage of information classified TRES SECRET UE/EU TOP SECRET between buildings or premises within the EU shall be by military, government or diplomatic courier, as appropriate.

From within the EU to the territory of a third State

36. EUCI carried from within the EU to the territory of a third State shall be packaged in such a way that it is protected from unauthorised disclosure.

37. The carriage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET from within the EU to the territory of a third State shall be by one of the following means:

(a) military or diplomatic courier;

(b) hand carriage, provided that:

(i) the package bears an official seal, or is packaged so as to indicate that it is an official consignment and should not undergo customs or security scrutiny;

(ii) individuals carry a courier certificate identifying the package and authorising them to carry the package;

(iii) EUCI does not leave the possession of the bearer, unless it is stored in accordance with the requirements set out in Annex II;

(iv) EUCI is not opened *en route* or read in public places; and

(v) individuals are briefed on their security responsibilities.

38. The carriage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET released by the EU to a third State or international organisation shall comply with the relevant provisions under a security of information Agreement or an administrative arrangement in accordance with Article 12(2)(a) or (b).

39. Information classified RESTREINT UE/EU RESTRICTED may also be carried by postal services or commercial courier services.

40. The carriage of information classified TRES SECRET UE/EU TOP SECRET from within the EU to the territory of a third State shall be by military or diplomatic courier.

VI. DESTRUCTION OF EUCI

41. EU classified documents which are no longer required may be destroyed, without prejudice to the relevant rules and regulations on archiving.

42. Documents subject to registration in accordance with Article 9(2) shall be destroyed by the responsible registry on instruction from the holder or from a competent authority. The logbooks and other registration information shall be updated accordingly.

43. For documents classified SECRET UE/EU SECRET or TRES SECRET UE/EU TOP SECRET, destruction shall be performed in the presence of a witness who shall be cleared to at least the classification level of the document being destroyed.

44. The registrar and the witness, where the presence of the latter is required shall sign a destruction certificate, which shall be filed in the registry. The registry shall keep destruction certificates of TRES SECRET UE/EU TOP SECRET documents for a period of at least ten years and of documents CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET for a period of at least five years.

45. Classified documents, including those classified RESTREINT UE/EU RESTRICTED, shall be destroyed by methods which meet relevant EU or equivalent standards or which have been approved by Member States in accordance with national technical standards so as to prevent reconstruction in whole or in part.

46. The destruction of computer storage media used for EUCI shall be in accordance with paragraph 36 of Annex IV.

VII. INSPECTIONS AND ASSESSMENT VISITS

47. The term "inspection" shall be used hereinafter to designate any

(a) inspection in accordance with Article 9(3) and Article 15(2)(e), (f) and (g); or

(b) assessment visit in accordance with Article 12(5),

to evaluate the effectiveness of measures implemented for protecting EUCI.

48. Inspections shall be carried out, *inter alia* to:

(a) ensure that the required minimum standards for protecting EUCI laid down in this Decision are respected;

(b) emphasise the importance of security and effective risk management within the entities inspected;

(c) recommend countermeasures to mitigate the specific impact of loss of confidentiality, integrity or availability of classified information; and

(d) reinforce security authorities' ongoing security education and awareness programmes.

49. Before the end of each calendar year, the Council shall adopt the inspection programme foreseen in point (c) of Article 15(1) for the following year. The actual dates for each inspection shall be determined in agreement with the EU agency or body, Member State, third State or international organisation concerned.

Conduct of inspections

50. Inspections shall be conducted in order to check the relevant rules, regulations and procedures in the inspected entity and verify whether the entity's practices comply with the basic principles and minimum standards laid down in this Decision and in the provisions governing the exchange of classified information with that entity.

51. Inspections shall be conducted in two phases. Prior to the inspection itself a preparatory meeting shall be organised, if necessary, with the entity concerned. After this preparatory meeting the inspection team shall establish, in agreement with the said entity, a detailed inspection programme covering all areas of security. The inspection team shall have access to any location where EUCI is handled, in particular registries and CIS points of presence.

52. Inspections in Member States' national administrations shall be conducted under the responsibility of a joint GSC/ Commission inspection team in full cooperation with the officials of the entity being inspected.

53. Inspections of third States and international organisations shall be conducted under the responsibility of a joint GSC/Commission inspection team in full cooperation with the officials of the third State or international organisation being inspected.

54. Inspections of EU agencies and bodies established under Title V, Chapter 2, of the TEU, as well as Europol and Eurojust, shall be conducted by the GSC Security Office with assistance from experts of the NSA on whose territory the agency or body is located. The European Commission Security Directorate (ECSD) may be associated where it regularly exchanges EUCI with the agency or body in question.

55. In the case of inspections of EU agencies and bodies established under Title V, Chapter 2 of the TEU, as well as Europol and Eurojust, and of third States and international organisations, assistance and contributions from NSA experts shall be requested in accordance with detailed arrangements to be agreed by the Security Committee.

Inspection reports

56. At the end of the inspection the main conclusions and recommendations shall be presented to the inspected entity. Thereafter, a report on the inspection shall be drawn up under the responsibility of the GSC Security Authority (Security Office). Where corrective action and recommendations have been proposed, sufficient details shall be included in the report to support the conclusions reached. The report shall be forwarded to the appropriate authority of the inspected entity.

57. For inspections conducted in Member States' national administrations:

(a) the draft inspection report will be forwarded to the NSA concerned to verify that it is factually correct and that it contains no information classified higher than RESTREINT UE/EU RESTRICTED;

(b) unless the Member State NSA in question requests general distribution to be withheld, inspection reports shall be circulated to members of the Security Committee and to the ECSD; the report shall be classified RESTREINT UE/EU RESTRICTED;

A regular report shall be prepared under the responsibility of the GSC Security Authority (Security Office) to highlight the lessons learned from the inspections conducted in Member States over a specified period and examined by the Security Committee.

58. For assessment visits of third States and international organisations, the report shall be distributed to the Security Committee and to the ECSD. The report shall be classified at least RESTREINT UE/EU RESTRICTED. Any corrective action shall be verified during a follow-up visit and reported to the Security Committee.

59. For inspections of EU agencies and bodies established under Title V, Chapter 2, of the TEU, as well as Europol and Eurojust, inspection reports shall be distributed to members of the Security Committee and to the ECSD. The draft inspection report shall be forwarded to the agency or body concerned to verify that it is factually correct and that it contains no information classified higher than RESTREINT UE/EU RESTRICTED. Any corrective action shall be verified during a follow up visit and reported to the Security Committee.

60. The GSC Security Authority shall conduct regular inspections of organisational entities in the GSC for the purposes laid down in paragraph 48.

Inspection checklist

61. The GSC Security Authority (Security Office) shall draw up and update a security inspection checklist of items to be verified in the course of an inspection. This checklist shall be forwarded to the Security Committee.

62. The information to complete the checklist shall be obtained in particular during the inspection from the security management of the entity being inspected. Once completed with the detailed responses, the checklist shall be classified in agreement with the inspected entity. It shall not form part of the inspection report.

ANNEX IV

PROTECTION OF EUCI HANDLED IN CIS

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 10.

2. The following IA properties and concepts are essential for the security and correct functioning of operations on CIS:

Authenticity:	the guarantee that information is genuine and from *bona fide* sources;
Availability:	the property of being accessible and usable upon request by an authorised entity;
Confidentiality:	the property that information is not disclosed to unauthorised individuals, entities or processes;
Integrity:	the property of safeguarding the accuracy and completeness of information and assets;
Non-repudiation:	the ability to prove an action or event has taken place, so that this event or action cannot subsequently be denied.

