This document is meant purely as a documentation tool and the institutions do not assume any liability for its contents

►**B**

COUNCIL DECISION

of 19 March 2001

adopting the Council's security regulations

(2001/264/EC)

(OJ L 101, 11.4.2001, p. 1)

Amended by:

		Official Journal		
		No	page	date
►**M1**	Council Decision 2004/194/EC of 10 February 2004	L 63	48	28.2.2004
►**M2**	Council Decision 2005/571/EC of 12 July 2005	L 193	31	23.7.2005
►**M3**	Council Decision 2005/952/EC of 20 December 2005	L 346	18	29.12.2005
►**M4**	Council Decision 2007/438/EC of 18 June 2007	L 164	24	26.6.2007

▼B

COUNCIL DECISION

of 19 March 2001

adopting the Council's security regulations

(2001/264/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 2000/396/EC, ECSC, Euratom of 5 June 2000 adopting the Councils Rules of Procedure [1], and in particular Article 24 thereof,

Whereas:

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

(2) Such system should combine in a single text the subject matter covered by all previous decisions and provisions in the same field.

(3) In practice, the major part of EU information classified CONFIDENTIEL UE and above will concern the Common Security and Defence Policy.

(4) 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.

(5) The Council welcomes the intention of the Commission to introduce, by the date of application of this Decision, a comprehensive system that is in line with the Annexes thereto, with a view to ensuring a smooth functioning of the decision-making process of the Union.

(6) The Council underlines the importance of associating, where appropriate, the European Parliament and the Commission with the rules and standards of confidentiality which are necessary in order to protect the interests of the Union and its Member States.

(7) This Decision is taken without prejudice to Article 255 of the Treaty and to instruments implementing it.

(8) 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

The Council's security regulations contained in the Annex are hereby approved.

Article 2

1. The Secretary-General/High Representative shall take appropriate measures to ensure that, when handling EU classified information, the regulations referred to in Article 1 are respected within the General

[1] OJ L 149, 23.6.2000, p. 21.

▼B

Secretariat of the Council (hereinafter referred to as 'GSC') by GSC officials and other servants, by GSC external contractors, and by personnel seconded to the GSC, as well as within Council premises and EU decentralised agencies ([1]).

2. Members States shall take appropriate measures, in accordance with national arrangements, to ensure that, when EU classified information is handled, the regulations referred to in Article 1 are respected, within their services and premises by:

(a) members of Member States' permanent representations to the European Union as well as by members of national delegations attending meetings of the Council or of its bodies, or participating in other Council activities;

(b) other members of the Member States' national administrations handling EU classified information, whether they serve in the territory of the Member States or abroad; and

(c) Member States' external contractors and seconded personnel, handling EU classified information.

Member States shall forthwith inform the GSC of the measures taken.

3. The measures referred to in paragraphs 1 and 2 shall be taken before 30 November 2001.

Article 3

In keeping with the basic principles and minimum standards of security contained in part I of the Annex, the Secretary-General/High Representative may take measures in accordance with part II, Section I(1) and (2), of the Annex.

Article 4

As from the day of its application, this Decision shall replace:

(a) Council Decision 98/319/EC of 27 April 1998 relating to the procedures whereby officials and employees of the General Secretariat of the Council may be allowed access to classified information held by the Council ([2]);

(b) Decision of the Secretary-General/High Representative of 27 July 2000 on measures for the protection of classified information applicable to the General Secretariat of the Council ([3]);

(c) Decision 433/97 of the Secretary-General of the Council of 22 May 1997 on the Security Clearance procedure of the officials responsible for the functioning of the Cortesy network.

Article 5

1. This Decision shall take effect on the day of its publication.

2. It shall apply from 1 December 2001.

([1]) See Council Conclusions of 10 November 2000.
([2]) OJ L 140, 12.5.1998, p. 12.
([3]) OJ C 239, 23.8.2000, p. 1.

▼B

ANNEX

SECURITY REGULATIONS OF THE COUNCIL OF THE EUROPEAN UNION

▼B

CONTENTS

PART I

Basic principles and minimum standards of security…

PART II…

SECTION I

The organisation of security in the Council of the European Union…

SECTION II

Classifications and markings…

SECTION III

Classification management…

SECTION IV

Physical security…

SECTION V

General rules on the need-to-know principle and security clearance…

SECTION VI

Security clearance procedure for GSC officials and other servants…

SECTION VII

Preparation, distribution, transmission, storage and destruction of EU classified material…

SECTION VIII

Très secret UE/EU top secret registries…

SECTION IX

Security measures to be applied at the time of specific meetings held outside the Council premises and involving high sensitivity issues…

SECTION X

Breaches of security and compromise of EU classified information…

SECTION XI

Protection of information handled in information technology and communication systems…

SECTION XII

Release of EU classified information to third States or international organisations…

Appendices

Appendix 1

List of national security authorities…

Appendix 2

Comparison of national security classifications…

Appendix 3

Practical classification guide…

Appendix 4

Guidelines for release of EU classified information to third States or international organisations…

— Level 1 cooperation

Appendix 5…

▼B

Guidelines for release of EU classified information to third States or international organisations

— Level 2 cooperation…

Appendix 6

Guidelines for release of EU classified information to third States or international organisations…

— Level 3 cooperation

▼B

PART I

BASIC PRINCIPLES AND MINIMUM STANDARDS OF SECURITY

INTRODUCTION

1. These provisions lay down the basic principles and minimum standards of security to be respected in an appropriate manner by the Council, by the General Secretariat of the Council (hereinafter called 'GSC'), by the Member States and by the decentralised agencies of the European Union (hereinafter called 'EU decentralised agencies'), so that security is safeguarded and each may be assured that a common standard of protection is established.

2. The term 'EU classified information' means any information and material, an unauthorised disclosure of which could cause varying degrees of prejudice to the EU interests, or to one or more of its Member States, whether such information originates within the EU or is received from Member States, third States or international organisations.

3. Throughout these regulations:

   (a) by 'document' is meant any letter, note, minute, report, memorandum, signal/message, sketch, photograph, slide, film, map, chart, plan, notebook, stencil, carbon, typewriter or printer ribbon, tape, cassette, computer disk, CD ROM, or other physical medium on which information has been recorded;

   (b) by 'material' is meant 'document' as defined in (a) above and also any item of equipment or weapons, either manufactured or in the process of manufacture.

4. Security has the following principal objectives:

   (a) to safeguard EU classified information from espionage, compromise or unauthorised disclosure;

   (b) to safeguard EU information handled in communications and information systems and networks, against threats to its integrity and availability;

   (c) to safeguard installations housing EU information from sabotage and malicious wilful damage;

   (d) in the event of failure, to assess the damage caused, limit its consequences and adopt the necessary remedial measures.

5. The foundations of sound security are:

   (a) within each Member State, a national security organisation responsible for:

      (i) the collection and recording of intelligence on espionage, sabotage, terrorism and other subversive activities, and

      (ii) information and advice to its government, and through it, to the Council, on the nature of the threats to security and the means of protection against them;

   (b) within each Member State, and within the GSC, a technical INFOSEC authority responsible for working with the security authority concerned to provide information and advice on technical threats to security and the means for protection against them;

   (c) regular collaboration among government departments, agencies and the appropriate GSC services, in order to establish, and recommend, as appropriate:

      (i) what information, resources and installations need to be protected, and

      (ii) common standards of protection.

6. Where confidentiality is concerned, care and experience are needed in the selection of information and material to be protected and the assessment of the degree of protection it requires. It is fundamental that the degree of protection should correspond with the security criticality of the individual piece of information and material to be protected. In order to ensure the smooth flow of information, steps shall be taken in order to avoid over classification. The classification system is the instrument for giving effect

▼B

to these principles; a similar system of classification should be followed in planning and organising ways to counter espionage, sabotage, terrorism and other threats so that the greatest measure of protection is given to the most important premises housing classified information and to the most sensitive points within them.

BASIC PRINCIPLES

7. **The security measures shall**:

(a) extend to all persons having access to classified information, classified information-carrying media, all premises containing such information and important installations;

(b) be designed to detect persons whose position might endanger the security of classified information and important installations housing classified information and provide for their exclusion or removal;

(c) prevent any unauthorised person from having access to classified information or to installations which contain it;

(d) ensure that classified information is disseminated solely on the basis of the need-to-know principle which is fundamental to all aspects of security;

(e) ensure the integrity (i.e. prevention of corruption or unauthorised alteration or unauthorised deletion) and the availability (i.e. access is not denied to those needing and authorised to have access) of all information, either classified or not classified, and especially of such information stored, processed or transmitted in electromagnetic form.

ORGANISATION OF SECURITY

Common minimum standards

8. The Council and each Member State shall ensure that common minimum standards of security are observed in all administrative and/or government departments, other EU institutions, agencies and contractors so that EU classified information can be passed in the confidence that it will be handled with equal care. Such minimum standards shall include criteria for the clearance of personnel, and procedures for the protection of EU classified information. ►**M3** Such minimum standards shall also include minimum standards to be applied when the GSC entrusts by contract tasks involving, entailing and/or containing EU classified information to industrial or other entities: these common minimum standards are contained in Section XIII of Part II. ◄

SECURITY OF PERSONNEL

Clearance of personnel

9. All persons who require access to information classified CONFIDENTIEL UE or above shall be appropriately cleared before such access is authorised. Similar clearance shall be required in the case of persons whose duties involve the technical operation or maintenance of communication and information systems containing classified information. This clearance shall be designed to determine whether such individuals:

(a) are of unquestioned loyalty;

(b) are of such character and discretion as to cast no doubt upon their integrity in the handling of classified information; or

(c) may be vulnerable to pressure from foreign or other sources, e.g. due to former residence or past associations which might constitute a risk to security.

Particularly close scrutiny in the clearance procedures shall be given to persons:

(d) to be granted access to TRÈS SECRET UE/EU TOP SECRET information;

(e) occupying positions involving regular access to a considerable volume of SECRET UE information;

▼B

(f) whose duties give them special access to mission-critical communication or information systems and thus the opportunity to gain unauthorised access to large amounts of EU classified information or to inflict serious damage upon the mission through acts of technical sabotage.

In the circumstances outlined in subparagraphs (d), (e) and (f), the fullest practicable use shall be made of the technique of background investigation.

10. When persons not having an established 'need to know' are to be employed in circumstances in which they may have access to EU classified information (e.g. messengers, security agents, maintenance personnel and cleaners, etc.), they shall first be appropriately security-cleared.

Records of personnel clearances

11. All services, bodies or establishments handling EU classified information or housing mission-critical communication or information systems shall maintain a record of the clearances granted to the personnel assigned thereto. Each clearance shall be verified as the occasion demands to ensure that it is adequate for that person's current assignment; it shall be re-examined as a matter of priority whenever new information is received indicating that continued assignment on classified work is no longer consistent with the interests of security. The record of clearances shall be held by the head of security for the service, body or establishment concerned.

Security instruction of personnel

12. All personnel employed in positions where they could have access to classified information shall be thoroughly instructed on taking up assignment and at regular intervals in the need for security and the procedures for accomplishing it. It is a useful procedure to require that all such personnel should certify in writing that they fully understand the security regulations relevant to their assignment.

Management responsibilities

13. Managers shall have the duty of knowing those of their staff who are engaged in classified work or who have access to mission-critical communication or information systems and of recording and reporting any incidents or apparent vulnerabilities, likely to have a bearing on security.

Security status of personnel

14. Procedures shall be established to ensure that, when adverse information becomes known concerning an individual, it is determined whether the individual is employed on classified work or has access to mission-critical communication or information systems, and the authority concerned informed. If it is established that such an individual constitutes a security risk, he or she shall be barred or removed from assignments where he or she might endanger security.

PHYSICAL SECURITY

Need for protection

15. The degree of physical security measures to be applied to ensure the protection of EU classified information shall be proportional to the classification, volume of and threat to the information and material held. Therefore care shall be taken to avoid both over- and under-classification, and classification shall be subject to regular review. All holders of EU classified information shall follow uniform practices regarding classification of that information and meet common standards of protection regarding custody, transmission and disposal of information and material requiring protection.

Checking

16. Before leaving areas containing EU classified information unattended, persons having custody thereof shall ensure that it is securely stored and that all security devices have been activated (locks, alarms, etc.). Further independent checks shall be carried out after working hours.

Security of buildings

17. Buildings housing EU classified information or mission-critical communication and information systems shall be protected against unauthorised access. The nature of the protection afforded to EU classified information,

▼B

e.g. barring of windows, locks for doors, guards at entrances, automated access control systems, security checks and patrols, alarm systems, intrusion detection systems and guard dogs, shall depend on:

(a) the classification, volume and location within the building of the information and material to be protected;

(b) the quality of the security containers for this information and material;

(c) the physical nature and location of the building.

18. The nature of the protection afforded to communication and information systems shall similarly depend upon an assessment of the value of the assets at stake and of the potential damage if security were compromised, upon the physical nature and location of the building in which the system is housed, and upon the location of the system within the building.

Contingency plans

19. Detailed plans shall be prepared in advance for the protection of classified information during a local or national emergency.

SECURITY OF INFORMATION (INFOSEC)

20. INFOSEC relates to the identification and application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems against loss of confidentiality, integrity or availability, whether accidental or intentional. Adequate countermeasures shall be taken in order to prevent access to EU information by unauthorised users, to prevent the denial of access to EU information to authorised users, and to prevent corruption or unauthorised modification or deletion of EU information.

COUNTER-SABOTAGE AND OTHER FORMS OF MALICIOUS WILFUL DAMAGE

21. Physical precautions for the protection of important installations housing classified information are the best protective security safeguards against sabotage and malicious wilful damage, and clearance of personnel alone is not an effective substitute. The competent national body shall collect intelligence regarding espionage, sabotage, terrorism and other subversive activities.

