COUNCIL OF
THE EUROPEAN UNION

Brussels, 8 October 2008

13823/08
ADD 1

LIMITE

CSC 33

NOTE

From :	The General Secretariat of the Council
To :	The Security Committee
Subject :	Draft Council decision on the security rules for the protection of EU classified information

Delegations will find attached a draft Council Decision on the security rules for the protection of EU classified information.

Draft

COUNCIL DECISION

of xx 2009

on the security rules for the protection of EU classified information

(2009/xxx/EC)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community and in particular Article 207(3) thereof,

Having regard to Council Decision 2006/683/EC, Euratom of 15 September 2006 adopting the Council's Rules of Procedure[1], and in particular Article 24 thereof,

Whereas:

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

(2) In order to safeguard the effectiveness of the security system thus established, Member States should be associated with its functioning by taking national measures necessary to respect the provisions of this Decision where their competent authorities and servants handle EU classified information.

(3) The Council and the European Commission are committed to applying equivalent standards of security for creating, handling and protecting EU classified information.

[1] OJ L 285, 16.10.2006, p. 47 . Decision as last amended by Decision 2007/881/EC (OJ L 346, 29.12.2007, p. 17).

(4) The Council underlines the importance of associating, where appropriate, the European Parliament and other EU institutions, bodies or offices with the rules and standards of confidentiality which are necessary in order to protect the interests of the European Union and the Member States.

(5) EU agencies established under Titles V or VI of the Treaty on European Union apply *mutatis mutandis* the security rules adopted by the Council for the protection of EU classified information.

(6) Crisis management operations established under Title V of the Treaty on European Union and their personnel apply *mutatis mutandis* the security rules adopted by the Council for the protection of EU classified information.

(7) EU Special Representatives and the members of their teams apply *mutatis mutandis* the security rules adopted by the Council for the protection of EU classified information.

(8) This Decision is taken without prejudice to Articles 255 and 286 of the Treaty and to instruments implementing them.

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

HAS DECIDED AS FOLLOWS:

Article 1

Purpose and scope

This Decision lays down the basic principles and minimum standards of security to be respected by the Council, by the General Secretariat of the Council (hereinafter "GSC") and by the Member States, in accordance with their respective national laws and regulations, so that each may be assured that a common level of protection is ensured for EU classified information.

Article 2

Definitions

For the purposes of this Decision:

(a) "EU classified information" (hereinafter "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 EU or of one or more of the Member States;

(b) "Information" means knowledge that can be communicated in any form;

(c) "Material" means documents or any item of machinery or equipment, either manufactured or in the process of manufacture;

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

(e) "Sensitive communication and information system" means a system enabling the collection, processing, storage, transmission, display and disposal of classified information in electronic format, or an unclassified system which is critical with respect to information confidentiality, availability, integrity, authenticity or non-repudiation for which accreditation is required.

Article 3

Security classifications and markings

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

   (a) TRES SECRET UE: 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: 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: 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: information and material the unauthorised disclosure of which could be detrimental to the interests of the European Union or of one or more of the Member States.

2. EUCI shall bear a classification marking in accordance with paragraph 1. It may bear additional markings.

Article 4

Responsibility for implementation

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

2. The Secretary-General/High Representative (hereinafter "SG/HR") shall take all appropriate measures to ensure that, when handling EUCI or any other classified information, the provisions of this Decision are respected within the GSC, including in its Liaison Offices located in third States, by GSC officials and other servants, by personnel seconded to the GSC and by GSC external 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, the provisions of this Decision are 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 of the 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' external contractors, whether on the territory of the Member States or abroad.

Article 5

The organisation of security in the Council

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

(a) agreements with third States or international organisations on the protection and exchange of classified information (hereinafter "security agreements");

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

(c) an annual inspection programme proposed by the SG/HR and recommended by the Security Committee for inspections of Member States' services and premises and assessment visits to third States and international organisations; and

(d) policy guidelines as foreseen in Article 7(2).

2. As the GSC's Security Authority, the SG/HR shall:

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

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

(c) authorise GSC officials, other servants and seconded national experts to access information classified CONFIDENTIEL UE or above, in accordance with the procedures set out in Annex I;

(d) as appropriate, order investigations into any unauthorised disclosure or loss of EUCI 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 the protection of EUCI in GSC premises;

(f) undertake periodic inspections of the security arrangements for the protection of EUCI in EU agencies established under Titles V or VI of the Treaty on European Union, in crisis management operations established under Title V of the Treaty on European Union and by EU Special Representatives and the members of their teams;

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

(h) coordinate security measures with the competent authorities of the Member States and, as appropriate, third States or international organisations.

The Security Office of the GSC shall be at the disposal of the SG/HR to assist in these responsibilities.

3. Member States shall:

(a) designate an NSA responsible for security arrangements for the protection of EUCI. NSAs are listed in Appendix 2. Within each Member State, the responsibilities of the NSA shall be defined for:

(i) the security of EUCI held by any national department, body or agency, public or private, at home or abroad;

(ii) the periodic inspection of the security arrangements for the protection of EUCI;

(iii) ensuring that all individuals, whether nationals or non-nationals, employed within a national administration who may be granted access to EU information classified CONFIDENTIEL UE or above are appropriately security cleared or are otherwise duly authorised in accordance with national laws and regulations; and

(iv) devising such security programmes as are considered necessary to prevent EUCI from falling into unauthorised hands;

(b) ensure that their national security organisations responsible for collecting and recording intelligence on espionage, sabotage, terrorism and other subversive activities provide information and advice to its government, and through it to the Council, on the nature of the threats to the security of EUCI and the means of protection against them; and

(c) respond to security clearance requests from agencies established under Titles V or VI of the Treaty on European Union, crisis management operations established under Title V of the Treaty on European Union or EUSRs and their teams.

4. A Security Committee is hereby established. It shall be composed of representatives of the Member States' NSAs and be attended by a representative of the European Commission. It shall be chaired by the SG/HR or by the SG/HR's designated delegate. It shall meet as instructed by the Council, or at the request of the SG/HR or of an NSA.

Representatives of agencies established under Titles V or VI of the Treaty on European Union may be invited to attend when questions concerning them are discussed.

5. The Security Committee shall:

(a) examine and assess any matter relating to the protection of classified information and of sensitive communication and information systems relevant for the Council's activities, and provide opinions or recommendations to the Council as appropriate;

(b) agree at its level relevant documentation to supplement the basic principles and minimum standards set out in this Decision and policy guidelines approved by the Council; and

(c) act as Security Accreditation Authority for sensitive communication and information systems within the remit of both the GSC and of Member States.

The Security Committee shall organise its activities in such a way that it can provide expert opinions or recommendations on specific issues.[1]

Article 6

Handling of classified information

1. EUCI shall be created, handled, transmitted, stored, destroyed, downgraded and declassified in accordance with the provisions of this Decision.

2. Where Member States introduce classified information bearing a national classification marking into the EU's structures or networks, the Council shall handle 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 1.

Article 7

Basic principles and minimum standards and their implementation

1. The basic principles and minimum standards referred to in Article 1 are laid down in Articles 8 to 14. Annexes I to VI set out provisions for implementing these principles and standards.

---

[1] The following language will be inserted into the final report to the Council when this Decision is approved:

Regarding the organisation of the Security Committee's work, expert configurations may be established by the Committee's full member configuration, which may also define terms of reference. All expert configurations will make periodic reports on their activities to the Committee's full member configuration and will refer to it any policy guidelines prior to submission to COREPER and the Council. With regard to Information Assurance matters, three expert configurations of the Security Committee already exist:

- *a configuration which deals with information assurance policy issues and cryptographic methods and products;*
- *a configuration which acts as Security Accreditation Authority for systems within the remit of both the GSC and of Member States; and*
- *a configuration of Appropriately Qualified Authorities for evaluating cryptographic products.*

2. Where necessary, the Council shall approve policy guidelines setting out detailed measures to ensure that these principles and standards are respected.

Article 8

Personnel security

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

2. Access to EUCI shall be granted on the basis of the need-to-know principle.

3. All individuals shall be informed of their responsibilities to protect EUCI in accordance with this Decision and shall be briefed about the relevant security rules before being granted access to EUCI and at regular intervals thereafter.

4. Member States' personnel referred to in Article 4(3) shall be appropriately security cleared or otherwise duly authorised in accordance with national laws and regulations before they may be granted access to information classified CONFIDENTIEL UE and above.

5. All individuals in the GSC, including officials, other servants and seconded national experts, shall be appropriately authorised in accordance with Annex I before they may be granted access to information classified CONFIDENTIEL UE and above.

6. A Personnel Security Clearance (hereinafter "PSC") or a Personnel Security Authorisation (hereinafter "PSA") is not required for individuals with an established need-to-know in order to be granted access to information classified RESTREINT UE.

7. For the purpose of this Decision:

   (a) a PSC issued by a competent national authority authorising access to national classified information shall be accepted by the GSC for access to EUCI up to the equivalent level as set out in the table of equivalence in Appendix 1;

   (b) a PSA issued by the GSC Appointing Authority shall be treated by the Member States as equivalent to a PSC for access to EUCI issued by a competent national authority.

8. The above principles and standards shall be implemented in accordance with the provisions set out in Annex I.

Article 9

Physical security

1. Physical security is the application of physical protective measures to prevent an unauthorised person from gaining access to EUCI.

2. The Member States and the GSC shall each establish and keep up-to-date physical security programmes consisting of active and passive security measures which meet the minimum standards set out in this Decision to ensure a common degree of protection commensurate with the security classification of the information to be protected and with the assessed threats. Physical security programmes shall be based on the principle of "security in depth".

3. All premises, buildings, offices, rooms, other areas and communication and information systems in which EUCI is handled or stored shall be protected by appropriate physical security measures and approved equipment.

4. Areas where EUCI is handled or stored shall be organised and structured so as to correspond to an Administrative Area, a Class I or Class II Security Area or a Technically Secure Area as defined in Annex II. Where EUCI is handled, processed, stored, displayed or transmitted in electronic format, the security requirements for such areas may be adapted on the basis of a risk assessment.

5. Physical security protection in such areas shall be commensurate with the threat to, and the security classification and quantity of the information to be protected.

6. The above principles and standards shall be implemented in accordance with the provisions set out in Annex II.

Article 10

Security of information

1. Security of information is the application of appropriate organisational and procedural protective measures to prevent, detect and recover from the deliberate or accidental compromise of information.

2. EUCI requires protection commensurate with its classification level throughout its life-cycle. It shall be managed to ensure that it is appropriately classified, clearly identified as classified information, and retains its classification level only as long as necessary. The classification level of EUCI shall not be changed and EUCI shall not be declassified without the prior written consent of the originator.

3. Information classified CONFIDENTIEL UE or above shall be registered prior to distribution and on reception. Registration means the application of procedures to allow the holder of classified documents to be identified and to record the life-cycle of a given classified document.

Where such information remains confined in electronic form within a classified communication and information system, the registration requirement shall be met by appropriate approved IT security measures.

Information classified TRES SECRET UE shall be registered in dedicated registries.

4. Services and premises where EUCI is created, handled, transmitted, stored or destroyed shall be subject to regular inspection.

5. Any breaches of security relating to EUCI or to sensitive communication and information systems shall be reported immediately to the competent security authority.