II. INFORMATION ASSURANCE PRINCIPLES

3. The provisions set out below shall form the baseline for the security of any CIS handling EUCI. Detailed requirements for implementing these provisions shall be defined in IA security policies and security guidelines.

Security risk management

4. Security risk management shall be an integral part of defining, developing, operating and maintaining CIS. Risk management (assessment, treatment, acceptance and communication) shall be conducted as an iterative process jointly by representatives of the system owners, project authorities, operating authorities and security approval authorities, using a proven, transparent and fully understandable risk assessment process. The scope of the CIS and its assets shall be clearly defined at the outset of the risk management process.

5. The competent authorities shall review the potential threats to CIS and shall maintain up-to-date and accurate threat assessments which reflect the current operational environment. They shall constantly update their knowledge of vulnerability issues and periodically review the vulnerability assessment to keep up with the changing information technology (IT) environment.

6. The aim of security risk treatment shall be to apply a set of security measures which results in a satisfactory balance between user requirements, cost and residual security risk.

7. The specific requirements, scale and the degree of detail determined by the relevant SAA for accrediting a CIS shall be commensurate with the assessed risk, taking account of all relevant factors, including the classification level of the EUCI handled in the CIS. Accreditation shall include a formal residual risk statement and acceptance of the residual risk by a responsible authority.

Security throughout the CIS-life cycle

8. Ensuring security shall be a requirement throughout the entire CIS life-cycle from initiation to withdrawal from service.

9. The role and interaction of each actor involved in a CIS with regard to its security shall be identified for each phase of the life-cycle.

10. Any CIS, including its technical and non-technical security measures, shall be subject to security testing during the accreditation process to ensure that the appropriate level of assurance is obtained and to verify that they are correctly implemented, integrated and configured.

11. Security assessments, inspections and reviews shall be performed periodically during the operation and maintenance of a CIS and when exceptional circumstances arise.

12. Security documentation for a CIS shall evolve over its life-cycle as an integral part of the process of change and configuration management.

Best practice

13. The GSC and the Member States shall cooperate to develop best practice for protecting EUCI handled on CIS. Best practice guidelines shall set out technical, physical, organisational and procedural security measures for CIS with proven effectiveness in countering given threats and vulnerabilities.

14. The protection of EUCI handled on CIS shall draw on lessons learned by entities involved in IA within and outside the EU.

15. The dissemination and subsequent implementation of best practice shall help achieve an equivalent level of assurance for the various CIS operated by the GSC and by Member States which handle EUCI.

Defence in depth

16. To mitigate risk to CIS, a range of technical and non-technical security measures, organised as multiple layers of defence, shall be implemented. These layers shall include:

(a) *Deterrence*: security measures aimed at dissuading any adversary planning to attack the CIS;

(b) *Prevention*: security measures aimed at impeding or blocking an attack on the CIS;

(c) *Detection*: security measures aimed at discovering the occurrence of an attack on the CIS;

(d) *Resilience*: security measures aimed at limiting impact of an attack to a minimum set of information or CIS assets and preventing further damage; and

(e) *Recovery*: security measures aimed at regaining a secure situation for the CIS.

The degree of stringency of such security measures shall be determined following a risk assessment.

17. The competent authorities shall ensure that they can respond to incidents which may transcend organisational and national boundaries to coordinate responses and share information about these incidents and the related risk (computer emergency response capabilities).

Principle of minimality and least privilege

18. Only the essential functionalities, devices and services to meet operational requirements shall be implemented in order to avoid unnecessary risk.

19. CIS users and automated processes shall be given only the access, privileges or authorisations they require to perform their tasks in order to limit any damage resulting from accidents, errors, or unauthorised use of CIS resources.

20. Registration procedures performed by a CIS, where required, shall be verified as part of the accreditation process.

Information Assurance awareness

21. Awareness of the risks and available security measures is the first line of defence for the security of CIS. In particular all personnel involved in the life-cycle of CIS, including users, shall understand:

(a) that security failures may significantly harm the CIS;

(b) the potential harm to others which may arise from interconnectivity and interdependency; and

(c) their individual responsibility and accountability for the security of CIS according to their roles within the systems and processes.

22. To ensure that security responsibilities are understood, IA education and awareness training shall be mandatory for all personnel involved, including senior management and CIS users.

Evaluation and approval of IT-security products

23. The required degree of confidence in the security measures, defined as a level of assurance, shall be determined following the outcome of the risk management process and in line with the relevant security policies and security guidelines.

24. The level of assurance shall be verified by using internationally recognised or nationally approved processes and methodologies. This includes primarily evaluation, controls and auditing.

25. Cryptographic products for protecting EUCI shall be evaluated and approved by a national CAA of a Member State.

26. Prior to being recommended for approval by the Council or the Secretary-General in accordance with Article 10(6), such cryptographic products shall have undergone a successful second party evaluation by an Appropriately Qualified Authority (AQUA) of a Member State not involved in the design or manufacture of the equipment. The degree of detail required in a second party evaluation shall depend on the envisaged maximum classification level of EUCI to be protected by these products. The Council shall approve a security policy on the evaluation and approval of cryptographic products.

27. Where warranted on specific operational grounds, the Council or the Secretary-General as appropriate may, upon recommendation by the Security Committee, waive the requirements under paragraphs 25 or 26 and grant an interim approval for a specific period in accordance with the procedure laid down in Article 10(6).

28. An AQUA shall be a CAA of a Member State that has been accredited on the basis of criteria laid down by the Council to undertake the second evaluation of cryptographic products for protecting EUCI.

29. The Council shall approve a security policy on the qualification and approval of non-cryptographic IT security products.

Transmission within Secured Areas

30. Notwithstanding the provisions of this Decision, when transmission of EUCI is confined within Secured Areas, unencrypted distribution or encryption at a lower level may be used based on the outcome of a risk management process and subject to the approval of the SAA.

Secure interconnection of CIS

31. For the purposes of this Decision, an interconnection shall mean the direct connection of two or more IT systems for the purpose of sharing data and other information resources (e.g. communication) in a unidirectional or multidirectional way.

32. A CIS shall treat any interconnected IT system as untrusted and shall implement protective measures to control the exchange of classified information.

33. For all interconnections of CIS with another IT system the following basic requirements shall be met:

(a) business or operational requirements for such interconnections shall be stated and approved by the competent authorities;

(b) the interconnection shall undergo a risk management and accreditation process and shall require the approval of the competent SAAs; and

(c) Boundary Protection Services (BPS) shall be implemented at the perimeter of all CIS.

34. There shall be no interconnection between an accredited CIS and an unprotected or public network, except where the CIS has approved BPS installed for such a purpose between the CIS and the unprotected or public network. The security measures for such interconnections shall be reviewed by the competent IAA and approved by the competent SAA.

When the unprotected or public network is used solely as a carrier and the data is encrypted by a cryptographic product approved in accordance with Article 10, such a connection shall not be deemed to be an interconnection.

35. The direct or cascaded interconnection of a CIS accredited to handle TRES SECRET UE/EU TOP SECRET to an unprotected or public network shall be prohibited.

Computer storage media

36. Computer storage media shall be destroyed in accordance with procedures approved by the competent security authority.

37. Computer storage media shall be reused, downgraded or declassified in accordance with a security policy to be established pursuant to Article 6(1).

Emergency circumstances

38. Notwithstanding the provisions of this Decision, the specific procedures described below may be applied in an emergency, such as during impending or actual crisis, conflict, war situations or in exceptional operational circumstances.