RELEASE OF CLASSIFIED INFORMATION TO THIRD STATES OR INTERNATIONAL ORGANISATIONS

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

23. If the Council receives classified information from third States, from international organisations or from other third parties, that information shall be given protection appropriate to its classification and equivalent to the standards established in these regulations for EU classified information, or such higher standards as may be required by the third party releasing the information. Mutual checks may be arranged.

24. The above principles shall be implemented in accordance with the detailed provisions set out in part II.

▼B

PART II

SECTION I

THE ORGANISATION OF SECURITY IN THE COUNCIL OF THE EUROPEAN UNION

The Secretary-General/High Representative

1. The Secretary-General/High Representative shall:

   (a) implement the Council's security policy;

   (b) consider security problems referred to him by the Council or its competent bodies;

   (c) examine questions involving changes in the Council security policy, in close liaison with the National Security (or other appropriate) Authorities of the Member States (hereinafter 'NSA'). Appendix 1 contains a list of those authorities.

2. In particular, the Secretary-General/High Representative shall be responsible for:

   (a) coordinating all matters of security relating to Council activities;

   (b) requesting that each Member State set up a central TRÈS SECRET UE/EU TOP SECRET registry and requiring such a registry to be set up in the EU decentralised agencies, where appropriate;

   (c) addressing to the designated authorities of the Member States requests for the NSA to provide security clearances for personnel employed in the GSC in accordance with Section VI;

   (d) investigating or ordering an investigation into any leakage of EU classified information which, on prima facie evidence, has occurred in the GSC or any of the EU decentralised agencies;

   (e) requesting the appropriate security authorities to initiate investigations when a leakage of EU classified information appears to have occurred outside the GSC or the EU decentralised agencies, and coordinating the enquiries when more than one security authority is involved;

   (f) carrying out jointly and in agreement with the NSA concerned, periodic examinations of the security arrangements for the protection of EU classified information in the Member States;

   (g) maintaining close liaison with all security authorities concerned in order to achieve overall coordination of security;

   (h) keeping the Council security policy and procedures constantly under review and, as required, preparing appropriate recommendations. In this regard, he shall present to the Council the annual inspection plan prepared by the GSC Security Office.

The Security Committee of the Council

3. A Security Committee shall be set up. It shall consist of representatives of the NSA of each Member State. It shall be chaired by the Secretary-General/High Representative or by his/her delegate. Representatives of EU decentralised agencies may also be invited to attend when questions concerning them are discussed.

4. The Security Committee shall meet as instructed by the Council, at the request of the Secretary-General/High Representative or of an NSA. The Committee shall have the power to examine and assess all issues of security relating to the proceedings of the Council, and to present recommendations to the Council as appropriate. As regards the activity of the GSC, the Committee shall have the power to make recommendations on security issues to the Secretary-General/High Representative.

The Security Office of the General Secretariat of the Council

5. In order to fulfil the responsibilities mentioned in paragraphs 1 and 2, the Secretary-General/High Representative shall have the GSC Security Office at

▼B

his disposal for coordinating, supervising and implementing security measures.

6. The Head of the GSC Security Office shall be the principal adviser to the Secretary-General/High Representative on security matters and shall act as secretary to the Security Committee. In this regard he shall direct the updating of the security regulations and coordinate security measures with the competent authorities of the Member States and, as appropriate, with international organisations linked to the Council by security agreements. To that effect, he/she shall act as a liaison officer.

7. The Head of the GSC Security Office shall be responsible for the accreditation of IT systems and networks within the GSC. The Head of the GSC Security Office and the relevant NSA shall jointly decide, where appropriate, on the accreditation of IT systems and networks involving the GSC, the Member States, EU decentralised agencies and/or third parties (States or international organisations).

EU decentralised agencies

8. Each director of an EU decentralised agency shall be responsible for the implementation of security within his or her establishment. He or she will normally nominate a member of his or her staff as being responsible to him or her in this field. This staff member is designated as a security official.

Member States

9. Each Member State should designate an NSA responsible for the security of EU classified information ([1]).

10. In the framework of each Member State administration, the corresponding NSA should be responsible for:

    (a) the maintenance of the security of EU classified information held by any national department, body or agency, public or private, at home or abroad;

    (b) authorising the establishment of TRÈS SECRET UE/EU TOP SECRET registries (this authority may be delegated to the TRÈS SECRET UE/EU TOP SECRET Control Officer of a Central Registry);

    (c) the periodic inspection of the security arrangements for the protection of EU classified information;

    (d) ensuring that all nationals as well as foreigners employed within a national department, body or agency who may have access to EU information classified TRÈS SECRET UE/EU TOP SECRET, SECRET UE and CONFIDENTIEL UE have been security cleared;

    (e) devising such security plans as are considered necessary to prevent EU classified information from falling into unauthorised hands.

Mutual security inspections

11. Periodic inspections of the security arrangements for the protection of EU classified information in the GSC and in the Permanent Representations of the Member States to the European Union, as well as to the Member States premises in the Council buildings shall be carried out by the GSC Security Office and by the NSA concerned, jointly and in mutual agreement ([2]).

12. Periodic inspections of the security arrangements for the protection of EU classified information in the EU decentralised agencies, shall be carried out by the GSC Security Office or, at the Secretary-General's request, by the NSA of the host Member State.

([1]) For a list of NSAs responsible for the security of EU classified information, see Appendix 1.

([2]) Without prejudice to the Vienna Convention of 1961 on diplomatic relations.

▼B

SECTION II

CLASSIFICATIONS AND MARKINGS

LEVELS OF CLASSIFICATION ([1])

Information is classified at the following levels:

1. TRÈS SECRET UE/EU TOP SECRET: this classification shall be applied only to 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 its Member States.

2. SECRET UE: this classification shall be applied only to information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of its Member States.

3. CONFIDENTIEL UE: this classification shall be applied to information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of its Member States.

4. RESTREINT UE: this classification shall be applied to information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of its Member States.

MARKINGS

5. A caveat marking may be used for specifying the field covered by the document or a particular distribution on a need-to-know basis.

6. The ESDP/PESD marking shall be applied to documents and copies thereof concerning the security and defence of the Union or of one or more of its Member States, or concerning military or non-military crisis management.

7. Certain documents, namely related to Information Technology (IT) Systems may bear an additional marking entailing supplementary security measures as defined in the appropriate regulations.

AFFIXING OF CLASSIFICATION AND MARKINGS

8. Classification and markings shall be applied as follows:

   (a) on RESTREINT UE documents, by mechanical or electronic means,

   (b) on CONFIDENTIEL UE documents, by mechanical means and by hand or by printing on pre-stamped, registered paper,

   (c) on SECRET UE and TRÈS SECRET UE/EU TOP SECRET documents, by mechanical means and by hand.

([1]) A comparative table of EU, NATO, WEU and Member States' security gradings may be found in Appendix 2.

▼B

SECTION III

CLASSIFICATION MANAGEMENT

1. Information shall be classified only when necessary. The classification shall be clearly and correctly indicated, and shall be maintained only as long as the information requires protection.

2. The responsibility for classifying information and for any subsequent downgrading or declassification ([1]) rests solely with the originator.

   Officials and other servants of the GSC shall classify, downgrade or declassify information on instruction from or with the agreement of their Director-General.

3. The detailed procedures for the treatment of classified documents have been so framed as to ensure that they are subject to protection appropriate to the information they contain.

4. The number of persons authorised to originate TRÈS SECRET UE/EU TOP SECRET documents shall be kept to a minimum, and their names kept on a list drawn up by the GSC, each Member State, and, where appropriate, by each EU decentralised agency.

APPLICATION OF CLASSIFICATIONS

5. The classification of a document shall be determined by the level of sensitivity of its contents in accordance with the definition at Section II, paragraphs 1 to 4. It is important that classification is correctly and sparingly used. This applies especially to TRÈS SECRET UE/EU TOP SECRET classification.

6. The originator of a document which is to be given a classification shall bear in mind the regulations set out above and curb any tendency to over- or under-classify.

   Although a high classification may, at first sight, appear to guarantee more protection to a document, routine over-classification can result in a loss of confidence in the validity of the classification system.

   On the other hand, documents shall not be underclassified with a view to avoiding the constraints connected with protection.

   A practical guide for the classification is contained in Appendix 3.

7. Individual pages, paragraphs, sections, annexes, appendices, attachments and enclosures of a given document may require different classifications and shall be marked accordingly. The classification of the document as a whole shall be that of its most highly classified part.

8. The classification of a letter or note covering enclosures shall be as high as the highest classification of its enclosures. The originator should indicate clearly at which level it should be classified when detached from its enclosures.

DOWNGRADING AND DECLASSIFICATION

9. EU classified documents may be downgraded or declassified only with the permission of the originator, and, if necessary, after discussion with other interested parties. Downgrading or declassification shall be confirmed in writing. The originating Institution, Member State, office, successor organisation or higher authority shall be responsible for informing its addressees of the change, and they in turn shall be responsible for informing any subsequent addressees, to whom they have sent or copied the document, of the change.

10. If possible, originators shall specify on classified documents a date or period when the contents may be downgraded or declassified. Otherwise, they shall keep the documents under review every five years, at the latest, in order to ensure that the original classification is necessary.

([1]) Downgrading (déclassement) means a reduction in the level of classification; declassification (déclassification) means the removal of any classification.

▼B

SECTION IV

PHYSICAL SECURITY

GENERAL

1. The main objective of physical security measures is to prevent an unauthorised person from gaining access to EU classified information and/or material.

SECURITY REQUIREMENTS

2. All premises, areas, buildings, offices, rooms, communication and information systems, etc. in which EU classified information and material is stored and/or handled shall be protected by appropriate physical security measures.

3. In deciding what degree of physical security protection is necessary, account shall be taken of all relevant factors such as:

   (a) the classification of information and/or material;

   (b) the amount and form (for example hard copy, computer storage media) of the information held;

   (c) the locally assessed threat from intelligence services which target the EU, the Member States, and/or other institutions or third parties holding EU classified information from, namely, sabotage, terrorism and other subversive and/or criminal activities.

4. The physical security measures applied shall be designed to:

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

   (b) deter, impede and detect actions by disloyal personnel (the spy within);

   (c) prevent those officials and other servants of the GSC, of government departments of the Member States and/or other institutions or third parties who do not have a need to know from having access to EU classified information.

PHYSICAL SECURITY MEASURES

Security areas

5. Areas where information classified CONFIDENTIEL UE or higher is handled and stored shall be so organised and structured as to correspond to one of the following:

   (a) Class I security area: an area where 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. Such an area requires:

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

      (ii) an entry control system, which admits only those duly cleared and specially authorised to enter the area;

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

   (b) Class II security area: an area where CONFIDENTIEL UE or above is handled and stored in such a way that it can be protected from access by unauthorised persons by means of internally established controls, e.g. premises containing offices in which CONFIDENTIEL UE or above is regularly handled and stored. Such an area requires:

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

      (ii) an entry control system which admits unescorted only those duly cleared and specially authorised to enter the area. For all other persons, provision shall be made for escorts or equivalent controls, to prevent unauthorised access to EU classified information and uncontrolled entry to areas subject to technical security inspections.

▼B

Those areas not occupied by duty personnel on a 24-hour basis shall be inspected immediately after normal working hours to ensure that EU classified information is properly secured.

Administrative area

6. Around or leading up to Class I or Class II security areas, an administrative area of lesser security may be established. Such an area requires a visibly defined perimeter allowing personnel and vehicles to be checked. Only RESTREINT UE information shall be handled and stored in administrative areas.

Entry and exit controls

7. Entry into Class I and Class II security areas shall be controlled by a pass or personal recognition system applicable to the permanent staff. A system of visitor checks designed to deny unauthorised access to EU classified information shall also be established. Pass systems may be supported by automated identification, which shall be regarded as a supplement to, but not a total replacement for guards. A change in the threat assessment may entail a strengthening of the entry and exit control measures, for example during the visit of prominent persons.

Guard patrols

8. Patrols of Class I and Class II security areas are to take place outside normal working hours to protect EU assets against compromise, damage or loss. The frequency of patrols will be determined by local circumstances but, as a guide, are to be conducted once every two hours.

Security containers and strong rooms

9. Three classes of containers shall be used for the storage of EU classified information:

   — Class A: containers nationally approved for storage of TRÈS SECRET UE/EU TOP SECRET information within a Class I or a Class II security area;

   — Class B: containers nationally approved for storage of SECRET UE and CONFIDENTIEL UE information within a Class I or a Class II security area;

   — Class C: office furniture suitable for storage of RESTREINT UE information only.

10. For strong rooms constructed within a Class I or a Class II security area, and for all Class I security areas where information classified CONFIDENTIEL UE and higher is stored on open shelves or displayed on charts, maps, etc., the walls, floors and ceilings, door(s) with lock(s) shall be certified by an NSA as offering equivalent protection to the class of security container approved for the storage of information of the same classification.

Locks

11. Locks used with security containers and strong rooms in which EU classified information is stored shall meet the following standards:

   — Group A: nationally approved for Class A containers;

   — Group B: nationally approved for Class B containers;

   — Group C: suitable for Class C office furniture only.

Control of keys and combinations

12. Keys of security containers shall not be taken out of the office building. Combination settings of security containers shall be committed to memory by persons needing to know them. For use in an emergency, the Security Officer of the establishment concerned shall be responsible for holding spare keys and a written record of each combination setting; the latter shall be held in separate sealed opaque envelopes. Working keys, spare security keys and combination settings shall be kept in separate security containers. These keys and combination settings should be given security protection no less stringent than the material to which they give access.

13. Knowledge of the combination settings of security containers shall be restricted to as few people as practicable. Combinations shall be reset:

▼B

(a) on receipt of a new container;

(b) whenever a change of personnel occurs;

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

(d) at intervals of preferably six months and at least every 12 months.