6. When a security authority discovers or is informed of a breach of security, in particular where it is known or where there are grounds for suspecting that EUCI has been compromised or lost, it shall take all appropriate measures in accordance with the relevant laws and regulations to investigate the case in order to establish the facts, assess and minimise any damage, prevent a recurrence and notify the appropriate authorities of the action taken.

7. Any individual who is responsible for compromising EUCI or any other classified information held by the Council shall be liable to disciplinary action in accordance with the relevant rules and regulations. Such action shall be without prejudice to any legal action, including possible criminal proceedings, against the individual concerned in accordance with the applicable laws and regulations.

8. The above principles and standards shall be implemented in accordance with the provisions set out in Annex III.

Article 11

Information assurance in sensitive communication and information systems

1. Information Assurance (IA) is the confidence that sensitive communication and information systems (CIS) (hereinafter "systems") will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users. IA involves identifying and applying security measures to protect and defend:

   (a) information processed, stored or transmitted in systems,

   (b) and such systems themselves, which consist of IT assets used to deliver the expected services and of any individuals interacting with those assets,

   by ensuring confidentiality, integrity and availability, and guaranteeing authenticity of information, and non-repudiation of actions performed through such systems.

2. Security measures shall be determined on the basis of a risk management process where the scope and assets of a system, the risks to it, and the required countermeasures shall be identified through a system-specific security requirement statement (SSRS).

3. All systems processing EUCI shall undergo an accreditation process.

   Accreditation shall aim to obtain assurance that all appropriate security measures have been implemented and that a sufficient level of protection of the system resources has been achieved, in accordance with the provisions of this Decision.

   Accreditation shall be based on a consistent risk management scheme.

   On the basis of recommendations from the relevant authorities, the Security Authority may decide that an unclassified sensitive communication and information system shall undergo an accreditation process.

4. The accreditation decision shall determine the maximum authorised classification level that may be handled by a system and the terms and conditions of such an authorisation.

5. Systems processing information classified CONFIDENTIEL UE and above shall be protected against the compromise of information through unintentional electromagnetic emissions ("TEMPEST countermeasures").

6. During transmission by electronic means:

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

   (b) the confidentiality of information classified CONFIDENTIEL UE or RESTREINT UE shall be protected by cryptographic methods or products approved by the SG/HR as CAA, upon recommendation of the Security Committee.

   Notwithstanding the previous subparagraph, during transmission within Member States' national systems which are not interconnected to a system linked to the GSC, EUCI classified CONFIDENTIEL UE or RESTREINT UE may be protected by cryptographic methods or products approved by the CAA of a Member State. In this case the CAA shall inform the Security Committee about the cryptographic methods or products used and the maximum classification level of EUCI handled in such systems.

7. Any exceptions to paragraph 6 shall be allowed only under special emergency circumstances or specific technical configurations as specified in Annex IV.

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

   (a) an IA Authority

(b) an IA Operational Authority

(c) a Security Accreditation Authority (SAA)

(d) a Crypto Approval Authority (CAA)

(e) a Distribution Authority.

9. The above principles and standards shall be implemented in accordance with the provisions set out in Annex IV.

Article 12

Industrial security

1. Industrial security is the application of protective measures to prevent, detect and recover from the loss or compromise of EUCI handled by contractors or subcontractors in pre-contract negotiations and actual contracts entered into by the GSC.

2. Activities related to negotiating and awarding contracts involving or entailing access to or the release of EUCI (hereinafter "classified contracts") and to the performance of such contracts by industrial or other entities shall be governed by the relevant provisions of this Decision. Such provisions shall also govern the release of or access to EUCI during the public procurement procedure.

3. The GSC shall ensure that the minimum standards on industrial security and the requirements deriving from them are complied with when awarding classified contracts.

4. Each Member State shall ensure that all contractors and subcontractors involved in such classified contracts comply with the minimum standards on industrial security.

5. All industrial or other entities participating in classified contracts which involve handling information classified CONFIDENTIEL UE or SECRET UE within their facilities shall hold a national Facility Security Clearance (hereinafter "FSC").

6. Unless required by Member States' national laws and regulations, an FSC is not required for an industrial or other entity participating in classified contracts involving information classified RESTREINT UE.

7. The above principles and standards shall be implemented in accordance with the provisions set out in Annex V.

Article 13

Exchange of classified information with third States and international organisations

1. Where the Council determines that there is a need to exchange classified information 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 EU shall enter into agreements to that effect, to be concluded by the Council; or

   (b) the SG/HR may enter into administrative arrangements to that effect, if the classification level of information to be released by the EU is no higher than RESTREINT UE.

3. When the Council receives classified information from a third State or international organisation, that information shall be given protection, appropriate to its classification level, which shall be at least equivalent to the standards for EUCI established in this Decision.

4. Agreements or administrative arrangements concluded with third States or international organisations shall contain provisions to ensure that when third States or international organisations receive classified information from the Council, that information is given protection appropriate to its classification level and according to standards which are no less stringent than those established for EUCI in this Decision. Mutual assessment visits shall be arranged to verify ability to comply with the required security standards.
Where such agreements or administrative arrangements cover the transmission of EUCI on electronic systems of third States or international organisations, the Council shall ensure that EUCI is protected in accordance with the EU's requirements. The Council may adopt policy guidelines on the transmission of EUCI within third parties' internal networks.

5. The decision to release EUCI originating in the Council to a third State or international organisation shall be taken 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 information for which release is desired is not the Council, the GSC shall first seek the originator's consent to release. If the originator cannot be established, the Council will assume the former's responsibility.

6. With regard to third States and international organisations with which the EU has concluded a security agreement or the SG/HR has put in place an administrative arrangement, the Council may authorise the SG/HR to take the decision referred to in paragraph 5. The SG/HR may delegate such authorisation to senior GSC officials in relevant functions.

With regard to third States and international organisations with which the EU has not concluded a security agreement or the SG/HR has not put in place an administrative arrangement, the decision referred to in paragraph 5 shall be taken by the Permanent Representatives' Committee.

7. The above principles and standards shall be implemented in accordance with the provisions set out in Annex VI.

Article 14

Implementing security in depth

1. Security authorities shall ensure that the measures provided for in Annexes I to VI are implemented in combination so that they provide an effective level of protection for EUCI commensurate with the risk of loss or compromise in any particular circumstances.

2. Contingency plans shall be drawn up for the protection or destruction of EUCI during emergency situations in order to prevent unauthorised access and disclosure and loss of availability. IA in sensitive communication and information systems shall be an integral part of such contingency plans.

Article 15

Replacement of previous decisions

This Decision cancels and replaces Council Decision 2001/264/EC[1] adopting the Council's security regulations and all subsequent amendments thereof.

Article 16

Entry into force

This Decision shall apply from the date of its publication.

Done at Brussels, xx

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

Security of information

ANNEX IV

Information Assurance in sensitive communication and information systems

ANNEX V

Industrial security

ANNEX VI

Exchange of classified information with third states and international organisations

PERSONNEL SECURITY

I. INTRODUCTION

1. This Annex sets out the criteria and procedures for determining the eligibility of an individual, taking into account his or her loyalty, trustworthiness and reliability, to be authorised to have access to EUCI and the investigative and administrative procedures to be followed to that effect.

I.1. Definitions

2. The following definitions shall apply:

   (a) *Security investigation:* an investigative procedure conducted by the competent national authority of a Member State in accordance with the relevant laws and regulations in force in the Member State concerned in order to determine the vulnerability of an individual and to provide an assurance that nothing adverse is known which would prevent the individual from being granted a personnel security clearance for access to information classified CONFIDENTIEL UE or above;

   (b) *Personnel Security Clearance (PSC):* an administrative decision by the competent national authority of a Member State which is taken following completion of the relevant investigative personnel security procedures and which certifies that an individual may, provided his or her need-to-know has been determined, be granted access to EUCI up to a specified level;

(c) *Personnel Security Authorisation (PSA):* an administrative decision by the GSC Appointing Authority authorising individuals in the GSC, including officials, other servants and seconded national experts, to access information classified CONFIDENTIEL UE and above. Such authorisations may only be issued by the GSC Appointing Authority following a request for a security investigation to the competent national authorities of the Member State of which the individual subject to authorisation is a national and where such a request has resulted in a positive opinion or an administrative decision by these authorities;

(d) *Personnel Security Clearance Certificate (PSCC):* a certificate issued by a competent authority establishing an individual has been security cleared and holds a valid PSC or PSA. The certificate shall show the level of classified information to which that individual may have access, and the date of expiry of the relevant PSC or PSA.

II. AUTHORISING ACCESS TO EUCI

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

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

(b) he or she has been granted an appropriate PSC or PSA or is otherwise duly authorised in accordance with national laws and regulations; and

(c) he or she has been briefed on EU security rules and procedures and has acknowledged his or her obligation and responsibilities with regard to protecting such information.

4. Each Member State and the GSC shall identify the positions in their structures which require respectively a PSC or PSA and indicate the minimum level of clearance for such positions.

III. REQUIREMENTS FOR PERSONNEL SECURITY CLEARANCE (PSC) AND PERSONNEL SECURITY AUTHORISATION (PSA)

5. NSAs or other competent national authorities shall be responsible for carrying out security investigations on their nationals who require access to information classified CONFIDENTIEL UE or above. Standards of investigation shall be in accordance with national laws and regulations and shall be no less stringent than those set out in paragraphs 6 to 9.

III.1. Criteria for Assessing Eligibility for a PSC or PSA

6. The principal criteria to be used for determining the loyalty, trustworthiness and reliability of an individual for the purpose of granting and revalidating a PSC or a PSA shall include considering whether an 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 to overthrow the government of a Member State, or a change in the form of government of a Member State;

(d) is, or has recently been, a supporter of any organisation described in sub-paragraph (c), or who is, or who has recently 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 indicating habitual criminal tendencies;

(g) has serious financial difficulties or unexplained affluence;

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

(i) is or has been involved in conduct, including any form of sexual misconduct, which may give rise to the risk of vulnerability to blackmail or pressure;

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

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

(l) is suffering, or has suffered, from any illness or mental or emotional condition which may cause significant defects in judgement or reliability or may make the individual, unintentionally, a potential security risk. In all such cases competent medical advice shall be sought; or

(m) may be liable to pressure through relatives or close associates who could be vulnerable to foreign intelligence services, terrorist groups or other subversive organisations or individuals whose interests may threaten the security interests of the EU and/or Member States.

7. Holding dual nationality, one of which may be non-EU, shall not in itself constitute a reason to deny a clearance, provided that the NSA granting the clearance is content that there is no conflict of loyalty.

8. Where appropriate and in accordance with national legislation, a spouse's, cohabitant's or close family member's character, conduct and circumstances may also be relevant when considering an individual's eligibility for a clearance.

III.2. Investigative Requirements for CONFIDENTIEL UE, SECRET UE and TRES SECRET UE PSCs and PSAs

9. The initial security clearance for access to information classified CONFIDENTIEL UE and SECRET UE shall be based on enquiries covering at least the last 5 years, or from age 18 to the present, whichever is the shorter; and shall include the following:

(a) the completion of a national Personnel Security Questionnaire;

(b) identity check / citizenship / nationality status – the individual's date and place of birth shall be verified and his or her 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 for any officially recorded indication of disloyalty or unreliability. The records of law enforcement agencies with legal jurisdiction where the individual has resided or been employed for at least six months shall be checked.