39. EUCI may be transmitted using cryptographic products which have been approved for a lower classification level or without encryption with the consent of the competent authority if any delay would cause harm clearly outweighing the harm entailed by any disclosure of the classified material and if:

(a) the sender and recipient do not have the required encryption facility or have no encryption facility; and

(b) the classified material cannot be conveyed in time by other means.

40. Classified information transmitted under the circumstances set out in paragraph 38 shall not bear any markings or indications distinguishing it from information which is unclassified or which can be protected by an available cryptographic product. Recipients shall be notified of the classification level, without delay, by other means.

41. Should recourse be made to paragraph 38 a subsequent report shall be made to the competent authority and to the Security Committee.

III. INFORMATION ASSURANCE FUNCTIONS AND AUTHORITIES

42. The following IA functions shall be established in the Member States and the GSC. These functions do not require single organisational entities. They shall have separate mandates. However, these functions, and their accompanying responsibilities, may be combined or integrated in the same organisational entity or split into different organisational entities, provided that internal conflicts of interests or tasks are avoided.

Information Assurance Authority

43. The IAA shall be responsible for:

(a) developing IA security policies and security guidelines and monitoring their effectiveness and pertinence;

(b) safeguarding and administering technical information related to cryptographic products;

(c) ensuring that IA measures selected for protecting EUCI comply with the relevant policies governing their eligibility and selection;

(d) ensuring that cryptographic products are selected in compliance with policies governing their eligibility and selection;

(e) coordinating training and awareness on IA;

(f) consulting with the system provider, the security actors and representatives of users in respect to IA security policies and security guidelines; and

(g) ensuring appropriate expertise is available in the expert sub-area of the Security Committee for IA issues.

TEMPEST Authority

44. The TEMPEST Authority (TA) shall be responsible for ensuring compliance of CIS with TEMPEST policies and guidelines. It shall approve TEMPEST countermeasures for installations and products to protect EUCI to a defined level of classification in its operational environment.

Crypto Approval Authority

45. The Crypto Approval Authority (CAA) shall be responsible for ensuring that cryptographic products comply with national cryptographic policy or the Council's cryptographic policy. It shall grant the approval of a cryptographic product to protect EUCI to a defined level of classification in its operational environment. As regards the Member States, the CAA shall in addition be responsible for evaluating cryptographic products.

Crypto Distribution Authority

46. The Crypto Distribution Authority (CDA) shall be responsible for:

(a) managing and accounting for EU crypto material;

(b) ensuring that appropriate procedures are enforced and channels established for accounting, secure handling, storage and distribution of all EU crypto material; and

(c) ensuring the transfer of EU crypto material to or from individuals or services using it.

Security Accreditation Authority

47. The SAA for each system shall be responsible for:

(a) ensuring that CIS comply with the relevant security policies and security guidelines, providing a statement of approval for CIS to handle EUCI to a defined level of classification in its operational environment, stating the terms and conditions of the accreditation, and criteria under which re-approval is required;

(b) establishing a security accreditation process, in accordance with the relevant policies, clearly stating the approval conditions for CIS under its authority;

(c) defining a security accreditation strategy setting out the degree of detail for the accreditation process commensurate with the required level of assurance;

(d) examining and approving security-related documentation, including risk management and residual risk statements, system-specific security requirement statements (hereinafter referred to as "SSRSs"), security implementation verification documentation and security operating procedures (hereinafter referred to as "SecOPs"), and ensuring that it complies with the Council's security rules and policies;

(e) checking implementation of security measures in relation to the CIS by undertaking or sponsoring security assessments, inspections or reviews;

(f) defining security requirements (e.g. personnel clearance levels) for sensitive positions in relation to the CIS;

(g) endorsing the selection of approved cryptographic and TEMPEST products used to provide security for a CIS;

(h) approving, or where relevant, participating in the joint approval of the interconnection of a CIS to other CIS; and

(i) consulting the system provider, the security actors and representatives of the users with respect to security risk management, in particular the residual risk, and the terms and conditions of the approval statement.

48. The GSC SAA shall be responsible for accrediting all CIS operating within the remit of the GSC.

49. The relevant SAA of a Member State shall be responsible for accrediting CIS and components thereof operating within the remit of a Member State.

50. A joint Security Accreditation Board (SAB) shall be responsible for accrediting CIS within the remit of both the GSC SAA and Member States' SAAs. It shall be composed of an SAA representative from each Member State and be attended by an SAA representative of the Commission. Other entities with nodes on a CIS shall be invited to attend when that system is under discussion.

The SAB shall be chaired by a representative of the GSC SAA. It shall act by consensus of SAA representatives of institutions, Member States and other entities with nodes on the CIS. It shall make periodic reports on its activities to the Security Committee and shall notify all accreditation statements to it.

Information Assurance Operational Authority

51. The IA Operational Authority for each system shall be responsible for:

(a) developing security documentation in line with security policies and security guidelines, in particular the SSRS including the residual risk statement, the SecOPs and the crypto plan within the CIS accreditation process;

(b) participating in selecting and testing the system-specific technical security measures, devices and software, to supervise their implementation and to ensure that they are securely installed, configured and maintained in accordance with the relevant security documentation;

(c) participating in selecting TEMPEST security measures and devices if required in the SSRS and ensuring that they are securely installed and maintained in cooperation with the TA;

(d) monitoring implementation and application of the SecOps and, where appropriate, delegating operational security responsibilities to the system owner;

(e) managing and handling cryptographic products, ensuring the custody of crypto and controlled items and, if so required, ensuring the generation of cryptographic variables;

(f) conducting security analysis reviews and tests, in particular to produce the relevant risk reports, as required by the SAA;

(g) providing CIS-specific IA training;

(h) implementing and operating CIS-specific security measures.

ANNEX V

INDUSTRIAL SECURITY

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 11. It lays down general security provisions applicable to industrial or other entities in pre-contract negotiations and throughout the life-cycle of classified contracts let by the GSC.

2. The Council shall approve a policy on industrial security outlining in particular detailed requirements regarding FSCs, Security Aspects Letters (SALs), visits, transmission and carriage of EUCI.

II. SECURITY ELEMENTS IN A CLASSIFIED CONTRACT

Security classification guide (SCG)

3. Prior to launching a call for tender or letting a classified contract, the GSC, as the contracting authority, shall determine the security classification of any information to be provided to bidders and contractors, as well as the security classification of any information to be created by the contractor. For that purpose, the GSC shall prepare an SCG to be used for the performance of the contract.

4. In order to determine the security classification of the various elements of a classified contract, the following principles shall apply:

(a) in preparing an SCG, the GSC shall take into account all relevant security aspects, including the security classification assigned to information provided and approved to be used for the contract by the originator of the information;

(b) the overall level of classification of the contract may not be lower than the highest classification of any of its elements; and

(c) where relevant, the GSC shall liaise with the Member States' NSAs/DSAs or any other competent security authority concerned in the event of any changes regarding the classification of information created by or provided to contractors in the performance of a contract and when making any subsequent changes to the SCG.

Security aspects letter (SAL)

5. The contract-specific security requirements shall be described in an SAL. The SAL shall, where appropriate, contain the SCG and shall be an integral part of a classified contract or sub-contract.

6. The SAL shall contain the provisions requiring the contractor and/or subcontractor to comply with the minimum standards laid down in this Decision. Non-compliance with these minimum standards may constitute sufficient grounds for the contract to be terminated.