Intrusion detection devices

14. When alarm systems, closed circuit television and other electrical devices are used to protect EU classified information, an emergency electrical supply shall be available to ensure the continuous operation of the system if the main power supply is interrupted. Another basic requirement is that a malfunction in or tampering with such systems shall result in an alarm or other reliable warning to the surveillance personnel.

Approved equipment

15. NSAs shall maintain, from their own or from bilateral resources, up-to-date lists by type and model of the security equipment which they have approved for the direct or indirect protection of classified information under various specified circumstances and conditions. The GSC Security Office shall maintain a similar list, based, *inter alia*, on information from NSAs. EU decentralised agencies shall consult with the GSC Security Office and, as appropriate, with the NSA of their host Member State before purchasing such equipment.

Physical protection of copying and telefax machines

16. Copying and telefax machines shall be physically protected to the extent necessary to ensure that only authorised persons can use them and that all classified products are subject to proper controls.

PROTECTION AGAINST OVERLOOKING AND EAVESDROPPING

Overlooking

17. All appropriate measures shall be taken by day and by night to ensure that EU classified information is not seen, even accidentally, by any unauthorised person.

Eavesdropping

18. Offices or areas in which information classified SECRET UE and above is regularly discussed shall be protected against passive and active eavesdropping attacks where the risk demands it. The assessment of the risk of such attacks shall be the responsibility of the competent security authority after consultation, as necessary, with NSAs.

19. To determine the protective measures to be taken in premises sensitive to passive eavesdropping (e.g. insulation of walls, doors, floors and ceilings, measurement of compromising emanations) and to active eavesdropping (e.g. search for microphones), the GSC Security Office may request assistance from experts from NSAs. Security officers of EU decentralised agencies may request technical inspections to be carried out by the GSC Security Office and/or the assistance from experts from NSAs.

20. Likewise, when circumstances require, the telecommunications equipment and the electrical or electronic office equipment of any kind used during meetings at SECRET UE level and above may be checked by technical security specialists of NSAs at the request of the competent Security Officer.

TECHNICALLY SECURE AREAS

21. Certain areas may be designated as technically secure areas. A special entry check shall be carried out. Such areas shall be kept locked by an approved method when not occupied and all keys treated as security keys. Such areas shall be subject to regular physical inspections, which will also be undertaken following any unauthorised entry or suspicion of such an entry.

22. A detailed inventory of equipment and furniture shall be kept in order to monitor their movements. No item of furniture or equipment shall be brought into such an area until it has undergone a careful inspection by specially trained security personnel, designed to detect any listening devices. As a

▼B

general rule, the installation of communication lines in technically secure areas should be avoided.

▼B

SECTION V

GENERAL RULES ON THE NEED-TO-KNOW PRINCIPLE AND SECURITY CLEARANCE

1. Access to EU classified information will be authorised only for persons having a 'need-to-know' for carrying out their duties or missions. Access to TRÈS SECRET UE/EU TOP SECRET, SECRET UE and CONFIDENTIEL UE information will be authorised only for persons in possession of the appropriate security clearance.

2. The responsibility for determining 'need-to-know' will rest within the GSC, the EU decentralised agencies and with the Member State's service or department in which the person concerned is to be employed, according to the requirements of the task.

3. The clearance of personnel will be the responsibility of the official's employer based on relevant applicable procedures. As regards GSC officials and other servants, the security clearance procedure is provided for in Section VI.

   This will result in the issue of a 'security certificate' showing the level of classified information to which the cleared person may have access and the date of expiry.

   A security certificate for a given classification may give the holder access to information with a lower classification.

4. Persons other than officials or other servants of the GSC or of Member States, for example members, officials or servants of EU institutions, with whom it may be necessary to discuss, or to whom it may be necessary to show, EU classified information, must have a security clearance as regards EU classified information and be briefed as to their responsibility for security. The same rule shall apply, in similar circumstances, to external contractors, experts or consultants.

SPECIFIC RULES ON ACCESS TO TRÈS SECRET UE/EU TOP SECRET INFORMATION

5. All persons who are to have access to TRÈS SECRET UE/EU TOP SECRET information shall first be screened for access to such information.

6. All persons who are required to have access to TRÈS SECRET UE/EU TOP SECRET information shall be designated by the Head of their department and their names kept in the appropriate TRÈS SECRET UE/EU TOP SECRET registry.

7. Before having access to TRÈS SECRET UE/EU TOP SECRET information, all persons shall sign a certificate to the effect that they have been briefed on Council security procedures and that they fully understand their special responsibility for safeguarding TRÈS SECRET UE/EU TOP SECRET information, and the consequences which the EU rules and national law or administrative rules provide when classified information passes into unauthorised hands, either by intent or through negligence.

8. In the case of persons having access to TRÈS SECRET UE/EU TOP SECRET information at meetings, etc., the competent Control Officer of the service or body in which that person is employed shall notify the body organising the meeting that the persons concerned have such authorisation.

9. The names of all persons ceasing to be employed on duties requiring access to TRÈS SECRET UE/EU TOP SECRET information shall be removed from the TRÈS SECRET UE/EU TOP SECRET list. In addition, the attention of all such persons shall be drawn again to their special responsibility for the safeguarding of TRÈS SECRET UE/EU TOP SECRET information. They shall also sign a declaration stating that they will neither use nor pass on TRÈS SECRET UE/EU TOP SECRET information in their possession.

SPECIFIC RULES ON ACCESS TO SECRET UE AND CONFIDENTIEL UE INFORMATION

10. All persons who are to have access to SECRET UE or CONFIDENTIEL UE information shall first be screened to the appropriate grading.

▼B

11. All persons who are to have access to SECRET UE or CONFIDENTIEL UE information shall be acquainted with the appropriate security regulations and shall be aware of the consequences of negligence.

12. In the case of persons having access to SECRET UE or CONFIDENTIEL UE information at meetings, etc., the Security Officer of the body in which that person is employed shall notify the body organising the meeting that the persons concerned have such authorisation.

SPECIFIC RULES ON ACCESS TO RESTREINT UE INFORMATION

13. Persons with access to RESTREINT UE information will be made aware of these security regulations and of the consequences of negligence.

TRANSFERS

14. When a member of staff is transferred from a post which involves the handling of EU classified material, the Registry will oversee the proper transfer of that material from the outgoing to the incoming official.

SPECIAL INSTRUCTIONS

15. Persons who are required to handle EU classified information should, on first taking up their duties and periodically thereafter, be made aware of:

    (a) the dangers to security arising from indiscreet conversation;

    (b) precautions to take in their relations with the press;

    (c) the threat presented by the activities of intelligence services which target the EU and Member States as regards EU classified information and activities;

    (d) the obligation to report immediately to the appropriate security authorities any approach or manoeuvre giving rise to suspicions of espionage activity or any unusual circumstances relating to security.

16. All persons normally exposed to frequent contact with representatives of countries whose intelligence services target the EU and Member States as regards EU classified information and activities shall be given a briefing on the techniques known to be employed by various intelligence services.

17. There are no Council security regulations concerning private travel to any destination by personnel cleared for access to EU classified information. The competent security authorities will, however, acquaint the officials and other servants falling within their responsibility with travel regulations to which they may be subject. It will be the responsibility of the security officers to arrange refresher meetings for staff members on these special instructions.

▼B

SECTION VI

SECURITY CLEARANCE PROCEDURE FOR GSC OFFICIALS AND OTHER SERVANTS

1. Only officials and other servants of the GSC or persons working within the GSC who, by reason of their duties and for the requirements of the service, need to have knowledge of, or to use, classified information held by the Council, shall have access to such information.

2. In order to have access to information classified as 'TRÈS SECRET UE/EU TOP SECRET', 'SECRET UE' and 'CONFIDENTIEL UE', the persons referred to in paragraph 1 must have been authorised, in accordance with the procedure referred to in paragraphs 4 and 5.

3. Authorisation shall be granted only to persons who have undergone security screening by the competent national authorities of the Member States (NSA) in accordance with the procedure referred to in paragraphs 6 to 10.

4. The appointing authority within the meaning of Article 2, first subparagraph of the Staff Regulations shall be responsible for granting the authorisations referred to in paragraphs 1, 2 and 3.

   The appointing authority shall grant authorisation after obtaining the opinion of the competent national authorities of the Member States on the basis of security screening carried out in accordance with paragraphs 6 to 12.

5. Authorisation, which shall be valid for a period of five years, may not exceed the duration of the tasks on the basis of which it was granted. It may be renewed by the appointing authority in accordance with the procedure referred to in paragraph 4.

   Authorisation shall be withdrawn by the appointing authority where it considers there are justifiable grounds for doing so. Any decision to withdraw authorisation shall be notified to the person concerned, who may ask to be heard by the appointing authority, and to the competent national authority.

6. The aim of security screening shall be to establish that there are no objections to allowing the person to have access to classified information held by the Council.

7. Security screening shall be carried out with the assistance of the person concerned and at the request of the appointing authority by the competent national authorities of the Member State of which the person subject to authorisation is a national. Should the person concerned reside in the territory of another Member State, the national authorities concerned may secure the cooperation of the authorities of the State of residence.

8. As part of the screening procedure, the person concerned shall be required to complete a personal information form.

9. The appointing authority shall specify in its request the type and level of classified information to be made available to the person concerned, so that the competent national authorities can carry out the screening process and give their opinion as to the level of authorisation it would be appropriate to grant to that person.

10. The whole security-screening process together with the results obtained shall be subject to the relevant rules and regulations in force in the Member State concerned, including those concerning appeals.

11. Where the competent national authorities of the Member State give a positive opinion, the appointing authority may grant the person concerned authorisation.

12. A negative opinion by the competent national authorities shall be notified to the person concerned, who may ask to be heard by the appointing authority. Should it consider it necessary, the appointing authority may ask the competent national authorities for any further clarification they can provide. If the negative opinion is confirmed, authorisation shall not be granted.

13. All persons granted authorisation within the meaning of paragraphs 4 and 5 shall, at the time the authorisation is granted and at regular intervals thereafter, receive any necessary instructions concerning the protection of classified information and the means of ensuring such protection. Such

▼B

persons shall sign a declaration acknowledging receipt of the instructions and give an undertaking to obey them.

14. The appointing authority shall take any measure necessary in order to implement this section, in particular as regards the rules governing access to the list of authorised persons.

15. Exceptionally, if required by the service, the appointing authority may, after giving the national competent authorities notification and provided there is no reaction from them within a month, grant temporary authorisation for a period not exceeding six months, pending the outcome of the screening referred to in paragraph 7.

16. The provisional and temporary authorisations thus granted shall not give access to TRÈS SECRET UE/EU TOP SECRET information; such access shall be limited to officials who have effectively undergone a screening with positive results, in accordance with paragraph 7. Pending the outcome of the screening, the officials requested to be cleared at TRÈS SECRET UE/EU TOP SECRET level, may be authorised temporarily and provisionally, to access information classified up to, and including SECRET UE.

▼B

SECTION VII

PREPARATION, DISTRIBUTION, TRANSMISSION, STORAGE AND DESTRUCTION OF EU CLASSIFIED MATERIAL

Contents

General provisions

Chapter I Preparation and distribution of EU classified documents…

Chapter II Transmission of EU classified documents…

Chapter III Electrical and other means of technical transmission…

Chapter IV Extra copies and translations of, and extracts from, EU classified documents…

Chapter V Musters and checks, storage and destruction of EU classified documents…

Chapter VI Specific rules applicable to documents intended for the Council…

▼B

General provisions

This section details measures for the preparation, distribution, transmission, storage and destruction of EU classified documents as defined in paragraph 3 (a) of the Basic Principles and Minimum Standards of Security set out in part I of this Annex. It shall be used as a reference for the adaptation of those measures for other EU classified material, according to its type and on a case-by-case basis.

Chapter I

Preparation and distribution of EU classified documents

PREPARATION

1. The EU classifications and markings shall be applied as established in Section II and appear at the top and bottom centre of each page, and each page shall be numbered. Each EU classified document shall bear a reference number and a date. In the case of TRÈS SECRET UE/EU TOP SECRET and SECRET UE documents, this reference number shall appear on each page. If they are to be distributed in several copies, each one shall bear a copy number, which will appear on the first page, together with the total number of pages. All annexes and enclosures shall be listed on the first page of a document classified CONFIDENTIEL UE and above.

2. Documents classified CONFIDENTIEL UE and above shall be typed, translated, stored, photocopied, reproduced magnetically or microfilmed only by persons who have been cleared for access to EU classified information up to at least the appropriate security classification of the document in question, except in the special case described in paragraph 27 of this section.

   The provisions regulating the computerised production of classified documents are set out in Section XI.

DISTRIBUTION

3. EU classified information shall be distributed only to persons with a need to know and having the appropriate security clearance. The initial distribution shall be specified by the originator.

4. TRÈS SECRET UE/EU TOP SECRET documents shall be circulated through TRÈS SECRET UE/EU TOP SECRET registries (see Section VIII). In the case of TRÈS SECRET UE/EU TOP SECRET messages, the competent registry may authorise the Head of the communications centre to produce the number of copies specified in the list of addressees.

5. Documents classified SECRET UE and below may be redistributed by the original addressee to other addressees based on a need to know. The originating authorities shall, however, clearly state any caveats they wish to impose. Whenever such caveats are imposed, the addressees may redistribute the documents only with the originating authorities' authorisation.

6. Every document classified CONFIDENTIEL UE and above shall, on arriving at or leaving an establishment, be recorded by the establishment's registry. The particulars to be entered (references, date and where applicable the copy number) shall be such as to identify the documents and be entered into a logbook or in special protected computer media.

Chapter II

Transmission of EU classified documents

PACKAGING

7. Documents classified CONFIDENTIEL UE and above shall be transmitted in heavy duty, opaque double envelopes. The inner envelope shall be marked with the appropriate EU security classification as well as, if possible, full particulars of the recipient's job title and address.