10. The initial security clearance for access to information classified TRES SECRET UE shall be based on enquiries covering at least the last 10 years, or from age 18 to the present, whichever is the shorter. If interviews are conducted as stated in sub-paragraph (e) below, enquiries shall cover at least the last 7 years, or from age 18 to the present, whichever is the shorter. In addition to the requirements stated in paragraph 6 above, the following shall be required for clearances for access to information classified TRES SECRET UE; these factors may also be relevant for the assessment of CONFIDENTIEL UE and SECRET UE clearances, where they are 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 on attendance since the 18th birthday, or during an appropriate period as judged by the investigating security authority, at schools, universities and other education establishments;

(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 will be verified; and

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

11. In accordance with national security laws and regulations, sufficient additional enquiries shall be conducted to develop all relevant information available on an individual and to substantiate or disprove adverse information. Lack of coverage in any investigative category shall be compensated for through other investigative means.

12. Indications of potential vulnerability to pressure (e.g. debts or the potential vulnerability of a spouse/cohabitant/close family member) need not be a reason to deny clearance if the individual's loyalty, trustworthiness and reliability are undisputed. The NSA or competent national authority shall assess the risks associated with each case in order to determine whether the individual may be granted a PSC.

III.3. Personnel security clearance procedures

13. The relevant personnel security questionnaire for the level of EUCI to which the individual may require access, once completed, shall be forwarded by the individual concerned to the competent security authority. The competent national authorities shall undertake a security investigation, with the consent of the individual concerned, in accordance with the laws and regulations of the Member State. Should the individual concerned reside in the territory of another Member State, the competent authorities shall seek assistance from the competent authority of the State of residence.

14. For individuals in the GSC, including officials, other servants and seconded national experts, 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 is undertaken for the level of EUCI to which the individual may require access. Following completion of the security investigation, the relevant NSA shall provide the GSC Security Authority with an opinion taking the appropriate administrative form prescribed by national legislation:

(a) where that opinion is positive, the GSC Appointing Authority may grant a PSA to the individual concerned, for the validity period of the opinion;

(b) where that opinion is negative, the GSC Appointing Authority shall notify the individual concerned, who may ask to be heard by the GSC Appointing Authority. The GSC Appointing Authority may ask the competent NSA for any further clarification it can provide. If the negative opinion is confirmed, a PSA shall not be granted. The individual may have recourse to appeals in accordance with the laws and regulations of the Member State concerned.

15. Notwithstanding paragraph 14, national experts seconded to the GSC for a position requiring a PSA shall be required to present a valid national personnel security clearance certificate to the GSC Security Authority prior to taking up their assignment. The GSC Appointing Authority shall issue a PSA on the basis of this certificate. For revalidation of a PSA, the procedure foreseen in paragraph 14 shall apply.

16. PSAs shall remain valid for any assignment within the GSC held by that individual.

17. Exceptionally, if required by the needs of the service, the GSC Appointing Authority may, after giving the competent NSA notification and provided that no objections are received within one month, grant a temporary PSA for GSC officials, other servants and national experts seconded to the GSC. Such temporary PSAs shall be valid for a period not exceeding six months pending completion of the security investigation. They shall not permit access to information classified TRES SECRET UE.

18. If an individual's period of service does not commence within 12 months of the issue of a new PSC to fill a post at the GSC, or if there is a break of 12 months in an individual's service, during which time he or she has not been employed in a position with a national administration of a Member State or the GSC, the PSC or PSA shall be referred to the relevant NSA for confirmation that it remains valid and appropriate.

III.4. Revalidation of PSCs or PSAs

19. After the initial granting of a PSC or PSA and provided the individual has had uninterrupted service with a national administration or the GSC and has a continuing need for access to EUCI, the PSC or PSA shall be reviewed for revalidation at intervals not exceeding 5 years for a TRES SECRET UE clearance and 10 years for SECRET UE and CONFIDENTIEL UE clearances, with effect from the date of the last security investigation on which it was based. All security investigations for the renewal of a PSC or PSA shall cover the period since the previous such investigation. Requests for revalidation shall be made in a timely manner taking account of the average time required for such investigations.

20. The relevant NSA shall review any information arising during the course of these records checks against the background of its own records and send its decision or opinion to the authority requesting the revalidation.

21. For the renewal of TRES SECRET UE, SECRET UE and CONFIDENTIEL UE clearances, the procedures outlined in paragraphs 9 and 10 shall, as appropriate, be carried out.

22. Where the responsible NSA has received the relevant personnel security questionnaire before a PSC or PSA expires, and the necessary security investigation has not been completed, the competent authority may extend the validity of the existing PSC or PSA for a period of up to 12 months. If, at the end of this additional 12-month period, the revalidation has still not been completed, the individual shall only be assigned to duties which do not require a PSC or PSA.

III.5. Procedures where adverse information comes to light

23. If adverse information becomes known concerning an individual, a decision shall be made by the responsible NSA or the GSC Appointing Authority about the respective PSC or PSA. In cases where individuals are considered to represent an unacceptable security risk, their PSC or PSA shall be withdrawn and the individuals shall be excluded from access to EUCI and from positions where such access is possible or where they might endanger security.

24. PSAs for GSC officials, other servants and national experts seconded to the GSC may be withdrawn where the GSC Appointing Authority considers that there are justifiable grounds for doing so. Any decision to withdraw a PSA and the reasons for doing so shall be notified to the individual concerned and to the competent NSA. The individual in question may ask to be heard by the GSC Appointing Authority.

25. The relevant NSA shall notify the GSC Security Authority when a PSC is withdrawn from a national expert seconded to the GSC. In such cases, the GSC Appointing Authority shall revoke any PSA based on that PSC. The individual in question may ask to be heard by the GSC Appointing Authority.

III.6. Records of PSCs and PSAs

26. Records of the PSCs and PSAs granted to individuals for access to EUCI shall be maintained respectively by each Member State and by the GSC. These records shall contain at least details of the level of the PSC or PSA, its date of issue and its period of validity.

27. The competent security authority may issue a personnel security clearance certificate for access to EUCI showing the level of classified information to which that individual may be granted access and the date of expiry of the relevant PSC or PSA.

IV. SECURITY EDUCATION AND AWARENESS

28. All cleared individuals shall acknowledge in writing that they have understood their responsibilities with regard to the protection of EUCI and the consequences if EUCI passes into unauthorised hands. A record of such a written acknowledgement shall be kept by the Member State and by the GSC, as appropriate.

29. All individuals who are authorised to have access to, or required to handle EUCI, shall initially be made aware, and periodically reminded of the dangers to security arising from indiscreet conversations with persons having no need-to-know, contacts with the media, and the threat presented by the activities of intelligence services which target the EU and the Member States. Individuals shall be briefed on these dangers and must report immediately to the appropriate security authorities any approach they consider suspicious or unusual.

30. All individuals who cease to be employed in duties requiring access to EUCI shall be made aware of, and acknowledge in writing, their responsibilities for the continued safeguarding of EUCI.

V. EXCEPTIONAL CIRCUMSTANCES

V.1. Provisional assignments

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

(a) the individual holds a current PSC or PSA;

(b) action has been initiated to obtain the level of PSC or PSA required for the position;

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

(d) satisfactory checks have been made that the individual has not seriously or repeatedly infringed security regulations.

32. Provisional assignment of personnel shall not extend beyond six months from the date the individual takes up the position. The competent authority may extend the assignment for another six months if the investigation has been initiated and no adverse information has come to light.

V.2. One time Access

33. Exceptionally, individuals may be authorised access on a one-time basis to EU information classified one level higher than that to which they are cleared. The following criteria must be fulfilled:

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

(b) access shall be limited to specific items of EUCI in support of the task described by the superior;

(c) the individual holds a current PSC;

(d) satisfactory checks have been made that the individual has not seriously or repeatedly infringed security regulations;

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

34. This procedure shall not be used on a recurring basis for access to EUCI. If this is required, or if access is required for more than 6 months, a PSC or PSA for the necessary level must be obtained.

V.3. Emergency Access

35. In very exceptional circumstances, i.e. missions in hostile environments or during periods of mounting international tension when emergency measures require it, Member States and the SG/HR or the Deputy Secretary-General may grant, in writing, access to EUCI to individuals who do not possess the requisite PSC or PSA, 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 the access was given.

36. In the case of information classified TRES SECRET UE, this emergency access shall be confined wherever possible to those individuals who have been authorised access to either the national equivalent of TRES SECRET UE or to information classified SECRET UE.

V.4. Exemptions

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

V.5. Access to EUCI by Third Country Nationals

38. Individuals who are third country nationals or who are working for an international organisation with whom the EU has not concluded a security agreement may be granted access to EUCI on a case-by-case basis, provided that:

(a) access is necessary in support of a specific EU programme, project, contract, operation, or related task;

(b) the individual is granted a national security clearance based on clearance procedures no less stringent than that required for a Member State national in accordance with this Decision; and

(c) the prior written consent of the Member State, the EU institution or EU agency that originated the information is obtained.

VI. ATTENDANCE AT MEETINGS IN THE COUNCIL

39. Individuals assigned to participate in meetings of the Council or of Council preparatory bodies discussing information classified CONFIDENTIEL UE and above may only do so upon confirmation of the individual's PSC certificate. For delegates from Member States the PSC certificate shall be forwarded by the appropriate national authorities to the GSC Security Office, or exceptionally be hand carried by the delegate concerned. Where applicable, a consolidated list of names may be used, giving the relevant personal data of the individuals concerned and other details required in a PSC certificate.

VII. COURIERS, GUARDS AND ESCORTS

40. Couriers, guards and escorts employed to carry documents classified CONFIDENTIEL UE and above shall be appropriately security cleared. Couriers, guards and escorts shall be briefed on EU security procedures and shall be instructed on their duties for protecting the EUCI entrusted to them.

PHYSICAL SECURITY

I. INTRODUCTION

1. This Annex sets out provisions for implementing the principles and standards for physical security measures for the protection of EUCI laid down in this Decision.

II. SECURITY REQUIREMENTS

2. In deciding what combination of physical security measures and approved equipment is necessary to protect premises, buildings, offices, rooms and other areas, as well as communication and information systems, in which EUCI is handled or stored, account shall be taken of all relevant factors, in particular:

   (a) the level of classification of EUCI;

   (b) amount and form of the information held;

   (c) the need-to-know and security clearance of personnel;

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

   (e) the way in which the information will be stored

3. Physical security measures shall be designed to:

(a) deny surreptitious or forced entry by an intruder;

(b) deter impede and detect actions by disloyal personnel;

(c) allow for segregation of personnel in terms of access to EUCI in accordance with the need-to-know principle; and

(d) detect and enable action to be taken as soon as possible following any security breaches.

4. When acquiring equipment for the physical protection of EUCI, the GSC shall ensure that the equipment meets any technical standards endorsed by the Security Committee. Where necessary and appropriate in the acquisition process, the GSC may also refer to lists of approved equipment for the physical protection of national classified information established by NSA's.

5. The GSC shall apply a risk management process for the protection of EUCI on its premises to ensure that a commensurate level of physical protection is applied against the assessed risk.