Programme/project security instructions (PSI)

7. Depending on the scope of programmes or projects involving access to or handling or storage of EUCI, specific Programme/Project Security Instructions (PSI) may be prepared by the contracting authority designated to manage the programme or project. The PSI shall require the approval of the Member States' NSAs/DSAs or any other competent security authority participating in the programme/project and may contain additional security requirements.

III. FACILITY SECURITY CLEARANCE (FSC)

8. An FSC shall be granted by the NSA or DSA or any other competent security authority of a Member State to indicate, in accordance with national laws and regulations, that an industrial or other entity can protect EUCI at the appropriate classification level (CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET) within its facilities. It shall be presented to the GSC, as the contracting authority, before a contractor or subcontractor or potential contractor or subcontractor may be provided with or granted access to EUCI.

9. When issuing an FSC, the relevant NSA or DSA shall, as a minimum:

(a) evaluate the integrity of the industrial or other entity;

(b) evaluate ownership, control, or the potential for undue influence that may be considered a security risk;

(c) verify that the industrial or any other entity has established a security system at the facility which covers all appropriate security measures necessary for the protection of information or material classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET in accordance with the requirements laid down in this Decision;

(d) verify that the personnel security status of management, owners and employees who are required to have access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET has been established in accordance with the requirements laid down in this Decision;

(e) verify that the industrial or any other entity has appointed a Facility Security Officer who is responsible to its management for enforcing the security obligations within such an entity.

10. Where relevant, the GSC, as the contracting authority, shall notify the appropriate NSA/DSA or any other competent security authority that an FSC is required in the pre-contractual stage or for performing the contract. An FSC or PSC shall be required in the pre-contractual stage where EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET has to be provided in the course of the bidding process.

11. The contracting authority shall not award a classified contract with a preferred bidder before having received confirmation from the NSA/DSA or any other competent security authority of the Member State in which the contractor or subcontractor concerned is registered that, where required, an appropriate FSC has been issued.

12. The NSA/DSA or any other competent security authority which has issued an FSC shall notify the GSC as contracting authority about changes affecting the FSC. In the case of a sub-contract, the NSA/DSA or any other competent security authority shall be informed accordingly.

13. Withdrawal of an FSC by the relevant NSA/DSA or any other competent security authority shall constitute sufficient grounds for the GSC, as the contracting authority, to terminate a classified contract or exclude a bidder from the competition.

IV. CLASSIFIED CONTRACTS AND SUB-CONTRACTS

14. Where EUCI is provided to a bidder at the pre-contractual stage, the invitation to bid shall contain a provision obliging the bidder which fails to submit a bid or which is not selected to return all classified documents within a specified period of time.

15. Once a classified contract or sub-contract has been awarded, the GSC, as the contracting authority, shall notify the contractor's or subcontractor's NSA/DSA or any other competent security authority about the security provisions of the classified contract.

16. When such contracts are terminated, the GSC, as the contracting authority (and/or the NSA/DSA or any other competent security authority, as appropriate, in the case of a sub-contract) shall promptly notify the NSA/DSA or any other competent security authority of the Member State in which the contractor or subcontractor is registered.

17. As a general rule, the contractor or subcontractor shall be required to return to the contracting authority, upon termination of the classified contract or sub-contract, any EUCI held by it.

18. Specific provisions for the disposal of EUCI during the performance of the contract or upon its termination shall be laid down in the SAL.

19. Where the contractor or subcontractor is authorised to retain EUCI after termination of a contract, the minimum standards contained in this Decision shall continue to be complied with and the confidentiality of EUCI shall be protected by the contractor or subcontractor.

20. The conditions under which the contractor may subcontract shall be defined in the call for tender and in the contract.

21. A contractor shall obtain permission from the GSC, as the contracting authority, before sub-contracting any parts of a classified contract. No subcontract may be awarded to industrial or other entities registered in a non-EU Member State which has not concluded a security of information Agreement with the EU.

22. The contractor shall be responsible for ensuring that all sub-contracting activities are undertaken in accordance with the minimum standards laid down in this Decision and shall not provide EUCI to a subcontractor without the prior written consent of the contracting authority.

23. With regard to EUCI created or handled by the contractor or subcontractor, the rights incumbent on the originator shall be exercised by the contracting authority.

V. VISITS IN CONNECTION WITH CLASSIFIED CONTRACTS

24. Where the GSC, contractors or subcontractors require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET in each other's premises for the performance of a classified contract, visits shall be arranged in liaison with the NSAs/DSAs or any other competent security authority concerned. However, in the context of specific projects, the NSAs/ DSAs may also agree on a procedure whereby such visits can be arranged directly.

25. All visitors shall hold an appropriate PSC and have a "need-to-know" for access to the EUCI related to the GSC contract.

26. Visitors shall be given access only to EUCI related to the purpose of the visit.

VI. TRANSMISSION AND CARRIAGE OF EUCI

27. With regard to the transmission of EUCI by electronic means, the relevant provisions of Article 10 and Annex IV shall apply.

28. With regard to the carriage of EUCI, the relevant provisions of Annex III shall apply, in accordance with national laws and regulations.

29. For the transport of classified material as freight, the following principles shall be applied when determining security arrangements:

(a) security shall be assured at all stages during transportation from the point of origin to the final destination;

(b) the degree of protection afforded to a consignment shall be determined by the highest classification level of material contained within it;

(c) an FSC at the appropriate level shall be obtained for companies providing transportation. In such cases, personnel handling the consignment shall be security cleared in accordance with Annex I;

(d) prior to any cross-border movement of material classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, a transportation plan shall be drawn up by the consignor and approved by the NSA/DSAs or any other competent security authority concerned;

(e) journeys shall be point to point to the extent possible, and shall be completed as quickly as circumstances permit;

(f) whenever possible, routes should be only through Member States. Routes through States other than Member States should only be undertaken when authorised by the NSA/DSA or any other competent security authority of the States of both the consignor and the consignee.

VII. TRANSFER OF EUCI TO CONTRACTORS LOCATED IN THIRD STATES

30. EUCI shall be transferred to contractors and subcontractors located in third States in accordance with security measures agreed between the GSC, as the contracting authority, and the NSA/DSA of the concerned third State where the contractor is registered.

VIII. HANDLING AND STORAGE OF INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED

31. In liaison, as appropriate, with the NSA/DSA of the Member State the GSC, as the contracting authority, shall be entitled to conduct visits of contractors'/subcontractors' facilities on the basis of contractual provisions in order to verify that the relevant security measures for the protection of EUCI at the level RESTREINT UE/EU RESTRICTED as required under the contract have been put in place.

32. To the extent necessary under national laws and regulations, NSAs/DSAs or any other competent security authority shall be notified by the GSC as the contracting authority of contracts or sub-contracts containing information classified RESTREINT UE/EU RESTRICTED.

33. An FSC or a PSC for contractors or subcontractors and their personnel shall not be required for contracts let by the GSC containing information classified RESTREINT UE/EU RESTRICTED.

34. The GSC, as the contracting authority, shall examine the responses to invitations to tender for contracts which require access to information classified RESTREINT UE/EU RESTRICTED, notwithstanding any requirement relating to FSC or PSC which may exist under national laws and regulations.

35. The conditions under which the contractor may subcontract shall be in accordance with paragraph 21.

36. Where a contract involves handling information classified RESTREINT UE/EU RESTRICTED in a CIS operated by a contractor, the GSC as contracting authority shall ensure that the contract or any sub-contract specifies the necessary technical and administrative requirements regarding accreditation of the CIS commensurate with the assessed risk, taking account of all relevant factors. The scope of accreditation of such CIS shall be agreed between the contracting authority and the relevant NSA/DSA.