8. Only a Registry Control Officer, or his substitute, may open the inner envelope and acknowledge receipt of the documents enclosed, unless that envelope is addressed to an individual. In such a case, the appropriate Registry shall log the arrival of the envelope, and only the individual to whom it is addressed may open the inner envelope and acknowledge receipt of the documents it contains.

▼B

9. A receipt form shall be placed in the inner envelope. The receipt, which will not be classified, should quote the reference number, date and copy number of the document, but never its subject.

10. The inner envelope shall be enclosed in an outer envelope bearing a package number for receipting purposes. Under no circumstances shall the security classification appear on the outer envelope.

11. For documents classified CONFIDENTIEL UE and above, couriers and messengers shall obtain receipts against the package numbers.

TRANSMISSION WITHIN A BUILDING OR GROUP OF BUILDINGS

12. Within a given building or group of buildings, classified documents may be carried in a sealed envelope bearing only the addressee's name, on condition that it is carried by a person cleared to the level of classification of the documents.

TRANSMISSION OF EU DOCUMENTS WITHIN A COUNTRY

13. Within a country, TRÈS SECRET UE/EU TOP SECRET documents should be sent only by means of official messenger service or by persons authorised to have access to TRÈS SECRET UE/EU TOP SECRET information.

14. Whenever a messenger service is used for the transmission of a TRÈS SECRET UE/EU TOP SECRET document outside the confines of a building or group of buildings, the packaging and receipting provisions contained in this Chapter shall be complied with. Delivery services shall be so staffed as to ensure that packages containing TRÈS SECRET UE/EU TOP SECRET documents remain under the direct supervision of a responsible official at all times.

15. Exceptionally, TRÈS SECRET UE/EU TOP SECRET documents may be taken by officials, other than messengers, outside the confines of a building or group of buildings for local use at meetings and discussions, provided that:

    (a) the bearer is authorised to have access to those TRÈS SECRET UE/EU TOP SECRET documents;

    (b) the mode of transportation complies with national rules governing the transmission of national TOP SECRET documents;

    (c) under no circumstances does the official leave the TRÈS SECRET UE/EU TOP SECRET documents unattended;

    (d) arrangements are made for the list of documents so carried to be held in the TRÈS SECRET UE/EU TOP SECRET Registry holding the documents and recorded in a log, and checked against this record on their return.

16. Within a given country, SECRET UE and CONFIDENTIEL UE documents may be sent either by post, if such transmission is permitted under national regulations and is in accordance with the provisions of those regulations, or by messenger service or by persons cleared for access to EU classified information.

17. Each Member State or, EU decentralised agency, should prepare instructions on the personal carrying of EU classified documents based on these regulations. The bearer should be required to read and sign these instructions. In particular, the instructions should make it clear that, under no circumstances, may documents:

    (a) leave the bearer's possession unless they are in safe custody in accordance with the provisions contained in Section IV;

    (b) be left unattended in public transport or private vehicles, or in places such as restaurants or hotels. They may not be stored in hotel safes or left unattended in hotel rooms;

    (c) be read in public places such as aircraft or trains.

TRANSMISSION FROM ONE MEMBER STATE TO ANOTHER

18. Material classified CONFIDENTIEL UE and above should be conveyed from one Member State to another by diplomatic or military courier services.

19. However, the personal carriage of material classified SECRET UE and CONFIDENTIEL UE may be permitted if provisions for the carriage are such as to ensure that they cannot fall into any unauthorised person's hands.

▼B

20. NSAs may authorise personal carriage when diplomatic and military couriers are not available or the use of such couriers would result in a delay that would be detrimental to EU operations and the material is urgently required by the intended recipient. Each Member State should prepare instructions covering the personal carriage of material classified up to and including SECRET UE internationally by persons other than diplomatic and military couriers. The instructions should require that:

    (a) the bearer has the appropriate security clearance granted by Member States;

    (b) a record is held in the appropriate office or registry of all material so carried;

    (c) packages or bags containing EU material bear an official seal to prevent or discourage inspection by customs, and labels with identification and instructions to the finder;

    (d) the bearer carries a courier certificate and/or mission order recognised by all EU States authorising him to carry the package as identified;

    (e) no EU non-Member State or its frontier is crossed when travelling overland unless the shipping State has a specific guarantee from that State;

    (f) the bearer's travel arrangements with regard to destinations, routes to be taken and means of transportation to be used will be in accordance with EU Regulations or — if national regulations with respect to such matters are more stringent — in accordance with such regulations;

    (g) the material must not leave the possession of the bearer unless it is housed in accordance with the provisions for safe custody contained in Section IV;

    (h) the material must not be left unattended in public or private vehicles, or in places such as restaurants or hotels. It must not be stored in hotel safes or left unattended in hotel rooms;

    (i) if the material being carried contains documents, these must not be read in public places (for example in aircraft, trains, etc.).

    The person designated to carry the classified material must read and sign a security briefing that contains, as a minimum, the instructions listed above and procedures to be followed in an emergency or in case the package containing the classified material is challenged by customs or airport security officials.

TRANSMISSION OF RESTREINT UE DOCUMENTS

21. No special provisions are laid down for the conveyance of RESTREINT UE documents, except that they should be such as to ensure that they cannot fall into any unauthorised person's hands.

COURIER PERSONNEL SECURITY

22. All couriers and messengers employed to carry SECRET UE and CONFIDENTIEL UE documents shall be appropriately security cleared.

Chapter III

Electrical and other means of technical transmission

23. Communications security measures are designed to ensure the secure transmission of EU classified information. The detailed rules applicable to the transmission of such EU classified information are dealt with in Section XI.

24. Only accredited communications centres and networks and/or terminals and systems may transmit information classified CONFIDENTIEL UE and SECRET UE.

Chapter IV

Extra copies and translations of and extracts from EU classified documents

25. Only the originator may authorise the copy or translation of TRÈS SECRET UE/EU TOP SECRET documents.

▼B

26. If persons without TRÈS SECRET UE/EU TOP SECRET clearance require information which, although contained in a TRÈS SECRET UE/EU TOP SECRET document, does not have that classification, the Head of the TRÈS SECRET UE/EU TOP SECRET Registry may be authorised to produce the necessary number of extracts from that document. He/she shall, at the same time, take the necessary steps to ensure that these extracts are given the appropriate security classification.

27. Documents classified SECRET UE and lower may be reproduced and translated by the addressee, within the framework of the national security regulations and on condition that it complies strictly with the need-to-know principle. The security measures applicable to the original document shall also be applicable to reproductions and/or translations thereof. EU decentralised agencies shall follow these security regulations.

Chapter V

Musters and checks, storage and destruction of EU classified documents

MUSTERS AND CHECKS

28. Every year, each TRÈS SECRET UE/EU TOP SECRET Registry as referred to in Section VIII shall carry out an itemised muster of TRÈS SECRET UE/EU TOP SECRET documents in accordance with the regulations set out in Section VIII, (9) to (11). EU classified documents below the level of TRÈS SECRET UE/EU TOP SECRET shall be subject to internal checks in accordance with national guidelines, and, in the case of the GSC or EU decentralised agencies, according to instructions from the Secretary General/High Representative.

    These operations shall afford the opportunity to secure holders' views as to:

    (a) the possibility of downgrading or declassifying certain documents;

    (b) documents to be destroyed.

ARCHIVE STORAGE OF EU CLASSIFIED INFORMATION

29. To minimise storage problems, the control officers of all registries shall be authorised to have TRÈS SECRET UE/EU TOP SECRET, SECRET UE and CONFIDENTIEL UE documents microfilmed or otherwise stored in magnetic or optical media for archive purposes, providing that:

    (a) the microfilming/storage process is undertaken by personnel with current clearance for the corresponding appropriate classification level;

    (b) the microfilm/storage medium is afforded the same security as the original documents;

    (c) the microfilming/storing of any TRÈS SECRET UE/EU TOP SECRET document is reported to the originator;

    (d) rolls of film, or other type of support, contain only documents of the same TRÈS SECRET UE/EU TOP SECRET, SECRET UE or CONFIDENTIEL UE classification;

    (e) the microfilming/storing of a TRÈS SECRET UE/EU TOP SECRET or SECRET UE document is clearly indicated in the record used for the annual inventory;

    (f) original documents which have been microfilmed or otherwise stored are destroyed, in accordance with the regulations set out in paragraphs 31 to 36.

30. These rules also apply to any other form of storage authorised by the NSA, such as electromagnetic media and optical disk.

ROUTINE DESTRUCTION OF EU CLASSIFIED DOCUMENTS

31. To prevent the unnecessary accumulation of EU classified documents, those regarded by the Head of the establishment holding them as out of date and surplus in number shall be destroyed as soon as practicable, in the following manner:

    (a) TRÈS SECRET UE/EU TOP SECRET documents shall be destroyed only by the Central Registry responsible for them. Each document destroyed shall be listed in a destruction certificate, signed by the TRÈS SECRET UE/EU TOP SECRET control officer and by the

▼B

officer witnessing the destruction, who shall be TRÈS SECRET UE/EU TOP SECRET cleared. A note to this effect shall be made in the logbook;

(b) the registry shall keep the destruction certificates, together with the distribution sheets, for a period of ten years. Copies shall be forwarded to the originator or to the appropriate central registry only when explicitly requested;

(c) TRÈS SECRET UE/EU TOP SECRET documents, including all classified waste resulting from the preparation of TRÈS SECRET UE/EU TOP SECRET documents such as spoiled copies, working drafts, typed notes and carbon paper, shall be destroyed, under the supervision of a TRÈS SECRET UE/EU TOP SECRET officer, by burning, pulping, shredding or otherwise reducing into an unrecognisable and non-reconstitutable form.

32. SECRET UE documents shall be destroyed by the registry responsible for those documents, under the supervision of a security cleared person, using one of the processes indicated in paragraph 31(c). SECRET UE documents that are destroyed shall be listed on signed destruction certificates to be retained by the Registry, together with the distribution forms, for at least three years.

33. CONFIDENTIEL UE documents shall be destroyed by the registry responsible for those documents, under the supervision of a security cleared person, by one of the processes indicated in paragraph 31(c). Their destruction shall be recorded in accordance with national regulations and, in the case of GSC or EU decentralised agencies, according to instructions from the Secretary-General/High Representative.

34. RESTREINT UE documents shall be destroyed by the registry responsible for those documents or by the user, in accordance with national regulations and, in the case of GSC or EU decentralised agencies, according to instructions from the Secretary-General/High Representative.

DESTRUCTION IN EMERGENCIES

35. The GSC, the Member States and the EU decentralised agencies shall prepare plans based on local conditions for the safeguarding of EU classified material in a crisis including if necessary emergency destruction and evacuation plans; they shall promulgate, within their respective organisations, instructions deemed necessary to prevent EU classified information from falling into unauthorised hands.

36. The arrangements for the safeguarding and/or destruction of SECRET UE and CONFIDENTIEL UE material in a crisis shall under no circumstances adversely affect the safeguarding or destruction of TRÈS SECRET UE/EU TOP SECRET material, including the enciphering equipment, whose treatment shall take priority over all other tasks. The measures to be adopted for the safeguarding and destruction of enciphering equipment in an emergency shall be covered by ad hoc instructions.

CHAPTER VI

Specific rules applicable to documents intended for the Council

37. Within the GSC, a 'Classified Information Office' shall monitor information classified as SECRET UE or CONFIDENTIEL UE contained in documents for the Council.

Under the authority of the Director-General for Personnel and Administration it shall:

(a) manage operations relating to the registration, reproduction, translation, transmission dispatch and destruction of such information;

(b) update the list of particulars on classified information;

(c) periodically question issues on the need to maintain the classification of information;

(d) lay down, in collaboration with the Security Office, the practical arrangements for classifying and declassifying information.

38. The Classified Information Office shall keep a register of the following particulars:

▼B

(a) the date of preparation of the classified information;

(b) the level of classification;

(c) the expiry date of the classification;

(d) the name and department of the issuer;

(e) the recipient or recipients, with serial number;

(f) the subject;

(g) the number;

(h) the number of copies circulated;

(i) the preparation of inventories of the classified information submitted to the Council;

(j) the register of declassification and downgrading of classified information.

39. The general rules provided for in Chapters I to V of this Section shall apply to the Classified Information Office of the GSC, unless modified by the specific rules laid down in this Chapter.

▼B

SECTION VIII

TRÈS SECRET UE/EU TOP SECRET REGISTRIES

1. The purpose of TRÈS SECRET UE/EU TOP SECRET registries is to ensure the recording, handling and distribution of TRÈS SECRET UE/EU TOP SECRET documents in accordance with security regulations. The head of the TRÈS SECRET UE/EU TOP SECRET registry, respectively in each Member State, in the GSC and, as appropriate in EU decentralised agencies, will be the TRÈS SECRET UE/EU TOP SECRET control officer.

2. Central registries will act as the main receiving and despatching authority in Member States, in the GSC and EU decentralised agencies, in which such registries have been set up, as well as, if appropriate, in other EU institutions, international organisations and third States with which the Council has agreements on security procedures for the exchange of classified information.

3. When necessary, subregistries shall be established, to be responsible for the internal management of TRÈS SECRET UE/EU TOP SECRET documents; they shall keep up-to-date records of the circulation of each document held on the Subregistry's charge.

4. TRÈS SECRET UE/EU TOP SECRET sub-registries shall be set up as specified in Section I in response to long term needs and shall be attached to a central TRÈS SECRET UE/EU TOP SECRET registry. If there is a need to consult TRÈS SECRET UE/EU TOP SECRET documents only temporarily and occasionally, these documents may be released without setting up a TRÈS SECRET UE/EU TOP SECRET subregistry provided rules are laid down to ensure that they remain under the control of the appropriate TRÈS SECRET UE/EU TOP SECRET registry and that all physical and personnel security measures are observed.