III. PHYSICAL SECURITY MEASURES

6. Physical security measures must be supported by sound personnel security, security of information, information assurance and industrial security measures, as set out in this Decision. Management of security risks shall involve establishing the most efficient and cost-effective methods of countering threats and compensating for vulnerabilities by a combination of protective measures. With a view to achieving efficiency and cost-effectiveness, physical security requirements shall be defined as part of the planning and design of facilities.

7. Security systems shall be maintained regularly to ensure that equipment operates at optimum performance. The effectiveness of individual security measures and components and of the overall security system shall be re-evaluated periodically. This shall be achieved by drawing up incident response plans.

III.1. Secure Areas

8. Four types of secure areas may be established for the physical protection of EUCI: Class I Security Areas, Class II Security Areas, Administrative Areas and Technically Secure Areas.

9. Areas in which information classified CONFIDENTIEL UE or above is handled and stored shall be organised and structured so as to correspond to one of the following two types of area:

(a) Class I Security Area: an area in which information classified CONFIDENTIEL UE or above is handled and stored in such a way that entry into the area constitutes, for all practical purposes, access to classified information contained in it. Such an area shall require:

(i) a clearly defined and protected perimeter through which all entry and exit is controlled;

(ii) an entry/exit control system which admits only those individuals who are appropriately cleared and specifically authorised to enter the area. Only visitors who are cleared and escorted and have been specifically authorised may enter the area ; and

(iii) specification of the level of highest security classification of the definition normally held in the area, i.e. the information to which entry gives access.

(b) Class II Security Area: an area in which information classified CONFIDENTIEL UE or above is handled and stored in such a way that it can be protected from access by unauthorised individuals by means of internally established controls. Such an area shall require:

(i) a clearly defined and protected perimeter through which all entry and exit is controlled;

(ii) an entry control system which admits unescorted access only to those individuals who are security cleared and specifically authorised to enter the area. For all other individuals, provision shall be made for escorts or equivalent controls, to prevent unauthorised access to EUCI and uncontrolled entry to areas subject to technical security inspections.

Class I and II areas which are not occupied by duty personnel on a 24-hour basis shall be inspected immediately after normal working hours and at random intervals outside normal working hours.

10. Information classified RESTREINT UE may be handled and stored in Administrative Areas. Administrative Areas are areas which may be established around or leading up to Class I or Class II Security areas. Such an area shall have a visibly defined perimeter which allows individuals and vehicles to be checked.

11. Areas to be protected against audio eavesdropping shall be designated as Technically Secure Areas. Persons or material entering these areas shall be controlled. Such areas shall be:

(a) locked and/or guarded in accordance with these provisions when not occupied, and any keys shall be treated as security keys;

(b) subject to regular physical and/or technical inspections as required by the competent security authority. Such inspections shall also be undertaken following any unauthorised entry or suspicion of such entry and entry by maintenance personnel; and

(c) as a general rule, free of communication lines, telephones and other electronic items;

12. The GSC and each Member State shall designate the competent authority responsible for certifying that an area meets the requirements to be designated a Class I Security Area, a Class II Security Area, a Technically Secure Area or an Administrative Area.

13. The following physical security measures may be implemented individually or in combination in order to establish secure areas:

(a) perimeter fence - a perimeter fence is a physical barrier which identifies the boundary of an area requiring protection. The effectiveness of any security perimeter shall be determined by the level of security at the points of access;

(b) intruder detection system (IDS) - IDS may be used on perimeters to enhance the level of security offered by the fence, or may be used 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. The control may be electronic, electro-mechanical, by security personnel and/or a receptionist, or by any other physical means;

(d) security personnel - appropriately cleared, trained and supervised security personnel may be employed 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 perimeters;

(f) security lighting - security lighting may be used in order to deter a potential intruder, in addition to providing 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 and detect unauthorised access.

III.2. Entry and Exit Controls

14. The competent security authority shall be authorised to conduct random entry and exit searches to act as a deterrent to unauthorised introduction of material, or the unauthorised removal of EUCI from a site or building.

III.3. Access Control

15. For each Class I or II Security Area and Technically Secure Area a procedure shall be established for authorising access to the area based on the individual's clearance and need to access the area.

16. A pass or personal recognition system shall be used to control entry into Class I or II Security Areas. Visitors shall be permitted escorted or unescorted access based upon checks on the individual and the individual visitor's access requirements.

IV. STORAGE OF EUCI

17. EUCI shall be stored only under conditions designed to deter and detect unauthorised access to the information.

18. Information classified TRES SECRET UE shall be stored in a Class I or Class II Security Area under one of the following conditions:

    (a) in an IDS-equipped vault, or in a nationally-approved security container in an area which is subject to continuous protection or periodic inspection by cleared security staff or duty personnel; or

    (b) an IDS-protected open storage area constructed in accordance with the supporting guidelines on the physical protection of EUCI and in combination with an incident response force.

19. Information classified SECRET UE shall be stored within an EU class I or II security area under one of the following conditions:

(a) in the same manner as prescribed for TRES SECRET UE information; or

(b) in a nationally-approved security container or vault without supplementary controls; or

(c) an open storage area, which is IDS-protected, or subject to continuous protection or periodic inspection by cleared security staff or duty personnel.

20. Information classified CONFIDENTIEL UE shall be stored in the same manner as prescribed for TRES SECRET UE or SECRET UE information except that supplementary controls (paragraph 19 (c)) are not required.

21. Information classified RESTREINT UE shall be stored in a locked container.

V. CONTROL OF KEYS AND COMBINATIONS

22. The competent security authority shall define procedures for the management of keys and combination settings for rooms and security containers.

23. Keys and combinations shall be afforded security protection no less stringent than applicable to the information to which they give access.

24. Knowledge of combination settings shall be restricted to the smallest possible number of individuals.

VI. PHYSICAL PROTECTION OF COPYING AND FAX MACHINES

25. Copying and fax machines processing EUCI shall be physically protected to the extent necessary to ensure that only authorised individuals can use them and that all EUCI stored in them is appropriately controlled. If EUCI is stored in them they shall be considered a classified system and are subject to Annex IV.

VII. PROTECTION AGAINST TECHNICAL ATTACKS

VII.1. Eavesdropping

26. Offices or areas in which information classified SECRET UE and above is regularly discussed shall be protected against passive and active eavesdropping by means of physical security measures and access control, where the risk warrants it. Responsibility for determining the risk shall be coordinated with technical specialists and decided by the competent security authority.

VII.2. Overlooking

27. When EUCI is at risk from overlooking, even accidentally, appropriate measures shall be taken to counter this risk in daylight, at night and in artificial light conditions.

VII.3. Examination of electrical / electronic equipment

28. Before being used in areas where meetings are held or work is being performed involving information classified SECRET UE and above, and in circumstances where the threat is assessed as high, communications equipment and electrical or electronic equipment of any kind shall be examined by technical or communications security experts to ensure that no intelligible information is inadvertently or illicitly transmitted by such equipment beyond the perimeter of the security area concerned.

VII.4. Technical security inspections

29. Regular technical security inspections shall be carried out in areas where information classified SECRET UE and above is discussed or where sensitive conversations are held.

ANNEX III

SECURITY OF INFORMATION

I. INTRODUCTION

1. This Annex sets out provisions on implementing the organisational and procedural protective measures foreseen in Article 10 throughout the life-cycle of EUCI in order to prevent, detect and recover from the deliberate or accidental compromise of such information.

II. CLASSIFICATION MANAGEMENT

II.1. Classifications and markings

2. EUCI shall bear security markings. It shall bear one of the four classification markings set out in Article 3(1) of this Decision, where "UE" indicates that the information corresponds to the definition contained in Article 2(a) of this Decision and TRES SECRET, SECRET, CONFIDENTIEL or RESTREINT designates the classification level.

3. EUCI may bear additional markings, such as:

(a) an identifier to designate the originating State or entity;

(b) any caveats, code-words or acronyms specifying the field covered by the document or a particular distribution on a need-to-know basis;

(c) releasability markings.

II.2. Classification

4. Information shall be classified only when this is necessary to ensure its confidentiality.

5. The classification level of a document shall be determined in accordance with Article 3 of this Decision and by reference to the practical classification guide in Appendix 3. The classification level assigned shall determine the personnel, physical, organisational, procedural and other security measures to afford the information the appropriate level of protection.

6. The security classification shall be clearly and correctly indicated. It shall be displayed in full on the top and bottom of all pages bearing classified information.

7. The classification level shall be maintained only as long as the information requires protection.

8. Information shall not be over-classified or under-classified.

9. Individual pages, paragraphs, sections, annexes, appendices, attachments and enclosures of a given document may require different classifications and shall be marked accordingly.

10. The overall classification level of a document 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. A sanitised document shall be reviewed before it is issued to determine its overall security classification level, since it may require a higher classification than would appear to be indicated by the classification of the remaining paragraphs or sections.

11. 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.

12. 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 (top and bottom), e.g.:

CONFIDENTIEL UE
Without attachment(s) RESTREINT UE.

II.3. Abbreviated classification markings

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

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

TRES SECRET UE	TS-UE
SECRET UE	S-UE
CONFIDENTIEL UE	C-UE
RESTREINT UE	R-UE

15. Where paragraphs or sections in classified documents are non-classified, they may bear one of the following two markings:

LIMITE[1]	L-UE
PUBLIC[2]	P-UE

[1] Information in principle internal to the Council.
[2] Information already in the public domain.

II.4. Downgrading and declassification of EUCI

16. The originator of EUCI shall be responsible for determining the security classification level and initial dissemination of the information. EUCI shall not be downgraded or declassified without the prior written consent of the originator.

17. At the time of its creation, the originator shall indicate, where possible, whether the information can be downgraded or declassified at a certain date or following a certain event. Information classified RESTREINT UE shall, in principle, contain a date when it becomes declassified.

18. Each Member State and the GSC shall establish a system to ensure that classified information which it has originated is reviewed no less frequently than every five years to ascertain whether the classification level still applies. Such a review is not necessary where the originator has indicated from the outset that the information shall be automatically downgraded or declassified and the information has been marked accordingly.

III. GENERATION OF EU CLASSIFIED DOCUMENTS

III.1. Generation of an EU classified document in paper form

19. When generating an EU classified document:

(a) each page of a classified document shall be marked at the top and bottom centre with the classification level. This marking may be added using a stamp. Documents classified SECRET UE and below may be printed on pre-stamped paper. For such documents prepared in a workstation, the marking may be added electronically in the header and footer;

(b) each page of a classified document shall be numbered;

(c) the document shall bear a reference number which is not itself classified information;

(d) the document shall be dated.

III.2. Generation of an EU classified document in electronic form

20. An EU classified document may be generated or analysed (i.e. using the "read" or "write" functions) in electronic form only on IT systems which are either "stand-alone" (i.e. not linked to any IT network) or linked to an IT network which has been accredited in accordance with Annex IV.

21. If the IT system is used by more than one person, the files containing classified information shall be appropriately protected in order to ensure that only persons with a need-to-know can access the information.

22. Where the system is accredited for handling EUCI up to a certain level, all details of EUCI handling shall be approved during the accreditation process. Users shall be able to find relevant guidance in the Secure Operating Procedures (SecOps) that shall be available for all accredited IT systems.