ANNEX VI

EXCHANGE OF CLASSIFIED INFORMATION
WITH THIRD STATES AND INTERNATIONAL ORGANISATIONS

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 12.

II. FRAMEWORKS GOVERNING THE EXCHANGE OF CLASSIFIED INFORMATION

2. Where the Council determines that a long-term need exists to exchange classified information,

– a security of information agreement shall be concluded, or

– an administrative arrangement shall be entered into,

in accordance with Article 12(2) and sections III and IV and based on a recommendation from the Security Committee.

3. Where EUCI generated for the purposes of an CSDP operation is to be provided to third States or international organisations participating in such an operation, and where neither of the frameworks referred to in paragraph 2 exists, the exchange of EUCI with the contributing third State or international organisation shall be regulated, in accordance with Section V, under:

– a framework participation agreement;

– an *ad hoc* participation agreement; or

– in the absence of either of the above, an *ad hoc* administrative arrangement.

4. In the absence of a framework referred to in paragraphs 2 and 3, and where a decision is taken to release EUCI to a third State or international organisation on an exceptional *ad hoc* basis in accordance with Section VI, written assurances shall be sought from the third State or international organisation concerned to ensure that it protects any EUCI released to it in accordance with the basic principles and minimum standards set out in this Decision.

III. SECURITY OF INFORMATION AGREEMENTS

5. Security of information agreements shall establish the basic principles and minimum standards governing the exchange of classified information between the EU and a third State or international organisation.

6. Security of information agreements shall provide for technical implementing arrangements to be agreed between the GSC Security Office, the ECSD and the competent security authority of the third State or international organisation in question. Such arrangements shall take account of the level of protection provided by the security regulations, structures and procedures in place in the third State or international organisation concerned. They shall be approved by the Security Committee.

7. No EUCI shall be exchanged by electronic means unless explicitly provided for in the security of information agreement or technical implementing arrangements.

8. Security of information agreements shall provide that prior to the exchange of classified information under the agreement, the GSC Security Office and the ECSD shall agree that the receiving party is able to protect and safeguard information provided to it in an appropriate manner.

9. When the Council concludes a security of information agreement, a registry shall be designated in each party as the main point of entry and exit for classified information exchanges.

10. In order to assess the effectiveness of the security regulations, structures and procedures in the third State or international organisation concerned, assessment visits shall be conducted by the GSC Security Office together with the ECSD and in mutual agreement with the third State or international organisation concerned. Such assessment visits shall be conducted in accordance with the relevant provisions of Annex III and shall evaluate:

(a) the regulatory framework applicable for protecting classified information;

(b) any specific features of the security policy and the way in which security is organised in the third State or international organisation which may have an impact on the level of classified information that may be exchanged;

(c) the security measures and procedures actually in place; and

(d) security clearance procedures for the level of EUCI to be released.

11. The team conducting an assessment visit on behalf of the EU shall assess whether the security regulations and procedures in the third State or international organisation in question are adequate for the protection of EUCI at a given level.

12. The findings of such visits shall be set out in a report on the basis of which the Security Committee shall determine the maximum level of EUCI which may be exchanged in hard copy, and where appropriate electronically, with the third party concerned as well as any specific conditions governing exchange with that party.

13. Every endeavour shall be made to conduct a full security assessment visit to the third State or international organisation in question before the Security Committee approves the implementing arrangements in order to establish the nature and the effectiveness of the security system in place. However, where this is not possible the Security Committee shall receive as full a report as possible from the GSC Security Office, based on the information available to it, informing the Security Committee about the security regulations applicable and the way in which security is organised in the third State or international organisation concerned.

14. The Security Committee may decide that pending examination of the outcome of an assessment visit, no EUCI can be released, or may be released only up to a specified level, or it may lay down other specific conditions governing the release of EUCI to the third State or international organisation in question. This shall be notified by the GSC Security Office to the third State or international organisation in question.

15. In mutual agreement with the third State or international organisation concerned, the GSC Security Office shall, at regular intervals, conduct follow-up assessment visits to verify that the arrangements in place continue to meet the minimum standards agreed.

16. Once the security of information agreement is in force and classified information is exchanged with the third State or international organisation concerned, the Security Committee may decide to modify the maximum level of EUCI which may be exchanged in paper form or by electronic means, in particular in the light of any follow-up assessment visit.

IV. ADMINISTRATIVE ARRANGEMENTS

17. Where a long-term need exists to exchange information classified as a general rule no higher than RESTREINT UE/EU RESTRICTED with a third State or international organisation, and where the Security Committee has established that the party in question does not have a sufficiently developed security system for it to be possible to enter into a security of information agreement, the Secretary-General may, subject to approval by the Council, enter into an administrative arrangement with the relevant authorities of the third State or international organisation in question.

18. Where, for urgent operational reasons, a framework for exchanging classified information needs to be put in place rapidly, exceptionally the Council may decide that an administrative arrangement be entered into for exchanging information of a higher classification level.

19. Administrative arrangements shall as a general rule take the form of an exchange of letters.

20. An assessment visit referred to in paragraph 10 shall be conducted and the report forwarded to, and deemed satisfactory by, the Security Committee before EUCI is actually released to the third State or international organisation in question. However, where there are exceptional reasons for exchanging classified information urgently which are brought to the attention of the Council, EUCI may be released provided every endeavour is made to conduct such an assessment visit as soon as possible.

21. No EUCI shall be exchanged by electronic means unless explicitly provided for in the administrative arrangement.

V. EXCHANGE OF CLASSIFIED INFORMATION IN THE CONTEXT OF CSDP OPERATIONS

22. Framework participation agreements govern the participation of third States or international organisations in CSDP operations. Such agreements shall include provisions on the release of EUCI generated for the purposes of CSDP operations to the contributing third States or international organisations. The maximum classification level of EUCI which may be exchanged shall be RESTREINT UE/EU RESTRICTED for civilian CSDP operations and CONFIDENTIEL UE/EU CONFIDENTIAL for military CSDP operations, unless otherwise laid down in the Decision establishing each CSDP operation.

23. *Ad hoc* participation agreements concluded for a specific CSDP operation shall include provisions on the release of EUCI generated for the purposes of that operation to the contributing third State or international organisation. The maximum classification level of EUCI which may be exchanged shall be RESTREINT UE/EU RESTRICTED for civilian CSDP operations and CONFIDENTIEL UE/EU CONFIDENTIAL for military CSDP operations, unless otherwise laid down in the Decision establishing each CSDP operation.

24. *Ad hoc* administrative arrangements on a third State's or international organisation's participation in a specific CSDP operation may cover *inter alia* the release of EUCI generated for the purposes of the operation to that third State or international organisation. Such *ad hoc* administrative arrangements shall be entered into in accordance with the procedures set out in paragraphs 17 and 18 of Section IV. The maximum classification level of EUCI which may be exchanged shall be RESTREINT UE/EU RESTRICTED for civilian CSDP operations and CONFIDENTIEL UE/EU CONFIDENTIAL for military CSDP operations, unless otherwise laid down in the Decision establishing each CSDP operation.

25. No implementing arrangements or assessment visits are required prior to implementing the provisions on release of EUCI in the context of paragraphs 22, 23 and 24.