5. Subregistries may not transmit TRÈS SECRET UE/EU TOP SECRET documents direct to other subregistries of the same central TRÈS SECRET UE/EU TOP SECRET registry without express approval by the latter.

6. All exchanges of TRÈS SECRET UE/EU TOP SECRET documents between subregistries not attached to the same central registry shall be routed through the central TRÈS SECRET UE/EU TOP SECRET registries.

CENTRAL TRÈS SECRET UE/EU TOP SECRET REGISTRIES

7. As the control officer, the head of a central TRÈS SECRET UE/EU TOP SECRET registry shall be responsible for:

   (a) the transmission of TRÈS SECRET UE/EU TOP SECRET documents in accordance with the regulations defined in Section VII;

   (b) maintaining a list of all its dependent TRÈS SECRET UE/EU TOP SECRET sub-registries together with names and signatures of the appointed control officers and their authorised deputies;

   (c) holding receipts from registries for all TRÈS SECRET UE/EU TOP SECRET documents distributed by the central registry;

   (d) maintaining a record of TRÈS SECRET UE/EU TOP SECRET documents held and distributed;

   (e) maintaining an up-to-date list of all central TRÈS SECRET UE/EU TOP SECRET registries with which he/she normally corresponds, together with the names and signatures of their appointed control officers and their authorised deputies;

   (f) the physical safeguarding of all TRÈS SECRET UE/EU TOP SECRET documents held within the registry in accordance with regulations contained in Section IV.

TRÈS SECRET UE/EU TOP SECRET SUBREGISTRIES

8. As the control officer, the head of a TRÈS SECRET UE/EU TOP SECRET subregistry shall be responsible for:

   (a) the transmission of TRÈS SECRET UE/EU TOP SECRET documents in accordance with regulations contained in Section VII and paragraphs 5 and 6 of Section VIII;

▼B

(b) maintaining an up-to-date list of all persons authorised to have access to the TRÈS SECRET UE/EU TOP SECRET information under his control;

(c) the distribution of TRÈS SECRET UE/EU TOP SECRET documents in accordance with the instructions of the originator or on a need-to-know basis, having first checked that the addressee has the requisite security clearance;

(d) maintaining an up-to-date record of all TRÈS SECRET UE/EU TOP SECRET documents held or circulating under his control or which have been passed to other TRÈS SECRET UE/EU TOP SECRET registries and holding all corresponding receipts;

(e) maintaining an up-to-date list of TRÈS SECRET UE/EU TOP SECRET registries with whom he is authorised to exchange TRÈS SECRET UE/EU TOP SECRET documents, together with the names and signatures of their control officers and authorised deputies;

(f) the physical safeguarding of all TRÈS SECRET UE/EU TOP SECRET documents held within the subregistry in accordance with the regulations laid down in Section IV.

INVENTORIES

9. Every twelve months, each TRÈS SECRET UE/EU TOP SECRET registry shall carry out an itemised inventory of all TRÈS SECRET UE/EU TOP SECRET documents for which it is accountable. A document is deemed to have been accounted for if the registry physically musters the document, or holds a receipt from the TRÈS SECRET UE/EU TOP SECRET registry to which the document has been transferred, a destruction certificate for the document or an instruction to downgrade or declassify that document.

10. Subregistries shall forward the findings of their annual inventory to the central registry to which they are answerable, on a date specified by the latter.

11. NSAs, as well as those EU institutions, international organisations and EU decentralised agencies in which a central TRÈS SECRET UE/EU TOP SECRET registry has been set up, shall forward the findings of the annual inventories conducted in central TRÈS SECRET UE/EU TOP SECRET registries to the Secretary-General/High Representative, by 1 April each year at the latest.

▼B

SECTION IX

SECURITY MEASURES TO BE APPLIED AT THE TIME OF SPECIFIC MEETINGS HELD OUTSIDE THE COUNCIL PREMISES AND INVOLVING HIGH SENSITIVITY ISSUES

GENERAL

1. When European Council, Council, Ministerial or other important meetings are held outside the Council premises in Brussels and Luxembourg, and where justified by the particular security requirements relating to the high sensitivity of the issues or information dealt with, the security measures described below should be taken. These measures concern only the protection of EU classified information; other security measures may have to be planned.

RESPONSIBILITIES

Host Member States

2. The Member State on whose territory the meeting is being held (the host Member State) should be responsible, in cooperation with the GSC security office, for the security of the European Council, Council, Ministerial or other important meetings and for the physical security of the principal delegates and their staff.

   As regards the protection of security, it should specifically ensure that:

   (a) plans are drawn up to deal with security threats and security-related incidents, the measures in question covering in particular the safe custody of EU classified documents in offices;

   (b) measures are taken to provide possible access to Council's communications system for the receipt and transmission of EU classified messages. The host Member State will also provide access if required to secure telephone systems.

Member States

3. The Member States' authorities should take the necessary steps to ensure that:

   (a) appropriate security clearance certification is provided for their national delegates, if necessary by signal or fax, either directly to the meeting security officer or via the GSC Security Office;

   (b) any specific threat is made known to the host Member State's authorities and, as appropriate, to the GSC Security Office so that appropriate action can be taken.

Meeting Security Officer

4. A security officer should be appointed and be responsible for the general preparation and control of general internal security measures and for coordination with the other security authorities concerned. The measures taken by him/her should in general relate to:

   (a) (i) protective measures at the meeting place to ensure that the meeting is conducted without any incident that might compromise the security of any EU classified information that may be used there;

   (ii) checking the personnel whose access to the place of the meeting, delegations' areas and conference rooms is permitted, and checking any equipment;

   (iii) constant coordination with the competent authorities of the host Member State and with the GSC Security Office.

   (b) the inclusion of security instructions in the meeting dossier with due regard for the requirements set out in these security regulations and any other security instructions considered necessary.

GSC Security Office

5. The GSC Security Office should act as an adviser on security for the preparation of the meeting; it should be represented there to help and advise the meeting security officer and delegations as necessary.

▼B

6. Each delegation to a meeting should designate a security officer, who will be responsible for dealing with security matters within his/her delegation and for maintaining liaison with the meeting security officer, as well as with the GSC Security Office representative as required.

SECURITY MEASURES

Security areas

7. The following security areas should be established:

   (a) a Class II security area, consisting of a drafting room, the GSC offices and reprographic equipment, as well as delegations' offices as appropriate;

   (b) a Class I security area, consisting of the conference room and interpreters' and sound engineers' booths;

   (c) administrative areas, consisting of the press area and those parts of the meeting place that are used for administration, catering and accommodation, as well as the area immediately adjacent to the Press Centre and the meeting place.

Passes

8. The meeting security officer should issue appropriate badges as requested by the delegations, according to their needs. Where required, a distinction may be made as regards access to different security areas.

9. The security instructions for the meeting should require all persons concerned to wear and display their badges prominently at all times within the place of the meeting, so that they can be checked as needed by security personnel.

10. Apart from badge-holding participants, as few people as possible should be admitted to the meeting place. National delegations wishing to receive visitors during the meeting should notify the meeting security officer. Visitors should be given a visitor's badge. A visitor's pass form bearing his/her name and the name of the person being visited should be filled in. Visitors should be accompanied at all times by a security guard or by the person being visited. The visitor's pass form should be carried by the accompanying person, who shall return it, together with the visitor's badge, to the security personnel when the visitor leaves the meeting place.

Control of photographic and audio equipment

11. No camera or recording equipment may be brought into a Class I security area, with the exception of equipment brought by photographers and by sound engineers duly authorised by the meeting security officer.

Checking of briefcases, portable computers and packages

12. Pass-holders allowed access to a security area may normally bring in their briefcases and portable computers (with own power supply only) without a check being made. In the case of packages for delegations, delegations may take delivery of the packages, which will either be inspected by the delegation security officer, screened by special equipment or opened by security personnel for inspection. If the meeting security officer considers it necessary, more stringent measures for the inspection of briefcases and packages may be laid down.

Technical security

13. The meeting room may be made technically secure by a technical security team, which may also conduct electronic surveillance during the meeting.

Delegations' documents

14. Delegations should be responsible for taking EU classified documents to and from meetings. They should also be responsible for the verification and security of those documents during their use in the premises assigned to them. The host Member States' help may be requested for the transportation of classified documents to and from the place of the meeting.

Safe custody of documents

15. If the GSC, the Commission or delegations are unable to store their classified documents in accordance with approved standards, they may lodge those documents in a sealed envelope with the meeting security officer, against

▼B

receipt, so that the latter can store the documents in accordance with approved standards.

Inspection of offices

16. The meeting security officer should arrange for the GSC and delegations' offices to be inspected at the end of each working day to ensure that all EU classified documents are being kept in a safe place; if not, he should take the requisite measures.

Disposal of EU classified waste

17. All waste should be treated as EU classified, and waste-paper baskets or bags should be given to the GSC and delegations for its disposal. Before leaving the premises they have been assigned, the GSC and delegations should take their waste to the meeting security officer, who should arrange for its destruction according to the regulations.

18. At the end of the meeting, all documents held but no longer wanted by the GSC or delegations should be treated as waste. A thorough search of GSC and delegations' premises should be made before the security measures adopted for the meeting are lifted. Documents for which a receipt was signed should, as far as applicable, be destroyed as prescribed in Section VII.

▼B

SECTION X

BREACHES OF SECURITY AND COMPROMISE OF EU CLASSIFIED INFORMATION

1. A breach of security occurs as the result of an act or omission contrary to a Council or national security regulation which might endanger or compromise EU classified information.

2. Compromise of EU classified information occurs when it has wholly or in part fallen into the hands of unauthorised persons, i.e. who do not have either the appropriate security clearance or the necessary need-to-know or if there is the likelihood of such an event having occurred.

3. EU classified information may be compromised as a result of carelessness, negligence or indiscretion as well as by the activities of services which target the EU or its Member States, as regards EU classified information and activities, or by subversive organisations.

4. It is important that all persons who are required to handle EU classified information are thoroughly briefed on security procedures, the dangers of indiscreet conversation and their relationships with the press. They should be aware of the importance of reporting any breach of security which may come to their notice at once to the security authority of the Member State, Institution or Agency in which they are employed.

5. When a security authority discovers or is informed of a breach of security relating to EU classified information or of the loss or disappearance of EU classified material, it shall take timely action in order to:

   (a) establish the facts;

   (b) assess and minimise the damage done;

   (c) prevent a recurrence;

   (d) notify the appropriate authorities of the effects of the breach of security.

   In this context, the following information shall be provided:

   (i) a description of the information involved, including its classification, reference and copy number, date, originator, subject and scope;

   (ii) 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;

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

6. It shall be the duty of each security authority, as soon as it is notified that such a breach of security may have occurred, to report the fact immediately, using the following procedure: the EU TOP SECRET sub-registry shall report the matter to the GSC Security Office via its central EU TOP SECRET registry; in the event of a compromise of EU classified information occurring within the jurisdiction of a Member State, it shall be reported to the GSC Security Office as specified in paragraph 5, through the NSA responsible.

7. Cases involving RESTREINT UE information need to be reported only when they present unusual features.

8. On being informed that a breach of security has occurred, the Secretary-General/High Representative 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, with a detailed description of the content and classification of the material involved. Damage done to the interests of the EU or of one or more of its Member States and action taken to prevent a recurrence should also be reported.

9. The originating authority shall inform the addressees and shall give appropriate instructions.

▼B

10. Any individual who is responsible for compromising EU classified information shall be liable to disciplinary action according to the relevant rules and regulations. Such action shall be without prejudice to any legal action.

▼B

SECTION XI

PROTECTION OF INFORMATION HANDLED IN INFORMATION TECHNOLOGY AND COMMUNICATION SYSTEMS

Contents

Chapter I	Introduction…
Chapter II	Definitions…
Chapter III	Security responsibilities…
Chapter IV	Non-technical security measures…
Chapter V	Technical security measures…
Chapter VI	Security during handling…
Chapter VII	Procurement…
Chapter VIII	Temporary or occasional use…

▼B

Chapter I

Introduction

GENERAL ASPECTS

1. The security policy and requirements in this section shall apply to all communications and information systems and networks (hereinafter SYSTEMS) handling information classified CONFIDENTIEL UE and above.

2. SYSTEMS handling RESTREINT UE information also require security measures to protect the confidentiality of that information. All SYSTEMS require security measures to protect the integrity and availability of those systems and of the information they contain. The security measures to be applied to those systems will be determined by the designated Security Accreditation Authority (SAA) and will be commensurate with the assessed risk and consistent with the policy stated in these security regulations.

3. Protection of sensor systems containing embedded IT SYSTEMS shall be determined and specified in the general context of the systems to which they belong using applicable provisions of this section to the extent possible.

THREATS TO, AND VULNERABILITIES OF SYSTEMS

4. In general terms, a threat can be defined as a potential for the accidental or deliberate compromise of security. In the case of SYSTEMS, such a compromise involves loss of one or more of the properties of confidentiality, of integrity and of availability. A vulnerability can be defined as a weakness or lack of controls that would facilitate or allow a threat actuation against a specific asset or target. A vulnerability may be an omission or it may relate to a deficiency in a control's strength, completeness or consistency; it may be technical, procedural or operational in nature.

5. EU classified and unclassified information handled in SYSTEMS in a concentrated form designed for rapid retrieval, communication and use is vulnerable to many risks. These include access to the information by unauthorised users or, conversely, denial of access to authorised users. There are also the risks of the unauthorised disclosure, corruption, modification or deletion of the information. Furthermore, the complex and sometimes fragile equipment is expensive and often difficult to repair or replace rapidly. These SYSTEMS are therefore attractive targets for intelligence gathering operations and sabotage, especially if security measures are thought to be ineffective.