23. If printers are not close to the component of the IT system (e.g. workstation) on which the document is prepared, measures shall be taken to ensure the need-to-know principle is respected. Steps shall also be taken to ensure that printed documents are not removed from the printer by unauthorised persons

IV. REGISTRATION OF CLASSIFIED DOCUMENTS

IV.1. General provisions

24. All documents classified CONFIDENTIEL UE and above and documents classified RESTREINT UE, or its equivalent, received from or sent to a third party shall be registered. In all cases, such documents shall be registered whenever they arrive at or leave an organisational entity.

25. Registration shall be recorded in a logbook or using an electronic registration tool. The recorded information shall be the minimum required to uniquely identify the document.

26. The holder of a registered classified document shall confirm possession by signing a receipt. The receipt shall contain only unclassified information, such as the reference number of the document, the registration number, the date and where appropriate the copy number of the document.

27. Electronic documents requiring registration shall be handled only in accredited IT systems. The specific registration rules for electronic documents shall be defined as part of the accreditation process.

28. Detailed registration requirements shall be set out in the SecOPs that shall be produced as part of the accreditation process.

29. Member States' national classified information introduced into the EU's structures or networks shall be registered in the same manner as EUCI in accordance with the table of equivalence of security classifications set out in Appendix 1.

IV.2. Registration of classified documents exchanged with third States or international organisations in accordance with Annex VI

30. Registries shall store classified information received from third parties separately from other classified information.

31. Classified information exchanged with third States or international organisations shall be registered in dedicated logbooks for that third party. Electronic logbooks shall provide appropriately separated directories per third party. Logbooks shall be kept separate from other registration information. Registries shall have specific logbooks per third party and shall organise their safes in such a way as to separate classified information arriving from different sources.

32. Agreements or administrative arrangements with third States or international organisations may provide for registration of EUCI classified RESTREINT UE.

33. Classified information received from third States or international organisations shall be forwarded through the registry system to the recipients.

V. COPYING AND TRANSLATION OF EU CLASSIFIED DOCUMENTS

34. Only the originator may authorise the copy or translation of TRES SECRET UE documents.

35. Where the originator of documents classified SECRET UE and below has not imposed caveats on their copying or translation, such documents may be copied or translated by the holder, on condition that the need-to-know principle is strictly complied with. Under no circumstances may holders of classified information requiring registration prepare and distribute copies without involving the responsible registry.

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

VI. DESTRUCTION OF EU CLASSIFIED DOCUMENTS

37. All registered classified documents shall be destroyed by the responsible registry. The logbooks and other registration information shall be updated accordingly. The 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. Both the registrar and the witness shall sign a destruction certificate, which shall be filed in the registry and a copy of which shall be given to the holder of the destroyed document.

38. RESTREINT UE documents may be destroyed by the holder in accordance with approved destruction methods. Registered documents classified RESTREINT UE shall be destroyed as other registered classified documents in accordance with paragraph 39.

39. In the GSC, destruction shall be performed by methods approved by the GSC Security Office.

VII. DETAILED ARRANGEMENTS ON THE SECURITY OF EU CLASSIFIED DOCUMENTS

40. The Council shall approve policy guidelines on the security of EU classified documents setting out in particular detailed arrangements on registering, copying, transmitting and destroying EU classified documents in both paper and electronic form.

VIII. REGISTRY SYSTEM

41. Registries shall be responsible for the receipt, registration, distribution and destruction of information classified CONFIDENTIEL UE and above. These tasks may be carried out either within a single registry or by establishing separate registries. When necessary for organisational reasons sub-registries shall be established and shall be attached to a registry. Unless otherwise specified, the term "registry" shall be used throughout this Annex to refer to either a central registry or a sub-registry.

42. Every organisational entity within the GSC and within Member States' national administrations in which EUCI is handled shall be attached to a registry. Registries shall ensure that EUCI is handled in accordance with this Decision in the organisational entities attached to them.

43. Registries shall be established as Class I or Class II Security Areas.

44. When the Council concludes a security agreement with a third party a registry shall be designated as the main point of entry and exit for classified information.

45. A Central Top Secret Registry shall be established and shall act as the main receiving and dispatching authority for TRES SECRET UE classified information. When necessary Top Secret sub-registries shall be established and shall be attached to the Central Top Secret Registry.

46. Top Secret sub-registries may not transmit TRES SECRET UE documents directly to other sub-registries of the same central Top Secret registry without the express approval of the latter. All exchanges of TRES SECRET UE documents between sub-registries not attached to the same central registry shall be routed through the central Top Secret registries.

47. The head of an EUCI registry shall be responsible for:

(a) the registration, storage, distribution, transmission and destruction of information classified CONFIDENTIEL UE or above, in accordance with this Annex;

(b) keeping a list of all its dependent sub-registries, together with the names and signatures of the persons in charge of the registries and their deputies;

(c) keeping an up-to-date list of all registries with which he or she normally corresponds, together with the names and signatures of the correspondents' heads of registry and deputies;

(d) keeping an up-to-date list of all persons in organisational entities attached to the registry who are authorised to have access to EUCI;

(e) ensuring that each registry carries out, every twelve months, an itemised inventory of all EUCI of the level CONFIDENTIEL UE or above for which it is accountable. A document shall be deemed to have been accounted for if the registry either physically musters the document, holds a receipt from the registry to which the document has been transferred, holds a destruction certificate for the document or holds an instruction to downgrade or declassify that document;

(f) ensuring that sub-registries forward the findings of their annual inventory to the central registry to which they are attached, on a date specified by the latter; and

(g) ensuring that the findings of the annual inventories conducted in central TRES SECRET UE registries are forwarded to the SG/HR by 31 March each year, at the latest.

IX. MEETINGS WHERE EUCI IS DISCUSSED

48. Only persons with a need-to-know may be present in a meeting room when classified items are discussed. For items classified CONFIDENTIEL UE and above only persons with a need-to-know and a valid clearance shall be allowed to remain in the room. The necessary procedures shall be put in place in order to verify need-to-know and the validity and level of clearance of persons in the room. The authority responsible for conducting the required checks shall receive the information in advance and shall control access to the meeting room.

49. Classified information shall not be left unattended in meeting rooms. Information classified CONFIDENTIEL UE and above shall be handled according to the provisions of this Annex. At the close of the meeting the room shall immediately be inspected to verify that no EUCI has been left behind.

50. When used for discussing information classified CONFIDENTIEL UE or above, meeting rooms shall be organised in such a way that they correspond to temporary Class I or Class II areas as defined in Annex II for the duration of the discussion of the classified item. The meeting room may be made technically secure and be subject to electronic surveillance during the meeting.

51. The necessary controls shall be put in place to ensure that no electronic devices (including portable computers, mobile phones and PDAs) are activated in the meeting room when information classified CONFIDENTIEL UE is discussed. When information classified SECRET UE and above is discussed, no electronic devices may be taken into the meeting room.

IX.1. Meetings outside the Council premises

52. Where meetings are held in the Member States outside the Council premises in Brussels and Luxembourg, and where justified by the particular security requirements relating in particular to the handling of classified information, the security measures described below shall be taken.

53. The Member State on whose territory the meeting is held shall be responsible for ensuring the security of such meetings, including the protection of EUCI and the physical security of the principal delegates and their staff.

54. The Security Authorities of the host Member State shall coordinate with the GSC Security Office in order to determine the security measures to be taken. Such measures may include the designation of a Security Officer, access control, the design of secure areas and the handling and destruction of classified information in accordance with the provisions of this Decision.

X. INSPECTIONS AND ASSESSMENT VISITS

55. The term "inspection" shall be used hereinafter to designate any inspection in accordance with Article 5(2)(e), (f) and (g) or assessment visit in accordance with Article 13(4) to evaluate the effectiveness of measures implemented for the protection of EUCI provided or exchanged.

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

(a) ensure that the required minimum standards set out in this Decision are applied;

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

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

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

57. Before the end of each calendar year, the Council shall adopt the inspection programme foreseen in Article 5(1)(c) for the following year. The actual dates for each inspection or assessment visit shall be determined in agreement with the Member State, third State or international organisation concerned.

X.1. Conduct of inspections

58. Inspections in Member States' national administrations and of third States and international organisations shall be conducted under the responsibility of a joint GSC/European Commission inspection team in full co-operation with the officials of the entity being inspected. They shall not be confined to checking all the detailed points in the relevant security instructions, but shall also ensure that the entity's practices comply with the standards set out in this Decision and in the provisions governing the exchange of classified information with a given third Party.

59. 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 State or organisation concerned, a detailed inspection programme covering all areas of security.

60. The inspection shall:

(a) identify the security organisation directly responsible for establishing, implementing and enforcing the security regulations and procedures; and

(b) after examination, determine whether the protection afforded by the inspected entity satisfies EU security requirements.

61. Third States and international organisations may apply security regulations and procedures that are similar to, or markedly different from, those provided for in this Decision. The inspection team shall be mindful of this fact and concentrate on whether the security regulations and procedures being inspected are adequate for the protection of EUCI at a given level.

X.2. Inspection reports

62. 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. 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.

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

(a) inspection reports shall be drawn up under the responsibility of the GSC Security Authority;

(b) 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;

(c) 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 only to Committee members) and to the European Commission Security Directorate;

(d) a regular report shall be prepared under the responsibility of the GSC Security Authority to highlight the main issues arising and lessons learned from the inspections conducted in Member States over a certain period.

64. For assessment visits of third States and international organisations, the report shall be drawn up under the responsibility of the GSC Security Authority and distributed to members of the Security Committee (and only to Committee members) and to the European Commission Security Directorate. The report shall be classified at least RESTREINT UE. Any corrective action shall be verified during a follow up visit.

65. For inspections of EU agencies, inspection reports shall be drawn up under the responsibility of the GSC Security Authority. The draft inspection report shall be forwarded to the agency concerned to verify that it is factually correct and that it contains no information classified higher than RESTREINT UE. Any corrective action shall be verified during a follow up visit.

66. The GSC Security Authority shall conduct regular inspections of organisational entities in the GSC for the purposes laid down in paragraph 56.

X.3. Inspection checklist

67. The GSC Security Authority shall be responsible for drawing up and updating a security inspection checklist of items to be verified in the course of an inspection or assessment visit in Member States or of EU agencies, third States and international organisations. This checklist and any updates shall be forwarded to the Security Committee.

68. The completed checklist shall contain the details supporting any recommendations or observations made after the inspection. Once completed, the checklist shall be classified at least CONFIDENTIEL UE. It shall not be distributed with the inspection report. The information to complete the checklist shall be obtained from the security management of the Member State, EU agency, third State or international organisation being inspected.

XI. BREACHES OF SECURITY AND COMPROMISE OF EUCI

69. A breach of security occurs as the result of an act or omission contrary to the security rules set out in this Decision which might endanger or compromise EUCI. Compromise of EUCI occurs when it has wholly or in part fallen into the hands of unauthorised persons, i.e. who do not have either the necessary need-to-know or the appropriate security clearance, or if there is a likelihood of such an event having occurred.

70. All individuals required to handle EUCI shall be made aware of the importance of reporting any breach of security which may come to their notice immediately to the relevant security authority.

71. The following information shall be provided in an initial report on any breach of security:

(a) a description of the classified information involved;

(b) a brief description of the circumstances of the breach of security, including the date and the period during which the information was exposed to compromise; and

(c) a statement of whether the originator has been informed.

72. Further reports shall follow as developments warrant. The timing of the reports depends on the sensitivity of the information and the circumstances.