26. Where the host State on whose territory an CSDP operation is conducted has no security of information agreement or administrative arrangement in place with the EU for the exchange of classified information, in the event of a specific and immediate operational need, an *ad hoc* administrative arrangement may be established. This possibility shall be provided for in the Decision establishing the CSDP operation. EUCI released under such circumstances shall be restricted to that generated for the purposes of the CSDP operation and classified no higher than RESTREINT UE/EU RESTRICTED. Under such an *ad hoc* administrative arrangement, the host State shall undertake to protect EUCI according to minimum standards which are no less stringent than those laid down in this Decision.

27. The provisions on classified information to be included in framework participation agreements, *ad hoc* participation agreements and *ad hoc* administrative arrangements referred to in paragraphs 22 to 24 shall provide that the third State or international organisation in question shall ensure that its personnel seconded to any operation will protect EUCI in accordance with the Council's security rules and with further guidance issued by the competent authorities, including the operation's chain of command.

28. If a security of information agreement is subsequently concluded between the EU and a contributing third State or international organisation, the security of information agreement shall supersede any framework participation agreement, *ad hoc* participation agreement or *ad hoc* administrative arrangement as far as the exchange and handling of EUCI is concerned.

29. No exchange of EUCI by electronic means shall be permitted under a framework participation agreement, *ad hoc* participation agreement or *ad hoc* administrative arrangement with a third State or international organisation, unless explicitly provided for in the agreement or arrangement in question.

30. EUCI generated for the purposes of an CSDP operation may be disclosed to personnel seconded to the said operation by third States or international organisations in accordance with paragraphs 22 to 29. When authorising access to EUCI in premises or in CIS of an CSDP operation by such personnel, measures shall be applied (including recording of EUCI disclosed) to mitigate the risk of loss or compromise. Such measures shall be defined in relevant planning or mission documents.

VI. EXCEPTIONAL *AD HOC* RELEASE OF EUCI

31. Where no framework is in place in accordance with sections III to V, and where the Council or one of its preparatory bodies determines the exceptional need to release EUCI to a third State or international organisation, the GSC shall:

(a) to the extent possible, verify with the security authorities of the third State or international organisation concerned that its security regulations, structures and procedures are such that EUCI released to it will be protected to standards no less stringent than those laid down in this Decision;

(b) invite the Security Committee, on the basis of available information, to issue a recommendation regarding the confidence that can be placed in the security regulations, structures and procedures in the third State or international organisation to which the EUCI is to be released.

32. If the Security Committee issues a recommendation in favour of releasing the EUCI, the matter shall be referred to the Committee of Permanent Representatives (COREPER), which shall take a decision on its release.

33. If the Security Committee's recommendation is not in favour of releasing the EUCI:

(a) for matters relating to CFSP/CSDP, the Political and Security Committee shall discuss the matter and formulate a recommendation for a decision by COREPER;

(b) for all other matters, COREPER shall discuss the matter and take a decision.

34. Where deemed appropriate, and subject to the prior written consent of the originator, COREPER may decide that the classified information may be released only in part or only if downgraded or declassified beforehand, or that the information to be released shall be prepared without reference to the source or original EU classification level.

35. Following a decision to release EUCI, the GSC shall forward the document concerned, which shall bear a releasability marking indicating the third State or international organisation to which it has been released. Prior to or upon actual release, the third party in question shall undertake in writing to protect the EUCI it receives in accordance with the basic principles and minimum standards set out in this Decision.

VII. AUTHORITY TO RELEASE EUCI TO THIRD STATES OR INTERNATIONAL ORGANISATIONS

36. Where a framework exists in accordance with paragraph 2 for exchanging classified information with a third State or international organisation, the Council shall take a decision to authorise the Secretary-General to release EUCI, in accordance with the principle of originator's consent, to the third State or international organisation in question.

37. Where a framework exists in accordance with paragraph 3 for exchanging classified information with a third State or international organisation, the Secretary-General shall be authorised to release EUCI, in accordance with the Decision establishing the CSDP operation and with the principle of originator's consent.

38. The Secretary-General may delegate such authorisations to senior GSC officials or other persons under his authority.

APPENDICES

APPENDIX A

Definitions

APPENDIX B

Equivalence of security classifications

APPENDIX C

List of National Security Authorities (NSAs)

APPENDIX D

List of abbreviations

APPENDIX A

DEFINITIONS

For the purposes of this Decision, the following definitions shall apply:

"Accreditation" means the process leading to a formal statement by the Security Accreditation Authority (SAA) that a system is approved to operate with a defined level of classification, in a particular security mode in its operational environment and at an acceptable level of risk, based on the premise that an approved set of technical, physical, organisational and procedural security measures has been implemented;

"Asset" means anything that is of value to an organisation, its business operations and their continuity, including information resources that support the organisation's mission;

"CIS life-cycle" means the entire duration of existence of a CIS, which includes initiation, conception, planning, requirements analysis, design, development, testing, implementation, operation, maintenance and decommissioning;

"Classified contract" means a contract entered into by the GSC with a contractor for the supply of goods, execution of works or provision of services, the performance of which requires or involves access to or the creation of EUCI;

"Classified subcontract" means a contract entered into by a contractor of the GSC with another contractor (i.e. the subcontractor) for the supply of goods, execution of works or provision of services, the performance of which requires or involves access to or the creation of EUCI;

"Communication and information system" (CIS) - see Article 10(2);

"Contractor" means an individual or legal entity possessing the legal capacity to undertake contracts;

"Cryptographic (Crypto) material" means cryptographic algorithms, cryptographic hardware and software modules, and products including implementation details and associated documentation and keying material;

"CSDP operation" means a military or civilian crisis management operation under Title V, Chapter 2, of the TEU;

"Declassification" means the removal of any security classification;

"Defence in depth" means the application of a range of security measures organised as multiple layers of defence;

"Designated Security Authority" (DSA) means an authority responsible to the National Security Authority (NSA) of a Member State which is responsible for communicating to industrial or other entities national policy on all matters of industrial security and for providing direction and assistance in its implementation. The function of DSA may be carried out by the NSA or by any other competent authority;

"Document" means any recorded information regardless of its physical form or characteristics;

"Downgrading" means a reduction in the level of security classification;

"EU classified information" (EUCI) - see Article 2(1);

"Facility Security Clearance" (FSC) means an administrative determination by an NSA or DSA that, from the security viewpoint, a facility can afford an adequate level of protection to EUCI of a specified security classification level and its personnel who require access to EUCI have been appropriately security cleared and briefed on the relevant security requirements necessary to access and protect EUCI;

"Handling" of EUCI means all possible actions to which EUCI may be subject throughout its life-cycle. It comprises its creation, processing, carriage, downgrading, declassification and destruction. In relation to CIS it also comprises its collection, display, transmission and storage;

"Holder" means a duly authorised individual with an established need-to-know who is in possession of an item of EUCI and is accordingly responsible for protecting it;

"Industrial or other entity" means an entity involved in supplying goods, executing works or providing services; this may be an industrial, commercial, service, scientific, research, educational or development entity or a self-employed individual;

"Industrial security" - see Article 11(1);

"Information Assurance" - see Article 10(1);

"Interconnection" - see Annex IV, paragraph 31;

"Management of classified information" - see Article 9(1);

"Material" means any document or item of machinery or equipment, either manufactured or in the process of manufacture;

"Originator" means the EU institution, agency or body, Member State, third state or international organisation under whose authority classified information has been created and/or introduced into the EU's structures;

"Personnel security" - see Article 7(1);

"Personnel Security Clearance" (PSC) means either or both of the following:

– "EU Personnel Security Clearance" (EU PSC) for access to EUCI means an authorisation by the GSC Appointing Authority which is taken in accordance with this Decision following completion of a security investigation conducted by the competent authorities of a Member State and which certifies that an individual may, provided his "need-to-know" has been determined, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date; the individual thus described is said to be "security cleared";