SECURITY MEASURES

6. The main purpose of the security measures stated in this section is to provide protection against unauthorised disclosure of information (the loss of confidentiality) and against the loss of integrity and availability of information. To achieve adequate security protection of a SYSTEM handling EU classified information, the appropriate standards of conventional security shall be specified, along with appropriate special security procedures and techniques particularly designed for each SYSTEM.

7. A balanced set of security measures shall be identified and implemented to create a secure environment in which a SYSTEM operates. The fields of application of those measures concern physical elements, personnel, non-technical procedures, computer and communications operating procedures.

8. Computer security measures (hardware and software security features) shall be required to implement the need-to-know principle, and to prevent or detect the unauthorised disclosure of information. The extent to which computer security measures are to be relied upon shall be determined during the process of establishing the security requirement. The process of accreditation shall determine that an adequate level of assurance is present to support this reliance on computer security measures.

▼B

SYSTEM-SPECIFIC SECURITY REQUIREMENT STATEMENT (SSRS)

9. For all SYSTEMS handling information classified CONFIDENTIEL UE and above, a SYSTEM-Specific Security Requirement Statement (SSRS) shall be required to be produced by the IT System Operational Authority (ITSOA) in cooperation with input and assistance as required from the project staff and INFOSEC Authority, and approved by the SAA. An SSRS shall also be required where the availability and integrity of the RESTREINT UE or unclassified information is deemed critical by the SAA.

10. The SSRS shall be formulated at the earliest stage of a project's inception and shall be developed and enhanced as the project develops, fulfilling different roles at different stages in the project and SYSTEM's life cycle.

11. The SSRS shall form the binding agreement between the IT System Operational Authority and the SAA against which the SYSTEM is to be accredited.

12. The SSRS is a complete and explicit statement of the security principles to be observed and of the detailed security requirements to be met. It is based on Council security policy and risk assessment, or imposed by parameters covering the operational environment, the lowest level of personnel security clearance, the highest classification of information handled, the security mode of operation or user requirements. The SSRS is an integral part of project documentation submitted to the appropriate authorities for technical, budgetary and security approval purposes. In its final form, the SSRS constitutes a complete statement of what it means for the SYSTEM to be secure.

SECURITY MODES OF OPERATION

13. All SYSTEMS handling information classified CONFIDENTIEL UE and above shall be accredited to operate in one, or where warranted by requirements during different time periods, more than one, of the following security modes of operation, or their national equivalent:

    (a) dedicated;

    (b) system high; and

    (c) multi-level.

Chapter II

Definitions

ADDITIONAL MARKINGS

14. Additional markings such as CRYPTO or any other EU-recognised special handling designator, shall apply where there is a need for limited distribution and special handling in addition to that designated by the security classification.

15. 'DEDICATED' SECURITY MODE OF OPERATION shall mean: a mode of operation in which ALL individuals with access to the SYSTEM are cleared to the highest classification level of information handled within the SYSTEM, and with a common need-to-know for ALL of the information handled within the SYSTEM.

    Notes:

    (1) The common need-to-know indicates there is no mandatory requirement for computer security features to provide separation of information within the SYSTEM.

    (2) Other security features (for example, physical, personnel and procedural) shall conform to the requirements for the highest classification level and all category designations of the information handled within the SYSTEM.

16. 'SYSTEM HIGH' SECURITY MODE OF OPERATION shall mean: a mode of operation in which ALL individuals with access to the SYSTEM are cleared to the highest classification level of information handled within the SYSTEM, but NOT ALL individuals with access to the SYSTEM have a common need-to-know for the information handled within the SYSTEM.

▼B

Notes:

(1) The lack of common need-to-know indicates that there is a requirement for computer security features to provide selective access to, and separation of, information within the SYSTEM.

(2) Other security features (for example, physical, personnel and procedural) shall conform to the requirements for the highest classification level and all category designations of the information handled within the SYSTEM.

(3) All information handled or being available to a SYSTEM under this mode of operation, together with output generated, shall be protected as potentially of the information category designation and of the highest classification level being handled until determined otherwise, unless there is an acceptable level of trust that can be placed in any labelling functionality present.

17. 'MULTI-LEVEL' SECURITY MODE OF OPERATION shall mean: a mode of operation in which NOT ALL individuals with access to the SYSTEM are cleared to the highest classification level of information handled within the SYSTEM, and NOT ALL individuals with access to the SYSTEM have a common need-to-know for the information handled within the SYSTEM.

Notes:

(1) This mode of operation permits, currently, the handling of information of different classification levels and of mixed information category designations.

(2) The fact that not all individuals are cleared to the highest levels, associated with a lack of common need-to-know, indicates that there is a requirement for computer security features to provide elective access to, and separation of, information within the SYSTEM.

18. INFOSEC shall mean: the application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems against loss of confidentiality, integrity or availability, whether accidental or intentional, and to prevent loss of integrity and availability of the systems themselves. INFOSEC measures include those of computer, transmission, emission and cryptographic security, and the detection, documentation and countering of threats to information and to the SYSTEMS.

19. COMPUTER SECURITY (COMPUSEC) shall mean: the application of hardware, firmware and software security features to a computer system in order to protect against, or prevent, the unauthorised disclosure, manipulation, modification/deletion of information or denial of service.

20. COMPUTER SECURITY PRODUCT shall mean: a generic computer security item which is intended for incorporation into an IT system for use in enhancing, or providing for, confidentiality, integrity or availability of information handled.

21. COMMUNICATIONS SECURITY (COMSEC) shall mean: the application of security measures to telecommunications in order to deny unauthorised persons information of value which might be derived from the possession and study of such telecommunications or to ensure the authenticity of such telecommunications.

Note:

Such measures include cryptographic, transmission and emission security; and also include procedural, physical, personnel, document and computer security.

22. EVALUATION shall mean: the detailed technical examination, by an appropriate authority, of the security aspects of a SYSTEM or of a cryptographic or a computer security product.

Notes:

(1) The evaluation investigates the presence of required security functionality and the absence of compromising side-effects from such functionality and assesses the incorruptibility of such functionality.

(2) The evaluation determines the extent to which the security requirements of a SYSTEM, or the security claims of a computer security product, are

▼B

satisfied and establishes the assurance level of the SYSTEM or of the cryptographic, or the computer security product's trusted function.

23. CERTIFICATION shall mean: the issue of a formal statement, supported by an independent review of the conduct and results of an evaluation, of the extent to which a SYSTEM meets the security requirement, or a computer security product meets pre-defined security claims.

24. ACCREDITATION shall mean: the authorisation and approval granted to a SYSTEM to process EU classified information in its operational environment.

Note:

Such accreditation should be made after all appropriate security procedures have been implemented and a sufficient level of protection of the system resources has been achieved. Accreditation should normally be made on the basis of the SSRS, including the following:

(a) a statement of the objective of accreditation for the system; in particular, what classification level(s) of information are to be handled and what system or network security mode(s) of operation is being proposed;

(b) production of a risk management review to identify the threats and vulnerabilities and measures to counter them;

(c) the Security Operating Procedures (SecOPs) with a detailed description of the proposed operations (e.g., modes, services, to be provided) and including a description of the SYSTEM security features which shall form the basis of accreditation;

(d) the plan for the implementation and maintenance of the security features;

(e) the plan for initial and follow-on system security or network security test, evaluation and certification; and

(f) certification, where required, together with other elements of accreditation.

25. IT SYSTEM shall mean: assembly of equipment, methods and procedures, and if necessary, personnel, organised to accomplish information processing functions.

Notes:

(1) This is taken to mean an assembly of facilities, configured for handling information within the system.

(2) Such systems may be in support of consultation, command, control, communications, scientific or administrative applications including word processing.

(3) The boundaries of a system will generally be determined as being the elements under the control of a single ITSOA.

(4) An IT system may contain subsystems some of which are themselves IT systems.

26. IT SYSTEM SECURITY FEATURES comprise all hardware/firmware/software functions, characteristics, and features; operating procedures, accountability procedures, and access controls, the IT area, remote terminal/workstation area, and the management constraints, physical structure and devices, personnel and communications controls needed to provide an acceptable level of protection for classified information to be handled in an IT system.

27. IT NETWORK shall mean: organisation, geographically disseminated, of IT systems interconnected to exchange data, and comprising the components of the interconnected IT systems and their interface with the supporting data or communications networks.

Notes:

(1) An IT network can use the services of one or several communications networks interconnected to exchange data; several IT networks can use the services of a common communications network.

(2) An IT network is called ‘local’ if it links several computers together in the same site.

▼B

28. IT NETWORK SECURITY FEATURES include the IT system security features of individual IT systems comprising the network together with those additional components and features associated with the network as such (for example, network communications, security identification and labelling mechanisms and procedures, access controls, programs and audit trails) needed to provide an acceptable level of protection for classified information.

29. IT AREA shall mean: an area which contains one or more computers, their local peripheral and storage units, control units and dedicated network and communications equipment.

    Note:

    This does not include a separate area in which remote peripheral devices or terminals/workstations are located even though those devices are connected to equipment in the IT area.

30. REMOTE TERMINAL/WORKSTATION AREA shall mean: an area containing some computer equipment, its local peripheral devices or terminals/workstations and any associated communications equipment, separate from an IT area.

31. TEMPEST countermeasures: security measures intended to protect equipment and communication infrastructures against the compromise of classified information through unintentional electromagnetic emissions.

Chapter III

Security responsibilities

GENERALITIES

32. The responsibilities of the Security Committee, defined in Section I, paragraph 4 include INFOSEC issues. The Security Committee shall organise its activities in such a way that it can provide expert advice on the above issues.

33. In case of problems regarding security (incidents, breaches, etc.), immediate action shall be taken by the responsible National Authority and/or the GSC Security Office. All problems shall be referred to the GSC Security Office

34. The Secretary-General/High Representative or, where appropriate, the Head of an EU decentralised agency, shall establish an INFOSEC Office to provide guidance to the security authority on the implementation and control of special security features designed as part of SYSTEMS.

SECURITY ACCREDITATION AUTHORITY (SAA)

35. The SAA shall be either:

    — an NSA,

    — the Authority designated by the Secretary-General/High Representative,

    — the security authority of a EU decentralised agency, or

    — their delegated/nominated representatives, depending on the SYSTEM to be accredited.

36. The SAA shall be responsible for ensuring the compliance of SYSTEMS with the Council's security policy. One of its tasks shall be to grant the approval of a SYSTEM to handle EU classified information to a defined level of classification in its operational environment. As regards the GSC and, as appropriate EU decentralised agencies, the SAA shall exercise responsibility for security on behalf of the Secretary-General/High Representative or of the Heads of decentralised agencies.

    The jurisdiction of the GSC SAA shall cover all the SYSTEMS that are in operation within the premises of the GSC. SYSTEMS and components of SYSTEMS in operation within a Member State shall remain under the jurisdiction of that Member State. When different components of a SYSTEM come under the jurisdiction of the GSC SAA and others SAAs, all the parties will appoint a joint accreditation board under the coordination of the GSC SAA.

▼B

INFOSEC AUTHORITY (IA)

37. The INFOSEC Authority is responsible for the INFOSEC office activities. As regards the GSC and, as appropriate, EU decentralised agencies, the INFOSEC Authority is responsible for:

— providing technical advice and assistance to the SAA,

— assisting in the development of the SSRS,

— reviewing the SSRS to ensure consistency with these security regulations and the INFOSEC policies and architecture documents,

— participating in the accreditation panels/boards as required and providing INFOSEC recommendation on accreditation to the SAA,

— providing support to the INFOSEC training and education activities,

— providing technical advice in investigation of INFOSEC related incidents,

— establishing technical policy guidance to ensure that only authorised software is used.

IT SYSTEM OPERATIONAL AUTHORITY (ITSOA)

38. The INFOSEC Authority shall delegate at the earliest stage possible the responsibility for the implementation and operation of controls and special security features of the SYSTEM to the ITSOA. This responsibility shall extend throughout the life cycle of the SYSTEM from the project concept stage to final disposal.

39. The ITSOA shall be responsible for all security measures designed as part of the overall SYSTEM. This responsibility includes the preparation of the SecOPs. The ITSOA shall specify the security standards and practices to be met by the supplier of the SYSTEM.

40. The ITSOA may delegate a part of its responsibilities where appropriate to, for instance the INFOSEC security officer and the INFOSEC site security officer. The various INFOSEC functions may be performed by a single person.

USERS

41. All users shall be responsible for ensuring that their actions do not adversely affect the security of the SYSTEM that they are using.

INFOSEC TRAINING

42. INFOSEC education and training shall be available at various levels, and for various personnel, as appropriate, within the GSC, EU decentralised Agencies or Member State government departments.

Chapter IV

Non-technical security measures

PERSONNEL SECURITY

43. Users of the SYSTEM shall be cleared and have a need-to-know, as appropriate for the classification and content of the information handled within their particular SYSTEM. Access to certain equipment or information specific to security of SYSTEMS will call for special clearance issued according to Council procedures.

44. The SAA shall designate all sensitive positions and specify the level of clearance and supervision required by all personnel occupying them.

45. SYSTEMS shall be specified and designed in a way that facilitates the allocation of duties and responsibilities to personnel so as to prevent one person having complete knowledge or control of the system security keys points. The aim should be that collusion between two or more individuals would be necessary for alteration or intentional degradation of the system or network to take place.

▼B

PHYSICAL SECURITY

46. IT and remote terminal/workstation areas (as defined in paragraphs 29 and 30) in which information classified CONFIDENTIEL UE and above is handled by IT means, or where potential access to such information is possible, shall be established as EU Class I or Class II security areas or national equivalent, as appropriate.

47. IT and remote terminal/workstation areas in which the security of the SYSTEM can be modified shall not be occupied by only one authorised official/other servant.

CONTROL OF ACCESS TO A SYSTEM

48. All information and material which allow access control to a SYSTEM shall be protected under arrangements commensurate with the highest classification and the category designation of the information to which it may give access.