73. On being informed that a breach of security has occurred, the SG/HR shall:

(a) notify the authority that originated the classified information in question;

(b) ask the appropriate security authorities to initiate investigations;

(c) coordinate enquiries where more than one security authority is affected;

(d) obtain a report on the circumstances of the breach, the date or period during which it may have occurred and was discovered, a description of the content and classification of the material involved, any damage done to interests of the EU or of one or more of its Member States and action taken to prevent a recurrence.

74. The originating authority shall inform all recipients of the EUCI and shall issue appropriate instructions.

INFORMATION ASSURANCE IN SENSITIVE COMMUNICATION AND INFORMATION SYSTEMS

I. INTRODUCTION

1. This Annex sets out provisions on Information Assurance (IA) for the protection of EU classified information (EUCI) handled on sensitive communication and information systems (hereinafter "CIS" or "systems") to ensure confidentiality, integrity, availability and, where appropriate, authenticity and non-repudiation.

2. The provisions set out in this Annex may also be used for the protection of EU systems handling information that is not classified but where unauthorised disclosure, breaches of confidentiality, integrity, availability, authenticity and/or non-repudiation or the privacy to which individuals are entitled could adversely effect the interests of the EU and/or one or more of its Member States.

3. A CIS comprises the entire assets of the system. This includes the infrastructure, organisation, personnel and components used for the collection, processing, storage, transmission, display, dissemination and disposal of information.

4. The following IA properties and concepts shall be regarded as essential for the security and correct functioning of operations on systems processing EUCI:

Authenticity:	the guarantee that information is genuine and unchanged;
Availability:	the property of being accessible and usable upon request by an authorised entity;
Confidentiality:	the property that sensitive information is not disclosed to unauthorised individuals, entities or processes;
Integrity:	the property of safeguarding the accuracy and completeness of 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

5. The IA detailed principles set out below shall form the baseline for the security of any sensitive CIS handling EU information. Detailed requirements implementing these provisions shall be defined in IA policy guidelines and technical guidance documents developed in support of this Annex.

II.1. Security risk management

6. The following definitions shall apply:

(a) A *threat* means a potential cause of an unwanted incident which may result in harm to a system or organisation; such threats may be accidental or deliberate (malicious) and are characterised by threatening elements, potential targets and attack methods. IA policy guidelines shall describe specific types of threats to CIS processing EUCI.

(b) A *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 or operational nature.

(c) *Risk* means the likelihood that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the system or organisation. It is measured as combination of the likelihood of threats being carried out and the impact. Risk can be related to the loss of all or any combination of the following: confidentiality, integrity, availability and, where applicable, authenticity and non-repudiation of information or CIS.

(d) *Residual risk* means the risk which remains after security measures have been implemented in a CIS, given that not all threats can be countered and not all vulnerabilities can be eliminated completely.

(e) *Accreditation* means the formal declaration by the Security Accreditation Authority (SAA) that a CIS is approved to operate with a defined level of classification or sensitivity, 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, managerial, physical and procedural safeguards is implemented. It also comprises monitoring the risk management process.

7. Security risk management refers to the following activities in order to direct and control a system under risk.

(a) *Risk assessment* consists of identifying threats and vulnerabilities and the related risk analysis, i.e. the analysis of likelihood and impact;

(b) *Risk treatment* consists of mitigating, removing or reducing the risk (through appropriate technical, physical, managerial or procedural measures), transferring the risk, or monitoring the risk;

(c) *Risk acceptance* is the decision after the risk treatment to agree to the further existence of an identified residual risk and to further treatments on such a residual risk;

(d) *Risk communication* consists of developing awareness among CIS user communities, informing approval authorities and reporting to operating authorities.

8. The authorities responsible and others services and individuals involved in the area of IA shall be aware of the potential threats to CIS and shall maintain up-to-date and accurate threat assessments which reflect the current operational environment. They shall also constantly update their knowledge of vulnerability issues and periodically review the vulnerability assessment to meet the changing IT environment.

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

10. Security risk treatment shall aim to apply a balanced set of countermeasures which result in a satisfactory compromise between user requirements, cost and residual security risk.

11. Accreditation of a CIS shall include a formal residual risk statement and the acceptance of the residual risk by an authority responsible.

II.2. Security and system life cycle

12. Security shall be a continuous and dynamic concern throughout the whole CIS life-cycle from initiation to withdrawal from service.

13. The security role of each participant's interaction with the others shall be identified for each phase of the life-cycle.

14. The CIS security documentation evolves over its life cycle and shall be considered as within the scope of consistent change and configuration management. Any changes to the Accreditation Document Set (ADS), which is part of the CIS security documentation required for system accreditation, shall be approved by the SAA.

II.3. Best practices

15. The GSC and the Member States shall co-operate to develop commonly shared best practices for the protection of EUCI processed on CIS. Best practice guidance shall consist of technical, physical, organisational and procedural security measures for CIS whose effectiveness in countering given threats and vulnerabilities has been proven, such as relevant provisions of the ISO/IEC 2700x series.

16. The protection of EUCI processed on CIS shall benefit from lessons learned by those entities involved in IA, both within and outside the GSC.

17. The communication and subsequent implementation of best practice shall contribute to achieving a homogeneous level of security for the various CIS operated by the GSC and Member States.

II.4. Network defence

18. For the security of systems processing EUCI a range of countermeasures (physical, procedural, organisational and technical), organised as multiple lines of defence ('Network Defence'), shall be implemented. The degree of stringency of the technical and other countermeasures shall be determined by a risk assessment.

19. Over and above countermeasures applied to CIS to mitigate risk, additional methods of reducing the impact in the event of CIS's defences being compromised shall be considered. These methods shall include the following defence layers:

(a) *Deterrence*: security measures aimed at deterring 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 detecting 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 / CIS assets and preventing further damage;

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

20. Capabilities to respond to incidents which may transcend organisational and national boundaries shall be established to coordinate responses and share information about these incidents and related risk constellations with third parties.

II.5. Minimality and least privilege

21. In order to avoid unnecessary risk only the essential functionalities, devices and services for operational requirements shall be implemented.

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

II.6. Information Assurance awareness

23. Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. In particular all personnel involved in the life cycle of CIS shall understand:

(a) that security failures may significantly harm the systems and networks processing EUCI under their control;

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

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

24. To ensure that security responsibilities are understood, IA education and awareness training shall be mandatory for senior management, CIS users and operating staff. CIS operators and users shall in addition be trained and comply with the applicable Security Operating Procedures (SecOPs).

II.7. Evaluation and assurance

25. The required degree of confidence in countermeasures shall be determined in accordance with the results of the risk analysis process.

26. The degree of confidence or assurance shall be verified by using commonly used or nationally approved processes and methodologies. This includes primarily evaluation, controls and auditing. Where a degree of assurance is required for IT security products or systems, a qualification and selection scheme shall be used, based upon generally accepted evaluation methods such as the Common Criteria standard (ISO/IEC 15408).

27. Prior to being recommended for approval by the Council or the SG/HR, in accordance with Article 11(6), cryptographic methods or products for the protection of EUCI:

(a) shall initially be evaluated and approved by a national Crypto Approval Authority of a Member State, and

(b) shall undergo a successful second 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 examined in a second evaluation shall depend on the envisaged maximum classification level of EUCI to be protected by these methods or products.

28. An AQUA shall be a cryptographic evaluation authority of a Member State that has been accredited on the basis of objective criteria to undertake the second evaluation of EU cryptographic devices.

29. Policy guidelines shall be approved by the Council to implement the evaluation schemes.

30. Communication and information systems, including technical security countermeasures, shall be subject to testing and evaluation during the accreditation process to verify they are correctly integrated and configured.

31. Security assessments, inspections and reviews shall be performed periodically during the operational phase and during maintenance and also when exceptional circumstances arise.

II.8. Secure interconnection of CIS

32. A system interconnection shall mean the direct connection of two or more CIS for the purpose of sharing data and other information resources (e.g. communication) in a unidirectional or multidirectional way.

33. A system shall treat any interconnected CIS initially as untrusted and shall implement protective measures to control the exchange of information with the other CIS.

34. For all interconnections of CIS handling EUCI with another CIS, the following basic requirements shall be complied with:

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

(b) the interconnection shall undergo a risk management and accreditation process;

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

35. A CIS accredited to CONFIDENTIEL UE or above shall not be connected to an unprotected public network. Any other interconnection of such a system shall be accredited.

36. All interconnections of CIS handling EUCI, including cascaded and back-end interconnections, shall require the approval of the relevant Security Accreditation Authorities (SAAs).

II.9. Business continuity management

37. Business continuity measures shall be implemented to counteract interruptions to and protect CIS from the effects of and minimise the impact of major failures or disasters on CIS and recover from loss of information assets to an acceptable level through a combination of preventive and recovery measures.

38. The required implementation of business continuity measures for CIS shall be determined as a result of the risk analysis process.

II.10. Exceptional procedures

39. Notwithstanding the provisions set out in this Annex, exceptional procedures shall be permitted under emergency or specific circumstances as described in the following paragraphs.

40. Transmission of EUCI (provided it is not marked for any specific classified treatment, such as CRYPTO) protected by cryptographic products and methods approved for a lower classification level or even unencrypted transmission may be permitted with the consent of the Security Authority if and only if:

- the sender and recipient do not have the required encryption facility or no encryption facility, respectively; and

- the classified material cannot be conveyed in time by other means; and

- any delay would cause harm clearly outweighing the harm entailed by any disclosure of the classified material.

41. Under the circumstances set out in the previous subparagraph the information transmitted shall not show any markings or indications distinguishing them from an unclassified message or a message that can be protected by the available encryption facility. Their recipients shall be notified of the message classification level, without delay, by other means.

42. Should recourse be made to paragraph 40 a report shall be made to the appropriate Security Authority.

43. When transmission is confined within special secure areas, such as Class I or Class II areas, unencrypted distribution or encryption at a lower level may be used based on the result of a risk management process and with the approval of the SAA.

III. RESPONSIBILITIES OF AUTHORITIES

44. The following Information Assurance responsibilities shall be established in the Member States and the GSC. These authorities do not require single organisational entities. They shall have separate mandates, but 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.

III.1. Information Assurance Authority

45. The IA Authority shall have the following responsibilities:

(a) developing IA policy guidelines and guidance and monitor their effectiveness and pertinence;

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

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

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

(e) coordinating training and awareness on IA;

(f) ensuring the compliance of communication and information systems with the TEMPEST security policy guidelines (TEMPEST Authority); and

(g) consulting with the system provider, the security actors and representatives of users in respect to IA policy guidelines and guidance.

III.2. Information Assurance Operational Authority

46. The IA Operational Authority shall have the following responsibilities:

(a) developing system-specific security documentation in line with Council security policies and guidelines, in particular the system-specific security requirement statement (SSRS) including the residual risk statement, the security operating procedures (SecOPs), and the crypto plan within the system accreditation process;

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

(c) participating in selecting TEMPEST countermeasures and devices if required in the SSRS and ensuring that they are securely installed and maintained in cooperation with the IA Authority;

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

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

(f) providing system-specific IA training;

(g) implementing and operate system-specific network defence measures.

III.3. Security Accreditation Authority

47. The SAA shall be responsible for ensuring that systems comply with the Council's security policy. It shall grant the approval of a system to handle EUCI to a defined level of classification in its operational environment.