– "National Personnel Security Clearance" (national PSC) for access to EUCI means a statement by a competent authority of a Member State which is made following completion of a security investigation conducted by the competent authorities of a Member State and which certifies that an individual may, provided his "need-to-know" has been determined, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date; the individual thus described is said to be "security cleared";

"Personnel Security Clearance Certificate" (PSCC) means a certificate issued by a competent authority establishing that an individual is security cleared and holds a valid national or EU PSC, and which shows the level of EUCI to which that individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the date of validity of the relevant PSC and the date of expiry of the certificate itself;

"Physical security" - see Article 8(1);

"Programme/Project Security Instruction" (PSI) means a list of security procedures which are applied to a specific programme/project in order to standardise security procedures. It may be revised throughout the programme/project;

"Registration" - see Annex III, paragraph 18;

"Residual risk" means the risk which remains after security measures have been implemented, given that not all threats are countered and not all vulnerabilities can be eliminated;

"Risk" means the potential that a given threat will exploit internal and external vulnerabilities of an organisation or of any of the systems it uses and thereby cause harm to the organisation and to its tangible or intangible assets. It is measured as a combination of the likelihood of threats occurring and their impact.

– "Risk acceptance" is the decision to agree to the further existence of a residual risk after risk treatment;

– "Risk assessment" consists of identifying threats and vulnerabilities and conducting the related risk analysis, i.e. the analysis of probability and impact;

– "Risk communication" consists of developing awareness of risks among CIS user communities, informing approval authorities such risks and reporting them to operating authorities;

– "Risk treatment" consists of mitigating, removing, reducing (through an appropriate combination of technical, physical, organisational or procedural measures), transferring or monitoring the risk;

"Security Aspects Letter" (SAL) means a set of special contractual conditions issued by the contracting authority which forms an integral part of any classified contract involving access to or the creation of EUCI, that identifies the security requirements or those elements of the contract requiring security protection;

"Security Classification Guide" (SCG) means a document which describes the elements of a programme or contract which are classified, specifying the applicable security classification levels. The SCG may be expanded throughout the life of the programme or contract and the elements of information may be re-classified or downgraded; where an SCG exists it shall be part of the SAL;

"Security investigation" means the investigative procedures conducted by the competent authority of a Member State in accordance with its national laws and regulations in order to obtain an assurance that nothing adverse is known which would prevent an individual from being granted a national or EU PSC for access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above);

"Security mode of operation" means the definition of the conditions under which a CIS operates based on the classification of information handled and the clearance levels, formal access approvals, and need-to-know of its users. Four modes of operation exist for handling or transmitting classified information: dedicated mode, system-high mode, compartmented mode and multilevel mode;

– "Dedicated mode" means a mode of operation in which all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, and with a common need-to-know for all of the information handled within the CIS;

– "System-high mode" means a mode of operation in which all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, but not all individuals with access to the CIS have a common need-to-know for the information handled within the CIS; approval to access information may be granted by an individual;

– "Compartmented mode" means a mode of operation in which all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, but not all individuals with access to the CIS have a formal authorisation to access all of the information handled within the CIS; formal authorisation implies a formal central management of access control as distinct from an individual's discretion to grant access;

– "Multilevel mode" means a mode of operation in which not all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, and not all individuals with access to the CIS have a common need-to-know for the information handled within the CIS;

"Security risk management process" means the entire process of identifying, controlling and minimising uncertain events that may affect the security of an organisation or of any of the systems it uses. It covers the entirety of risk-related activities, including assessment, treatment, acceptance and communication;

"TEMPEST" means the investigation, study and control of compromising electromagnetic emanations and the measures to suppress them;

"Threat" means a potential cause of an unwanted incident which may result in harm to an organisation or any of the systems it uses; such threats may be accidental or deliberate (malicious) and are characterised by threatening elements, potential targets and attack methods;

"Vulnerability" means a weakness of any nature that can be exploited by one or more threats. A vulnerability may be an omission or it may relate to a weakness in controls in terms of their strength, completeness or consistency and may be of a technical, procedural, physical, organisational or operational nature.

APPENDIX B

EQUIVALENCE OF SECURITY CLASSIFICATIONS

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Belgium	Très Secret (Loi 11.12.1998) Zeer 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)	nota[1] below
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Czech Republic	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Denmark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Germany	STRENG GEHEIM	GEHEIM	VS[2]— VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Ireland	Top Secret	Secret	Confidential	Restricted
Greece	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Spain	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
France	Très Secret Défense	Secret Défense	Confidentiel Défense	nota[3] below
Italy	Segretissimo	Segreto	Riservatissimo	Riservato
Cyprus	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)

---

1 Diffusion Restreinte / Beperkte Verspreiding is not a security classification in Belgium. Belgium handles and protects "RESTREINT UE/EU RESTRICTED" information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

2 Germany: VS = Verschlusssache.

3 France does not use the classification "RESTREINT" in its national system. France handles and protects "RESTREINT UE/EU RESTRICTED" information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

Latvia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lithuania	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembourg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hungary	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Netherlands	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Poland	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Romania	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovenia	Strogo tajno	Tajno	Zaupno	Interno
Slovakia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finland	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Sweden[1]	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
United Kingdom	Top Secret	Secret	Confidential	Restricted

[1] Sweden: the security classification markings in the top row are used by the defence authorities and the markings in the bottom row by other authorities.

APPENDIX C

LIST OF NATIONAL SECURITY AUTHORITIES (NSAs)

BELGIUM Autorité nationale de Sécurité SPF Affaires étrangères, Commerce extérieur et Coopération au Développement 15, rue des Petits Carmes B-1000 Bruxelles Telephone Secretariat: + 32/2/501 45 42 Fax: + 32/2/501 45 96 E-mail: nvo-ans@diplobel.fed.be	**DENMARK** Politiets Efterretningstjeneste (Danish Security Intelligence Service) Klausdalsbrovej 1 DK-2860 Søborg Telephone: + 45/33/14 88 88 Fax: + 45/33/43 01 90 Forsvarets Efterretningstjeneste (Danish Defence Intelligence Service) Kastellet 30 DK-2100 Copenhagen Ø Telephone: + 45/33/32 55 66 Fax: + 45/33/93 13 20
BULGARIA State Commission on Information Security 1A Angel Kanchev Str. BG-1000 Sofia Telephone: + 359/2/921 5911 Fax: + 359/2/987 3750 E-mail: dksi@government.bg Website: www.dksi.bg	**GERMANY** Bundesministerium des Innern Referat ÖS III 3 Alt-Moabit 101 D D-11014 Berlin Telephone: + 49/30/18 681 0 Fax: + 49/30/18 681 1441 E-mail: oesIII3@bmi.bund.de
CZECH REPUBLIC Národní bezpečnostní úřad (National Security Authority) Na Popelce 2/16 CZ-150 06 Praha 56 Telephone: + 420/257 28 33 35 Fax: + 420/257 28 31 10 E-mail: czech.nsa@nbu.cz Website: www.nbu.cz	**ESTONIA** National Security Authority Department Estonian Ministry of Defence Sakala 1 EE-15094 Tallinn Telephone: +372/7170 113, +372/7170 117 Fax: +372/7170 213 E-mail: nsa@kmin.ee