49. When no longer used for this purpose, the access control information and material shall be destroyed pursuant to paragraphs 61 to 63.

Chapter V

Technical security measures

SECURITY OF INFORMATION

50. It shall be incumbent upon the originator of the information to identify and classify all information-bearing documents, whether they be in the form of hard-copy output or computer storage media. Each page of hard-copy output shall be marked, at the top and bottom, with the classification. Output, whether it is the form of hard-copy or computer storage media shall have the same classification as the highest classification of the information used for its production. The way in which a SYSTEM is operated may also impact on the classification of outputs of that system.

51. It shall be incumbent upon an organisation and its information holders to consider the problems of aggregation of individual elements of information, and the inferences that can be gained from the related elements, and determine whether or not a higher classification is appropriate to the totality of the information.

52. The fact that the information may be a brevity code, transmission code or in any form of binary representation does not provide any security protection and should not, therefore, influence the classification of the information.

53. When information is transferred from one SYSTEM to another the information shall be protected during transfer and in the receiving SYSTEM in the manner commensurate with the original classification and category of the information.

54. All computer storage media shall be handled in a manner commensurate with the highest classification of the stored information or the media label, and at all times shall be appropriately protected.

55. Reusable computer storage media used for recording EU classified information shall retain the highest classification for which they have ever been used until that information has been properly downgraded or declassified and the media reclassified accordingly, or the media declassified or destroyed by an approved GSC or national procedure (see paragraphs 61 to 63).

CONTROL AND ACCOUNTABILITY OF INFORMATION

56. Automatic (audit trails) or manual logs shall be kept as a record of access to information classified SECRET UE and above. These records shall be retained in accordance with these security regulations.

57. EU classified outputs held within the IT area may be handled as one classified item and need not be registered, provided the material is identified, marked with its classification and controlled in an appropriate manner.

58. Where output is generated from a SYSTEM handling EU classified information, and transmitted to a remote terminal/workstation area from an IT

▼B

area, procedures, agreed by the SAA shall be established for controlling the remote output. For SECRET UE and above, such procedures shall include specific instructions for accountability of the information.

HANDLING AND CONTROL OF REMOVABLE COMPUTER STORAGE MEDIA

59. All removable computer storage media classified CONFIDENTIEL UE and above shall be handled as material and general rules will apply. Appropriate identification and classification markings need to be adapted to the specific physical appearances of the media, to enable it to be clearly recognised.

60. Users shall take the responsibility for ensuring that EU classified information is stored on media with the appropriate classification marking and protection. Procedures shall be established to ensure that, for all levels of EU information, the storage of information on computer storage media is being carried out in accordance with these security regulations.

DECLASSIFICATION AND DESTRUCTION OF COMPUTER STORAGE MEDIA

61. Computer storage media used for recording EU classified information may be downgraded or declassified if approved GSC or national procedures are applied.

62. Computer storage media which has held TRÈS SECRET UE/EU TOP SECRET or special category information shall not be declassified and reused.

63. If computer storage media cannot be declassified or is not reusable, it shall be destroyed by an approved GSC or national procedure.

COMMUNICATIONS SECURITY

64. When EU classified information is transmitted electromagnetically, special measures shall be implemented to protect the confidentiality, integrity and availability of such transmissions. The SAA shall determine the requirements for protecting transmissions from detection and interception. The information being transmitted in a communication system shall be protected based upon the requirements for confidentiality, integrity and availability.

65. When cryptographic methods are required to provide confidentiality, integrity and availability protection such methods or associated products shall be specifically approved for the purpose by the SAA.

66. During transmission, the confidentiality of information classified SECRET UE and above shall be protected by cryptographic methods or products approved by the Council upon recommendation of the Council Security Committee. During transmission, the confidentiality of information classified CONFIDENTIEL UE or RESTREINT UE shall be protected by cryptographic methods or products approved either by the SG/HR upon recommendation of the Council Security Committee or by a Member State.

67. Detailed rules applicable to the transmission of EU classified information shall be set out in specific security instructions approved by the Council upon recommendation of the Council Security Committee.

68. Under exceptional operational circumstances, information classified RESTREINT UE, CONFIDENTIEL UE and SECRET UE may be transmitted in clear text provided each occasion is explicitly authorised. Such exceptional circumstances are as follows:

    (a) during impending or actual crisis, conflict, or war situations; and

    (b) when speed of delivery is of paramount importance, and means of encryption are not available, and it is assessed that the transmitted information cannot be exploited in time to adversely influence operations.

69. A SYSTEM shall have the capability of positively denying access to EU classified information at any or all of its remote workstations or terminals, when required either by physical disconnection or by special software features approved by the SAA.

▼B

INSTALLATION AND RADIATION SECURITY

70. Initial installation of SYSTEMS and any major change thereto shall be so specified that installation is carried out by security cleared installers under constant supervision by technically qualified personnel who are cleared for access to EU classified information to the level equivalent to the highest classification which the SYSTEM is expected to store and handle.

71. All equipment shall be installed in accordance with current Council's security policy.

72. SYSTEMS handling information classified CONFIDENTIEL UE and above shall be protected in such a way that their security cannot be threatened by compromising emanations, the study and control of which is referred to as 'TEMPEST'.

73. TEMPEST countermeasures for GSC and EU decentralised agencies installations shall be reviewed and approved by a TEMPEST authority designated by the GSC Security authority. For national installations which handle EU classified information, the approval authority shall be the recognised national TEMPEST approval authority.

Chapter VI

Security during handling

SECURITY OPERATING PROCEDURES

74. SecOPs define the principles to be adopted on security matters, the operating procedures to be followed, and personnel responsibilities. The SecOPs shall be prepared under the responsibility of the ITSOA.

SOFTWARE PROTECTION/CONFIGURATION MANAGEMENT

75. Security protection of applications programs shall be determined on the basis of an assessment of the security classification of the program itself rather than of the classification of the information it is to process. The software versions in use should be verified at regular intervals to ensure their integrity and correct functioning.

76. New or modified versions of software should not be used for the handling of EU classified information until verified by the ITSOA.

CHECKING FOR THE PRESENCE OF MALICIOUS SOFTWARE/ COMPUTER VIRUSES

77. Checking for the presence of malicious software/computer viruses shall be periodically carried out in accordance with the requirements of the SAA.

78. All computer storage media arriving in the GSC or EU decentralised agencies or in the Member States should be checked for the presence of any malicious software or computer viruses, before being introduced to any SYSTEM.

MAINTENANCE

79. Contracts and procedures for scheduled and on-call maintenance of SYSTEMS for which a SSRS has been produced shall specify requirements and arrangements for maintenance personnel and their associated equipment entering to an IT area.

80. The requirements shall be clearly stated in the SSRS and the procedures shall be clearly stated in the SecOPs. Contractor maintenance requiring remote access diagnostic procedures shall be permitted only in exceptional circumstances, under stringent security control, and only with the approval of the SAA.

▼B

Chapter VII

Procurement

81. Any security product to be used with the SYSTEM to be procured should either have been evaluated and certified, or currently be under evaluation and certification by an appropriate Evaluation or Certification body against internationally acknowledged criteria (such as the Common Criteria for Information Technology Security Evaluation, see ISO 15 408).

82. In deciding whether equipment, particularly computer storage media, should be leased rather than purchased, it should be borne in mind that such equipment, once used for handling EU classified information, cannot be released outside an appropriately secure environment without first being declassified to the approval of the SAA and that such approval may not always be possible.

ACCREDITATION

83. All SYSTEMS for which a SSRS has to be produced, prior to handling EU classified information, shall be accredited, based upon information provided in the SSRS, SecOPs and any other relevant documentation, by the SAA. Subsystems and remote terminals/workstations shall be accredited as part of all the SYSTEMS to which they are connected. Where a SYSTEM supports both Council and other organisations, the GSC and relevant Security Authorities shall mutually agree on the accreditation.

84. The accreditation process may be carried out in accordance with an accreditation strategy appropriate to the particular SYSTEM and defined by the SAA.

EVALUATION AND CERTIFICATION

85. Prior to accreditation, in certain instances, the hardware, firmware and software security features of a SYSTEM shall be evaluated and certified as being capable of safeguarding information at the intended level of classification.

86. The requirements for evaluation and certification shall be included in system planning, and clearly stated in the SSRS.

87. The evaluation and certification processes shall be carried out in accordance with approved guidelines and by technically qualified and appropriately cleared personnel acting on behalf of the ITSOA.

88. The teams may be provided from a nominated Member State's evaluation or certification authority or its nominated representatives, for example a competent and cleared contractor.

89. The degree of evaluation and certification processes involved may be lessened (for example, only involving integration aspects) where SYSTEMS are based on existing nationally evaluated and certified computer security products.

ROUTINE CHECKING OF SECURITY FEATURES FOR CONTINUED ACCREDITATION

90. The ITSOA shall establish routine control procedures which shall ensure that all security features of the SYSTEM are still valid.

91. The types of change that would give rise to re-accreditation, or that require the prior approval of the SAA, shall be clearly identified and stated in the SSRS. After any modification, repair or failure which could have affected the security features of the SYSTEM, the ITSOA shall ensure that a check is made to ensure the correct operation of the security features. Continued accreditation of the SYSTEM shall normally depend on the satisfactory completion of the checks.

92. All SYSTEMS where security features have been implemented shall be inspected or reviewed on a periodic basis by the SAA. In respect of SYSTEMS handling TRÈS SECRET UE/EU TOP SECRET or additional markings information the inspections shall be carried out not less than once annually.

▼B

Chapter VIII

Temporary or occasional use

SECURITY OF MICROCOMPUTERS/PERSONAL COMPUTERS

93. Microcomputers/Personal Computers (PCs) with fixed disks (or other non-volatile storage media), operating either in stand-alone mode or as networked configurations, and portable computing devices (for example, portable PCs and electronic 'notebooks') with fixed hard disks, shall be considered as information storage media in the same sense as floppy diskettes or other removable computer storage media.

94. These equipment shall be afforded the level of protection, in terms of access, handling, storage and transportation, commensurate with the highest classification level of information ever stored or processed (until downgraded or declassified in accordance with approved procedures).

USE OF PRIVATELY-OWNED IT EQUIPMENT FOR OFFICIAL COUNCIL WORK

95. The use of privately-owned removable computer storage media, software and IT hardware (for example, PCs and portable computing devices) with storage capability shall be prohibited for handling EU classified information.

96. Privately-owned hardware, software and media shall not be brought into any Class I or Class II area where EU classified information is handled without the permission of the Head of the Security Office of the GSC or of a Member State's Department or of the respective EU decentralised agency.

USE OF THE CONTRACTOR-OWNED OR NATIONALLY-SUPPLIED IT EQUIPMENT FOR OFFICIAL COUNCIL WORK

97. The use of contractor-owned IT equipment and software in organisations in support of official Council work may be permitted by the Head of the Security Office of the GSC or of a Member State's Department or of the respective EU decentralised agency. The use of nationally-provided IT equipment and software by employees in the GSC or a EU decentralised agency may also be permitted; in this case, the IT equipment shall be brought under the control of the appropriate GSC's inventory. In either case, if the IT equipment is to be used for handling EU classified information, then the appropriate SAA shall be consulted in order that the elements of INFOSEC that are applicable to the use of that equipment are properly considered and implemented.

▼B

SECTION XII

RELEASE OF EU CLASSIFIED INFORMATION TO THIRD STATES OR INTERNATIONAL ORGANISATIONS

PRINCIPLES REGULATING THE RELEASE OF EU CLASSIFIED INFORMATION

1. The release of EU classified information to third States or international organisations will be decided by the Council on the basis of:

   — the nature and content of such information,

   — the recipients' need to know,

   — the measure of advantages to EU.

   The Member State originator of the EU classified information to be released will be asked for its agreement.

2. These decisions will be taken on a case-by-case basis, depending on:

   — the desired degree of cooperation with the third States or international organisations concerned,

   — the confidence that may be placed in them, which ensues from the level of security that would be applied to the EU classified information entrusted to those States or organisations and from the consistency between the security rules applicable there and those applied in EU; the Council Security Committee will give the Council its technical opinion on this point.

3. The acceptance of EU classified information by third States or international organisations will imply an assurance that the information will be used for no purposes other than those motivating the release or exchange of information, and that they will provide the protection required by the Council.

LEVELS

4. Once the Council has decided that classified information may be released to or exchanged with a given State or international organisation, it will decide on the level of cooperation that is possible. This will depend in particular on the security policy and regulations applied by that State or organisation.

5. There are three levels of cooperation:

   Level 1

   Cooperation with third States or with international organisations whose security policy and regulations are very close to EU's.

   Level 2

   Cooperation with third States or with international organisations whose security policy and regulations are markedly different from EU's.

   Level 3

   Occasional cooperation with third States or with international organisations whose policy and security regulations cannot be assessed.

6. Each level of cooperation will determine the security regulations, reworded in individual cases in the light of the Council Security Committee's technical opinion, that the beneficiaries will be asked to apply to the protection of the classified information released to them. These procedures and security regulations are detailed in Appendices 4, 5 and 6.

THE AGREEMENTS

7. Once the Council has decided that there is a permanent or long-term need for the exchange of classified information between the EU and third States or other international organisations, it will draw up ‘agreements on security procedures for the exchange of classified information’ with them, defining the purpose of cooperation and the reciprocal rules on the protection of the information exchanged.

▼B

8. In the case of Level 3 occasional cooperation, which by definition is limited in time and purpose, a simple memorandum of understanding defining the nature of the classified information to be exchanged and the reciprocal obligations regarding that information may take the place of the 'agreement on procedures for the exchange of classified information' on condition that it is classified no higher than RESTREINT UE.

9. Draft agreements on security procedures or memoranda of understanding, will be approved by the Security Committee before they are presented to the Council for a decision.