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

49. The Member State SAA shall be responsible for accrediting systems and system components of CISs operating within the remit a Member State.

50. A joint security accreditation board (SAB) shall act as SAA for systems with components within the remit of both the GSC SAA and Member States' SAAs. *Ad hoc* security accreditation panels may be established to act as SAA for other special systems.

51. In this context, the SAA's responsibilities shall include:

(a) establishing a security approval or accreditation process, in accordance with the Council's security policy, clearly stating the approval or accreditation conditions for systems processing EUCI under its authority;

(b) examining and approving security-related documentation, including risk management and residual risk statements, SSRSs, security implementation verification documentation and SecOPs, and ensure that it complies with the Council's security policy;

(c) providing a statement of approval or accreditation for CIS, stating the terms and conditions of the accreditation, and criteria under which re-approval or re-accreditation is required;

(d) checking implementation of security measures by undertaking or sponsoring security assessments, inspections or reviews;

(e) approving security criteria (e.g. personnel clearance levels) for sensitive positions in relation to the system;

(f) endorsing the selection of cryptographic and TEMPEST methods and products used to provide confidentiality, integrity and availability for a system; and

(g) approving, or when relevant participating in the joint approval of, the connection of a CIS handling EU information to other CISs; and

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

III.4. Crypto Approval Authority

52. The Crypto Approval Authority (CAA) shall be responsible for ensuring that cryptographic methods and products comply with national cryptographic policy or the Council's cryptographic policy, respectively. It shall grant the approval of a cryptographic method or product to protect national or 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 methods and products.

III.5. Distribution Authority

53. The Distribution Authority shall be responsible for:

(a) managing and accounting for EU crypto material;

(b) ensuring the transfer of EU crypto material to or from individuals or services using it; and

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

_____

INDUSTRIAL SECURITY

I. INTRODUCTION

1. This Annex sets out provisions on the security aspects of industrial activities related to negotiating and awarding contracts by the GSC involving or entailing access to, or the release of EUCI and to the performance of such contracts by industrial or other entities.

II. DEFINITIONS

2. For the purposes of this Annex, the following definitions shall apply:

   (a) *'Classified subcontract'*: a contract entered into by a contractor 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 generation of EUCI;

   (b) *'Contractor'*: an individual or legal entity possessing the legal capability to undertake contracts;

   (c) *'Designated Security Authority (DSA)'*: an authority responsible to the NSA of a Member State which is responsible for communicating to industrial or other entities the national policy in 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;

(d) *'Facility Security Clearance (FSC)'*: an administrative determination by an NSA or DSA that, from the security viewpoint, a facility can afford an adequate level of security protection to EU classified information 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;

(e) *'Overall level of the security classification of a contract'*: determination of the security classification of the whole contract, based on the classification of information and/or material that is to be, or may be, generated, released or accessed under any element of the overall contract. The overall level of security classification of a contract may not be lower than the highest classification of any of its elements, but may be higher because of the aggregation effect;

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

(g) *'Industrial or other entity'*: an entity involved in supplying goods, executing works or providing services; this may involve industrial, commercial, service, scientific, research, educational or development entities;

(h) *'Security Classification Guide (SCG)'*: 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. The SCG shall be part of the SAL.

III. ORGANISATION

3. The GSC may entrust by contract tasks involving or entailing access to or the release of EUCI to industrial or other entities registered in a Member State or in a third State which has concluded a security agreement with the EU.

4. Each Member State's NSA, DSA or any other competent national security authority shall ensure that these minimum standards are applied by contractors and sub-contractors located on their territory.

IV. EU CLASSIFIED CONTRACTS AND SUB-CONTRACTS

5. Prior to letting a classified contract or launching a call for tender for the letting of such, the GSC as the contracting authority shall determine the aspects of the services and supplies to be provided under the contract requiring a security classification; in doing so, the GSC shall prepare a SCG to be used for the performance of the contract.

6. The security classification of classified contracts shall take account of the following principles:

   (a) the GSC shall determine, as appropriate, the aspects of the contract which require protection and the consequent security classification; in doing so, it shall take into account the original security classification assigned by the originator to information generated before awarding the contract;

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

   (c) EUCI generated under contractual activities shall be classified in accordance with the SCG;

(d) when appropriate, the GSC shall be responsible for changing the overall level of classification of the contract, or security classification of any of its elements, in consultation with the originator, and for informing all interested parties;

(e) classified information released to the contractor or subcontractor or generated under contractual activity shall not be used for purposes other than those defined by the classified contract and shall not be disclosed to third parties without the prior written consent of the originator.

7. The NSAs or DSAs of the Member States shall ensure that contractors and subcontractors awarded classified contracts which involve classified information take all appropriate measures for safeguarding such EUCI released to or generated by them in the performance of the classified contract in accordance with national laws and regulations. Non-compliance with the security requirements may result in termination of the contract.

8. All industrial or other entities participating in classified contracts which involve access to information classified CONFIDENTIEL UE or SECRET UE shall hold a national FSC. The FSC shall be granted by the NSA or DSA of a Member State to confirm that a facility can afford and guarantee adequate security protection to EUCI at the appropriate classification level.

9. The NSA or DSA shall grant, in accordance with national laws and regulations, a PSC to all persons employed in industrial or other entities registered in that Member State whose duties require access to EU information classified CONFIDENTIEL UE or SECRET UE subject to a classified contract.

10. Classified contracts shall include an SAL as defined in paragraph 2(f). The SAL shall contain the SCG as defined in paragraph 2(h).

11. Before initiating the negotiation of a classified contract the GSC shall contact the NSA or DSA of the Member States in which the industrial or other entities concerned are registered in order to obtain confirmation that they hold or have applied for an FSC appropriate to the level of security classification of the contract.

12. The contracting authority shall not place a classified contract with a preferred bidder before having received the valid FSC certificate.

13. Unless required by Member States' national laws and regulations, an FSC shall not be required for contracts involving information classified RESTREINT UE.

14. In the case of bids in respect of classified contracts, invitations shall contain a provision requiring that a bidder which fails to submit a bid or which is not selected be required to return all documents within a specified period of time.

15. It may be necessary for a contractor to negotiate classified subcontracts with subcontractors at various levels. The contractor shall be responsible for ensuring that all subcontracting activities are undertaken in accordance with the common minimum standards contained in this Decision. However, the contractor shall not transmit EUCI or material to a subcontractor without the prior written consent of the originator.

16. The conditions under which the contractor may subcontract shall be defined in the tender and in the contract. No subcontract may be awarded to entities registered in a non-EU Member State without the express written authorisation of the GSC.

17. Throughout the life of the contract, compliance with all its security provisions shall be monitored by the relevant NSA or DSA in coordination with the GSC. Notification of security incidents shall be reported, in accordance with the provisions laid down in Article 10(5) and in Annex III to this Decision. Change or withdrawal of an FSC shall immediately be communicated to the GSC and to any other NSA or DSA to which it has been notified.

18. When a classified contract or a classified subcontract is terminated, the GSC and/or the NSA or DSA, as appropriate, shall promptly notify the NSA or DSA of the Member States in which the contractor or subcontractor is registered.

19. The common minimum standards contained in this Decision shall continue to be complied with, and the confidentiality of classified information shall be maintained by the contractors and subcontractors, after termination or conclusion of the classified contract or subcontract.

V. ISSUING OF FSCs

20. An FSC shall be granted by the NSA or DSA of the Member State where the contractor is incorporated or located. The FSC shall confirm that an industrial facility or other entity in the private sector can protect EUCI at the level of CONFIDENTIEL UE and above.

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

(a) the company has established a security system at the facility which covers all appropriate personnel and physical security measures necessary for the protection of information or material classified CONFIDENTIEL UE or above in accordance with the provisions of this Annex;

(b) the personnel security status of management, owners and employees who are required to have access to EU classified material at CONFIDENTIEL UE or above has been established in accordance with the requirements laid down in Annex I of this Decision; and

(c) the company has appointed a Facility Security Officer (FSO) who is responsible to its management and to the NSA or DSA for enforcing the security obligations within the company facilities and that the FSO is in a position to report directly to an appointed member of the Managing Board of the company.

VI. VISITS IN CONNECTION WITH CLASSIFIED CONTRACTS

22. Visits by personnel of the GSC to industrial or other entities in the Member States performing EU classified contracts shall be arranged with the relevant NSA or DSA.

23. Visits by employees of industrial or other entities within the framework of EU classified contracts shall be arranged between the NSAs or DSAs concerned. However, the NSAs or DSAs involved in an EU classified contract may agree on a procedure whereby the visits by employees of industrial or other entities can be arranged directly.

VII. TRANSMISSION AND TRANSPORTATION OF EUCI

24. With regard to the transmission of EUCI, the relevant provisions of Annex III of this Decision shall apply. In order to supplement such provisions, any existing procedures in force among Member States shall apply.

25. In general and with regard to all forms of transportation such as via hand carriage, commercial carriers, road, rail, sea or air, the international transportation of EU classified material relating to classified contracts shall be carried out in accordance with Member States national procedures. The following principles shall be applied when examining security arrangements for international transportation:

(a) security shall be assured at all stages during the transportation and under all circumstances, from the point of origin to the ultimate destination;

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

(c) an FSC shall be obtained, where appropriate, for companies providing transportation. In such cases, personnel handling the consignment shall be cleared in compliance with the common minimum standards contained in this Annex;

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

(e) whenever possible, routes should be only through EU Member States. Routes through non-EU States should only be undertaken when authorised by the NSA or DSA of the States of both the consignor and the consignee;

(f) prior to any movement of EU classified material, a Transportation Plan shall be made up by the consignor and approved by the NSAs or DSAs concerned.

_____

ANNEX VI

EXCHANGE OF CLASSIFIED INFORMATION WITH THIRD STATES AND INTERNATIONAL ORGANISATIONS

I. INTRODUCTION

1. This Annex sets out provisions for implementing the principles and standards contained in Article 13 for exchanging classified information with third States and international organisations. In particular, it sets out the possible frameworks governing the exchange of classified information (Section II), the conditions for releasing EUCI under security agreements, administrative arrangements or in the context of crisis management operations (Sections III toV), the *ad* hoc release of EUCI (Section VI) and the registration of classified information received from third States or international organisations (Section VII).

II. FRAMEWORKS GOVERNING THE EXCHANGE OF CLASSIFIED INFORMATION

2. Where the Council determines in accordance with Article 13(1) that there is a need to exchange classified information with a third State or international organisation, one of the following frameworks governing such exchange shall be established:

   (a) where the Council has established a permanent or long-term need to exchange classified information:

      (i) a security agreement; or

      (ii) an administrative arrangement;

(b) where the Council has established a need to release EUCI in the context of ESDP crisis management operations:

(i) a framework participation agreement; or

(ii) an *ad hoc* participation agreement; or

(iii) an *ad hoc* administrative arrangement;

(c) where a need arises exceptionally for EUCI to be released to a third State or international organisation: an undertaking by the third party concerned to protect the EUCI it receives in accordance with the basic principles and minimum standards set out in this Decision.

III. PERMANENT SECURITY AGREEMENTS

3. The EU may enter into permanent security agreements with third States or international organisations on the basis of Article 24 TEU.