IRELAND National Security Authority Department of Foreign Affairs 76 - 78 Harcourt Street Dublin 2 Ireland Telephone: + 353/1/ 478 08 22 Fax: + 353/1/ 408 29 59	**SPAIN** Autoridad Nacional de Seguridad Oficina Nacional de Seguridad Avenida Padre Huidobro s/n E-28023 Madrid Telephone: + 34/91/372 50 00 Fax: + 34/91/372 58 08 E-mail: nsa-sp@areatec.com
GREECE Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ) Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ) Διεύθυνση Ασφαλείας και Αντιπληροφοριών ΣΤΓ 1020 -Χολαργός (Αθήνα) Ελλάδα Τηλέφωνα: + 30/210/657 20 45 (ώρες γραφείου) + 30/210/657 20 09 (ώρες γραφείου) Φαξ: + 30/210/653 62 79 + 30/210/657 76 12 Hellenic National Defence General Staff (HNDGS) Military Intelligence Sectoral Directorate Security Counterintelligence Directorate GR-STG 1020 Holargos – Athens Telephone: + 30/210/657 20 45 + 30/210/657 20 09 Fax: + 30/210/653 62 79 + 30/210/657 76 12	**FRANCE** Secrétariat général de la Défense Nationale Service de Sécurité de Défense (SGDN/SSD) 51 Boulevard de la Tour-Maubourg F-75700 Paris 07 SP Telephone: + 33/1/71 75 81 77 Fax: + 33/1/71 75 82 00

ITALY Presidenza del Consiglio dei Ministri Autorità Nazionale per la Sicurezza D.I.S. - U.C.Se. Via di Santa Susanna, 15 I-00187 Roma Telephone: + 39/06/611 742 66 Fax: + 39/06/488 52 73	**LATVIA** National Security Authority Constitution Protection Bureau of the Republic of Latvia P.O.Box 286 LV-1001 Riga Telephone: + 371/6702 54 18 Fax: + 371/6702 54 54 Email: ndi@sab.gov.lv
CYPRUS ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ Εθνική Αρχή Ασφάλειας (ΕΑΑ) Υπουργείο Άμυνας Λεωφόρος Εμμανουήλ Ροΐδη 4 1432 Λευκωσία, Κύπρος Τηλέφωνα: + 357/22/80 75 69, + 357/22/80 76 43, + 357/22/80 77 64 Τηλεομοιότυπο: + 357/22/30 23 51 Ministry of Defence Minister's Military Staff National Security Authority (NSA) 4 Emanuel Roidi street CY-1432 Nicosia Telephone: + 357/22/80 75 69, + 357/22/80 76 43, +357 /22/80 77 64 Fax: + 357/22/30 23 51 E-mail: cynsa@mod.gov.cy	**LITHUANIA** Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija (The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority) Gedimino 40/1 LT-01110 Vilnius Telephone: + 370/5/266 32 01, + 370/5/266 32 02 Fax: + 370/5/266 32 00 E-mail: nsa@vsd.lt

LUXEMBOURG Autorité nationale de Sécurité Boîte postale 2379 L-1023 Luxembourg Telephone: + 352/2478 22 10 central + 352/2478 22 53 direct Fax: + 352/2478 22 43	**NETHERLANDS** Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Postbus 20010 NL-2500 EA Den Haag Telephone: + 31/70/320 44 00 Fax: + 31/70/320 07 33 Ministerie van Defensie Beveiligingsautoriteit Postbus 20701 NL-2500 ES Den Haag Telephone: + 31/70/318 70 60 Fax: + 31/70/318 75 22
HUNGARY Nemzeti Biztonsági Felügyelet (National Security Authority) P.O. Box 2 HU-1357 Budapest Telephone: + 361/346 96 52 Fax: + 361/346 96 58 E-mail: nbf@nbf.hu Website: www.nbf.hu	
MALTA Ministry of Justice and Home Affairs P.O. Box 146 MT-Valletta Telephone: + 356/21 24 98 44 Fax: + 356/25 69 53 21	**AUSTRIA** Informationssicherheitskommission Bundeskanzleramt Ballhausplatz 2 A-1014 Wien Telephone: + 43/1/531 15 25 94 Fax: + 43/1/531 15 26 15 E-mail: ISK@bka.gv.at

POLAND Agencja Bezpieczeństwa Wewnętrznego – ABW (Internal Security Agency) 2A Rakowiecka St. PL-00-993 Warszawa Telephone: + 48/22/585 73 60 Fax: + 48/22/585 85 09 E-mail: nsa@abw.gov.pl Website: www.abw.gov.pl Służba Kontrwywiadu Wojskowego (Military Counter-Intelligence Service) Classified Information Protection Bureau Oczki 1 PL-02-007 Warszawa Telephone: + 48/22/684 12 47 Fax: + 48/22/684 10 76 E-mail: skw@skw.gov.pl	**ROMANIA** Oficiul Registrului Național al Informațiilor Secrete de Stat (Romanian NSA - ORNISS National Registry Office for Classified Information) 4 Mures Street RO-012275 Bucharest Telephone: + 40/21/ 224 58 30 Fax: + 40/21/ 224 07 14 E-mail: nsa.romania@nsa.ro Website: www.orniss.ro
PORTUGAL Presidência do Conselho de Ministros Autoridade Nacional de Segurança Rua da Junqueira, 69 P-1300-342 Lisboa Telephone: +351/ 213 031 710 Fax: +351/ 213 031 711	**SLOVENIA** Urad Vlade RS za varovanje tajnih podatkov Gregorčičeva 27 SVN-1000 Ljubljana Telephone: + 386/1/478 13 90 Fax: + 386/1/478 13 99

SLOVAKIA Národný bezpečnostný úrad (National Security Authority) Budatínska 30 P.O. Box 16 SVK-850 07 Bratislava Telephone: + 421/2/68 69 23 14 Fax: + 421/2/63 82 40 05 Website: www.nbusr.sk	**SWEDEN** Utrikesdepartementet (Ministry for Foreign Affairs) SSSB S-103 39 Stockholm Telephone: + 46/8/405 10 00 Fax: + 46/8/723 11 76 E-mail: ud-nsa@foreign.ministry.se
FINLAND National Security Authority Ministry for Foreign Affairs P.O. Box 453 FI-00023 Government Telephone: + 358/9/160 56487 Fax: + 358/9/160 56494 E-mail: NSA@formin.fi	**UNITED KINGDOM** UK National Security Authority 26 Whitehall London SW1A 2WH Telephone: + 44/20/7276 5649 Fax: + 44/20/7276 5651

APPENDIX D

LIST OF ABBREVIATIONS

Acronym	**Meaning**
AQUA	Appropriately Qualified Authority
BPS	Boundary Protection Services
CAA	Crypto Approval Authority
CCTV	Closed Circuit Television
CDA	Crypto Distribution Authority
CFSP	Common Foreign and Security Policy
CIS	Communication and Information Systems handling EUCI
COREPER	Committee of Permanent Representatives
CSDP	Common Security and Defence Policy
DSA	Designated Security Authority
ECSD	European Commission Security Directorate
EUCI	EU Classified Information
EUSR	EU Special Representative

FSC	Facility Security Clearance
GSC	General Secretariat of the Council
IA	Information Assurance
IAA	Information Assurance Authority
IDS	Intrusion Detection System
IT	Information Technology
NSA	National Security Authority
PSC	Personnel Security Clearance
PSCC	Personnel Security Clearance Certificate
PSI	Programme/Project Security Instructions
SAA	Security Accreditation Authority
SAB	Security Accreditation Board
SAL	Security Aspects Letter
SecOPs	Security Operating Procedures
SCG	Security Classification Guide
SSRS	System-Specific Security Requirement Statement
TA	TEMPEST Authority