4. Such agreements shall cover all classified information exchange needs between the EU and the third party concerned. They shall not be limited in scope or in time. They shall set out the basic principles and minimum standards applicable to the exchange of classified information with the third party in question.

5. Permanent security agreements shall also provide for technical implementing arrangements to be agreed between the GSC Security Office, the European Commission's Security Directorate and the Security Authority of the third State or international organisation in question, to be approved by the Security Committee. The implementing arrangements shall take due account of the level of protection provided by the security regulations and structures in place in the third State or international organisation concerned.

6. In order to assess the third party's security regulations and structures, the GSC Security Office, in collaboration with the European Commission's Security Directorate, shall conduct assessment visits to evaluate:

   (a) the regulatory framework applicable for the protection of 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 actually in place; and

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

7. The findings of such visits shall be set out in a report on the basis of which the Security Committee shall recommend the maximum level of EUCI which may be exchanged in hard copy and/or electronically with the third party concerned.

8. 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 informing it about the security regulations applicable and the way in which security is organised in the third State or international organisation concerned.

9. 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 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.

10. Security agreements shall provide that prior to the exchange of classified information under the agreement in question, the GSC Security Office and the European Commission's Security Directorate shall agree that the receiving Party is able to protect and safeguard information provided to it in an appropriate manner.

11. No electronic exchange of EUCI shall be permitted unless explicitly provided for in the security Agreement and/or technical implementing arrangements. In such cases, the Security Committee shall determine the maximum level of EUCI which may be released electronically, and any specific conditions governing such exchange.

12. In mutual agreement with the third party concerned, the GSC Security Office shall, at regular intervals, conduct follow-up assessment visits to third parties with which the EU has a security Agreement governing the exchange of classified information to verify that the arrangements in place continue to meet the standards originally agreed on.

13. Once the 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 or electronic form, including in the light of any follow-up assessment visit.

IV. ADMINISTRATIVE ARRANGEMENTS

14. Where the Council establishes that there is a long-term need to exchange EUCI classified no higher than RESTREINT UE, the SG/HR may, subject to approval by COREPER, enter into an administrative arrangement with the relevant authorities of a third State or international organisation. The Council may decide that an administrative arrangement may be used provisionally for exchanging information of a higher classification level where a permanent security agreement is not yet in force and where, for operational reasons, a framework for exchanging classified information needs to be put in place rapidly.

15. Unless there are exceptional operational reasons for exchanging EUCI urgently which are brought to the attention of the Security Committee, a security assessment visit as described in paragraph 6 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.

16. No electronic exchange of EUCI shall be permitted unless explicitly provided for in the administrative arrangement. In such cases, the Security Committee shall determine the maximum level of EUCI which may be released electronically, and any specific conditions governing such exchange.

V. EXCHANGE OF CLASSIFIED INFORMATION IN THE CONTEXT OF CRISIS MANAGEMENT OPERATIONS

17. Where a military or civilian crisis management operation is established under the European Security and Defence Policy (ESDP), EUCI generated for the purposes of the operation may be released to certain third States or international organisations provided that an appropriate framework is in place.

18. Framework participation agreements may cover *inter alia* the exchange of EUCI generated for the purposes of military or civilian crisis management operations with a given third State. The maximum classification level of EUCI which may be exchanged with third States in the context of a given military or civilian crisis management operation shall be determined in the Joint Action establishing the said operation.

19. *Ad hoc* participation agreements may cover *inter alia* the release of EUCI generated for the purposes of a military or civilian crisis management operation to a given third State participating in a specific crisis management operation.

20. *Ad hoc* administrative arrangements on a third State's participation in a specific military or civilian crisis management operation may cover *inter alia* the release of EUCI generated for the purposes of the operation to that third State.

21. The provisions on classified information to be included in framework participation agreements, *ad hoc* participation agreements and *ad hoc* administrative arrangements in the context of ESDP crisis management operations shall provide that the third State in question shall ensure that its personnel seconded to the operation will protect EUCI in accordance with the Council's security rules and with further guidance issued by the competent authorities, including the Head of Mission or Operation Commander.

22. If the third State in question concludes a permanent security agreement with the EU thereafter, the permanent security agreement shall supersede any framework participation agreement, *ad hoc* participation agreement or *ad hoc* administrative arrangement as far as the handling of EUCI is concerned. Permanent administrative arrangements in force with the relevant authorities of a third State or an international organisation governing the exchange of EUCI may also constitute a framework for exchanging EUCI in the context of a military or civilian crisis management operation.

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

24. Access to EUCI in premises and/or in communication and information systems of an EU military or civilian crisis management operation by personnel seconded to the said operation by a contributing third State shall not be deemed equivalent to the release of classified information to the third State in question.

25. Where the host State on whose territory the operation is conducted has no security agreement or administrative arrangement in force 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 Joint Action establishing the ESDP mission. The EUCI released under such circumstances shall be restricted to that generated for the purposes of the mission and classified no higher than RESTREINT UE. Prior to or upon actual release, the third party in question shall give written confirmation that it undertakes to protect the EUCI it receives in accordance with the basic principles and minimum standards set out in this Decision.

VI. *AD HOC* RELEASE OF EUCI

26. Where no framework is in place and an exceptional need arises to release EUCI to a third State or international organisation, the GSC shall:

(a) where necessary, verify with the security authorities of the third State or international organisation concerned that its security regulations and structures are such as to guarantee that the EUCI released to it would be protected to standards no less stringent than those set out in the Council's security rules;

(b) seek the opinion of the Security Committee as to the confidence that can be placed in the security regulations and structures in the receiving third State or international organisation concerned.

27. If the Security Committee issues an opinion in favour of releasing the information, the matter shall be referred to COREPER, which shall take a decision on releasing the information.

28. If the Security Committee's opinion is not in favour of releasing the information:

(a) for matters relating to CFSP/ESDP, 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.

29. Where deemed appropriate, and subject to the prior consent of the originator, the Security Committee or COREPER, as appropriate, 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.

30. Following a decision to release EUCI, the GSC shall forward the document concerned, which will bear a 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 to protect the EUCI it receives in accordance with the basic principles and minimum standards set out in this Decision.

VII. REGISTRATION OF CLASSIFIED INFORMATION RECEIVED FROM THIRD STATES OR INTERNATIONAL ORGANISATIONS

31. The Central Registry within the GSC shall act as the main point of entry/exit for classified information addressed to the Council or to the SG/HR by a third State or international organisation. It shall keep a record within the Council of all classified information released to and received from third States or international organisations.

APPENDICES

APPENDIX 1

Equivalence of security classifications

APPENDIX 2

List of National Security Authorities (NSAs)

APPENDIX 3

Practical classification guide

APPENDIX 4

List of abbreviations

APPENDIX 1

Equivalence of security classifications

EU Classification	TRES SECRET UE	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
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
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*
Ireland	Top Secret	Secret	Confidential	Restricted
Italy	Segretissimo	Segreto	Riservatissimo	Riservato
Cyprus	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
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-Għola 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	SALAINEN	LUOTTAMUKSELLINEN	KÄYTTÖ RAJOITETTU
Sweden[4]	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] Diffusion Restreinte / Beperkte Verspreiding is not a security classification in Belgium. Belgium handles and protects "RESTREINT UE" 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" information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

[4] 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 2

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

BULGARIA

State Commission on Information Security
1 Angel Kanchev Str.
BG-1000 Sofia
Telephone: + 359/2/921 5911
Fax: + 359/2/987 3750

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

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

GERMANY

Bundesministerium des Innern
Referat IS 4
Alt-Moabit 101 D
D-11014 Berlin
Telephone: + 49/1/888 681 15 26
Fax: + 49/1/888 681 5 15 26

ESTONIA

Estonian National Security Authority
Security Department
Ministry of Defence of the Republic of Estonia
Sakala 1
EE-15094 Tallinn
Telephone: + 372/7170 077, + 372/7170 030
Fax: + 372/7170 213

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 09 (ώρες γραφείου)
+ 30/210/657 20 10 (ώρες γραφείου)
Φαξ: + 30/210/642 64 32
+ 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 09
+ 30/210/657 20 10
Fax: + 30/210/642 64 32
+ 30/210/657 76 12

SPAIN

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera Nacional Radial VI, km 8,5
E-28023 Madrid
Telephone: + 34/91/372 57 07
+ 34/91/372 50 27
Fax: + 34/91/372 58 08

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

IRELAND

National Security Authority
Department of Foreign Affairs
80 St. Stephens Green
IRL-Dublin 2
Telephone: + 353/1/478 08 22
Fax: + 353/1/478 14 84

ITALY

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Cesis III Reparto (UCSi)
Via di Santa Susanna, 15
I-1187 Roma
Telephone: + 39/06/611 742 66
Fax: + 39/06/488 52 73

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, + 357/99 35 80 00
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, + 357/99 35 80 00
Fax: + 357/22/30 23 51

LATVIA

National Security Authority of Constitution Protection
Bureau of the Republic of Latvia
Miera Iela 85 A
LV-1001 Riga
Telephone: + 371/702 54 18
Fax: + 371/702 54 54

LITHUANIA

National Security Authority of the Republic of Lithuania
Gedimino 40/1
LT-2600 Vilnius
Telephone: + 370/5/266 32 05
Fax: + 370/5/266 32 00

LUXEMBOURG

Autorité nationale de Sécurité
Boîte postale 2379
L-1023 Luxembourg
Telephone: + 352/478 22 10 central
+ 352/478 22 53 direct
Fax: + 352/478 22 43

HUNGARY

Nemzeti Biztonsági Felügyelet
Pf. 2
HU-1357 Budapest
Telephone: + 361/346 96 52
Fax: + 361/346 96 58

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

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

AUSTRIA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
A-1014 Wien
Telephone: + 43/1/531 15 25 94
Fax: + 43/1/531 15 26 15

POLAND

Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego – ABW)
Department for the Protection of Classified Information
2A Rakowiecka St.
PL-00-993 Warszawa
Telephone: + 48/22/585 73 60
Fax: + 48/22/585 85 09

Military Counter-Intelligence Service
(Służba Kontrwywiadu Wojskowego)
Classified Information Protection Bureau
Oczki 1
PL-02-007 Warszawa
Telephone: + 48/22/684 12 47
Fax: + 48/22/684 10 76

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P-1400-204 Lisboa
Telephone: + 351/21/301 17 10
Fax: + 351/21/303 17 11

ROMANIA

Romanian ANS - ORNISS
4 Mures Street
RO-012275 Bucharest
Telephone: 00 4 021 224 58 30
Fax: 00 4 021 224 07 14

SLOVENIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorèièeva 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

FINLAND

National Security Authority

Ministry for Foreign Affairs/Security Unit

Kanavakatu 3A

P.O. Box 176

FI-00161 Helsinki

Telephone: + 358/9/160 55510

Fax: + 358/9/160 55516

SWEDEN

Utrikesdepartementet

SSSB

S-103 39 Stockholm

Telephone: + 46/8/405 54 44

Fax: + 46/8/723 11 76

UNITED KINGDOM

UK National Security Authority

PO Box 49359

GB-London SW1P 1LU

Telephone: + 44/20 7930 8768

Fax: + 44/20 7821 8604

APPENDIX 3

Practical classification guide

This Appendix will be prepared at a later stage.

APPENDIX 4

List of abbreviations

This Appendix will be prepared at a later stage.