10. NSAs will provide the Secretary-General/High Representative with all necessary assistance to ensure that the information to be released is used and protected in accordance with the provisions of the agreements on security procedures or memoranda of understanding.

▼M3

SECTION XIII

COMMON MINIMUM STANDARDS ON INDUSTRIAL SECURITY

1. This Section deals with security aspects of industrial activities that are unique to negotiating and awarding contracts entrusting tasks involving, entailing and/or containing EU classified information and to their performance by industrial or other entities, including the release of, or access to, EU classified information during the public procurement procedure (bidding period and pre-contract negotiations).

DEFINITIONS

2. For the purposes of these common minimum standards, the following definitions shall apply:

   (a) 'Classified contract': any contract to supply products, execute works or provide services, the performance of which requires or involves access to or generation of EU classified information;

   (b) '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 EU classified information;

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

   (d) 'Designated Security Authority (DSA)': an authority responsible to the National Security Authority (NSA) of an EU 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;

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

   (f) '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;

   (g) 'Industrial security': the application of protective measures and procedures to prevent, detect and recover from the loss or compromise of EU classified information handled by a contractor or subcontractor in pre-contract negotiations and contracts;

   (h) 'National Security Authority (NSA)': the Government Authority of an EU Member State with ultimate responsibility for the protection of EU classified information;

   (i) '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;

   (j) '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 EU classified information, that identifies the security requirements or those elements of the contract requiring security protection;

   (k) '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 must be part of the SAL.

▼M3

ORGANISATION

3. The General Secretariat of the Council (GSC) may entrust by contract tasks involving, entailing and/or containing EU classified information to industrial or other entities registered in a Member State.

4. The GSC shall ensure that all requirements deriving from these minimum standards are complied with when awarding classified contracts.

5. Each Member State shall ensure that its NSA has appropriate structures to apply these minimum standards on industrial security. These may include one or more DSA.

6. The ultimate responsibility for protecting EU classified information within industrial or other entities rests with their management.

7. Whenever a contract or a subcontract falling within the scope of these minimum standards is awarded, the GSC and/or the NSA/DSA, as appropriate, will promptly notify the NSA/DSA of the Member State in which the contractor or subcontractor is registered.

CLASSIFIED CONTRACTS

8. The security classification of classified contracts must take account of the following principles:

   (a) the GSC determines, as appropriate, the aspects of the contract which require protection and the consequent security classification; in doing so, it must 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) EU classified information generated under contractual activities is classified in accordance with the SCG;

   (d) when appropriate, the GSC is 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 must not be used for purposes other than those defined by the classified contract and must not be disclosed to third parties without the prior written consent of the originator.

9. The NSAs/DSAs of the Member States are responsible for ensuring that contractors and subcontractors awarded classified contracts which involve information classified CONFIDENTIEL UE or SECRET UE take all appropriate measures for safeguarding such EU classified information 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.

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

11. The NSA/DSA is responsible for granting, in accordance with its national regulations, a Personnel Security Clearance (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.

12. Classified contracts must include the SAL as defined in point 2(j). The SAL must contain the SCG.

13. Before initiating the negotiation of a classified contract the GSC will contact the NSA/DSA of the Member States in which the industrial or other entities concerned are registered in order to obtain confirmation that they hold a valid FSC appropriate to the level of security classification of the contract.

▼M3

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

15. Unless required by Member States national laws and regulations, an FSC is not required for contracts involving information classified RESTREINT UE.

16. In the case of bids in respect of classified contracts, invitations must 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.

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

18. The conditions under which the contractor may subcontract must 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.

19. Throughout the life of the contract, compliance with all its security provisions will be monitored by the relevant NSA/DSA in coordination with the GSC. Notification of security incidents shall be reported, in accordance with the provisions laid down in Part II, Section X of these Security Regulations. Change or withdrawal of an FSC shall immediately be communicated to the GSC and to any other NSA/DSA to which it has been notified.

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

21. The common minimum standards contained in this Section 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.

22. Specific provisions for the disposal of classified information at the end of the contract will be laid down in the SAL or in other relevant provisions identifying security requirements.

VISITS

23. Visits by personnel of the GSC to industrial or other entities in the Member States performing EU classified contracts must be arranged with the relevant NSA/DSA. Visits by employees of industrial or other entities within the framework of EU classified contract must be arranged between the NSAs/DSAs concerned. However, the NSAs/DSAs involved in a EU classified contract may agree on a procedure whereby the visits by employees of industrial or other entities can be arranged directly.

TRANSMISSION AND TRANSPORTATION OF EU CLASSIFIED INFORMATION

24. With regard to the transmission of EU classified information, the provisions of Part II, Section VII, Chapter II, and where relevant of Section XI, of these Security Regulations shall apply. In order to supplement such provisions, any existing procedures in force among Member States will apply.

25. The international transportation of EU classified material relating to classified contracts are carried out in accordance with Member States national procedures. The following principles will be applied when examining security arrangements for international transportation:

    (a) security is 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 is determined by the highest classification level of material contained within it;

    (c) an FSC is obtained, where appropriate, for companies providing transportation. In such cases, personnel handling the consignment shall be

▼M3

cleared in compliance with the common minimum standards contained in this Section;

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

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

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

▼M4

Appendix 1

List of national security authorities

BELGIUM

Nationale veiligheidsoverheid/
Autorité nationale de sécurité
FOD Buitenlandse Zaken, Buitenlandse Handel en Ontwikkelingssamenwerking/
SPF affaires étrangères, commerce extérieur et coopération au développement
Karmelietenstraat 15/Rue des Petits Carmes 15
B-1000 Brussel/B-1000 Bruxelles
Tel. secretariaat/secrétariat: (32-2) 501 45 42
Fax (32-2) 501 45 96

BULGARIA

Държавна комисия по сигурността на информацията
ул. Ангел Кънчев 1
София 1000
България
Телефон: (359-2) 921 59 11
Факс: (359-2) 987 37 50

State Commission on Information Security
1 Angel Kanchev Str.
BG-1000 Sofia
Телефон: (359-2) 921 59 11
Факс: (359-2) 987 37 50

CZECH REPUBLIC

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
CZ-150 06 Praha 56
Tel.: (420) 257 28 33 35
Fax: (420) 257 28 31 10

DENMARK

Politiets Efterretningstjeneste
Klausdalsbrovej 1
DK-2860 Søborg
Telefon (45) 33 14 88 88
Fax (45) 33 43 01 90

Forsvarets Efterretningstjeneste
Kastellet 30
DK-2100 København Ø
Telefon (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
Telefon (49-1) 88 86 81 15 26
Fax (49-1) 888 68 15 15 26

▼M4

ESTONIA

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

Faks: + 372/7170 213

GREECE

Γενικό Επιτελείο Εθνικής Αμύνης (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) 652 76 12

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020
Holargos — Athens

Τηλέφωνα: (30-210) 657 20 09 (ώρες γραφείου)
(30-210) 657 20 10 (ώρες γραφείου)

Φαξ (30-210) 642 64 32
(30-210) 652 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

Tel. (34) 913 72 57 07
(34) 913 72 50 27

Fax (34) 913 72 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

Tél. (33) 171 75 81 77

Fax (33) 171 75 82 00

IRELAND

National Security Authority
Department of Foreign Affairs
80 St Stephens Green
Dublin 2
Telephone: + 353-1-478 08 22

▼M4

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
Tel. (39) 06 61 17 42 66

Fax (39) 06 488 52 73

CYPRUS

Υπουργείο Άμυνας
Στρατιωτικό Επιτελείο του Υπουργού
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

Φαξ (357-22) 30 23 51

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
CY-1432 Nicosia
Τηλέφωνα: (357-22) 80 75 69, (357-22) 80 76 43, (357-22) 80 77 64, (357) 99 35 80 00

Φαξ (357-22) 30 23 51

LATVIA

National Security Authority of Constitution Protection
Bureau of the Republic of Latvia
Miera iela 85 A
LV-1001 Rīga
Tālrunis: (371) 702 54 18

Fakss: (371) 702 54 54

LITHUANIA

National Security Authority of the Republic of Lithuania
Gedimino pr. 40/1 LTL-2600 Vilnius
Telefonas: (370) 5 266 32 05

Faksas: (370) 5 266 32 00

LUXEMBOURG

Autorité nationale de sécurité
Boîte postale 2379
L-1023 Luxembourg

Tél. (352) 47 82 210 central
(352) 47 82 253 direct

Fax (352) 47 82 243

▼M4

HUNGARY

Nemzeti Biztonsági Felügyelet
Pf.: 2
H-1357 Budapest
Telefon: (36-1) 346 96 52

Fax: (36-1) 346 96 58

MALTA

Ministeru tal-Ġustizzja u l-Affarijiet Interni
P.O. Box 146
MT-Valletta
Telefown: + 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
Telefoon: + 31/70/320 44 00

Fax 31/70/320 07 33

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
NL-2500 ES Den Haag
Telefoon: + 31/70/318 70 60

Fax 31/70/318 75 22

AUSTRIA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
A-1014 Wien
Telefon (43-1) 531 15 25 94

Fax (43-1) 531 15 26 15

POLAND

Agencja Bezpieczeństwa Wewnętrznego – ABW
Departament Ochrony Informacji Niejawnych
ul. Rakowiecka 2 A
00-993 Warszawa
Polska
Tel.: (48-22) 585 73 60

Faks: (48-22) 585 85 09

Służba Kontrwywiadu Wojskowego
Biuro Ochrony Informacji Niejawnych
ul. Oczki 1
02-007 Warszawa
Polska
Tel.: (48-22) 684 12 47

Faks: (48-22) 684 10 76

PORTUGAL

Presidência do Conselho de Ministros

▼M4

Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P-1400-204 Lisboa
Tel.: (+351) 21 301 17 10

Fax: (+351) 21 303 17 11

ROMANIA

Romanian ANS – ORNISS
Strada Mureş nr. 4
RO-012275 Bucureşti
Telefon: (40-21) 224 58 30

Fax: (40-21) 224 07 14

SLOVENIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
SI-1000 Ljubljana
Tel. (386-1) 478 13 90

Faks (386-1) 478 13 99

SLOVAKIA

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava 57
Slovenská republika
Tel.: (421-2) 68 69 23 14

Fax: (421-2) 63 82 40 05

FINLAND

Kansallinen turvallisuusviranomainen
Ulkoasiainministeriö/Turvallisuusyksikkö
Kanavakatu 3 A
PL 176
FI-00161 Helsinki
P. (358-9) 16 05 55 10

F. (358-9) 16 05 55 16

SWEDEN

Utrikesdepartementet
SSSB
S-103 39 Stockholm
Telefon (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: + 44-020 7930 8768

Fax + 44-020 7821 8604

▼M4

Appendix 2

Comparison of security classifications

EU Classification	Très secret UE/EU top secret	Secret UE	Confidentiel UE	Restreint UE
Belgium	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
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 ([1]) — 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 ([2])	Secret Défense	Confidentiel Défense	Néant ([3])
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!

▼M4

EU Classification	Très secret UE/EU top secret	Secret UE	Confidentiel UE	Restreint UE
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Netherlands	STG Zeer Geheim	STG Geheim	STG Confidentieel	Departementaalvertrouwelijk
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Poland	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Romania	Strict secret de importanţă 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	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
United Kingdom	Top Secret	Secret	Confidential	Restricted
NATO Classification	Cosmic Top Secret	NATO Secret	NATO Confidential	NATO Restricted
WEU Classification	Focal Top Secret	WEU Secret	WEU Confidential	WEU Restricted

(1) Germany: VS = Verschlusssache.
(2) France: the classification Très Secret Défense, which covers governmental priority issues, may be changed only with the Prime Minister's authorisation.
(3) France does not use the classification category 'DIFFUSION RESTREINTE' in its national system. France handles and protects documents bearing the marking 'RESTREINT UE' according to its national laws and regulations in force, which are not less stringent than the provisions of the Council's security regulations.

Appendix 3

Practical classification guide

This guide is indicative and may not be construed as modifying the substantial provisions laid down in Sections II and III.

Classification	When	Who	Markings	Downgrading/Declassification/Destruction	
				Who	When
TRÈS SECRET UE/EU TOP SECRET: This classification shall be applied only to 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 its Member States [SII(1)].	The compromise of assets marked TRÈS SECRET UE/EU TOP SECRET would be likely to: — threaten directly the internal stability of the EU or one of its Member States or friendly countries — cause exceptionally grave damage to relations with friendly governments — lead directly to widespread loss of life — cause exceptionally grave damage to the operational effectiveness or security of Member States or other contributors' forces, or to the continuing effectiveness of extremely valuable security or intelligence operations — cause severe long-term damage to the EU or Member States economy.	Member States: duly authorised persons (originators) [SIII(4)]; GSC: duly authorised persons (originators) [SIII(4)], SG/HR and DSG. Originators shall specify a date or period when the contents may be downgraded or declassified. Otherwise they shall keep the documents under review every five years at the latest, in order to ensure that the original classification is necessary [SIII(10)].	The classification TRÈS SECRET UE/EU TOP SECRET shall be applied to TRÈS SECRET UE/EU TOP SECRET documents, and where applicable introduce the defence marking ESDP, by mechanical means and by hand [SII(8)]. The EU classifications shall appear at the top and bottom centre of each page, and each page shall be numbered. Each document shall bear a reference number and a date; this reference number shall appear on each page. If they are to be distributed in several copies, each one shall bear a copy number, which will appear on the first page, together with the total number of pages. All annexes and enclosures shall be listed on the first page [SVII(1)].	Declassification or down grading rests solely with the originator, or the SG/HR or DSG, who shall inform of the change any subsequent addressees to whom they have sent or copied the document [SVIII(9)]. TRÈS SECRET UE/EU TOP SECRET documents shall be destroyed by the Central Registry or subregistry responsible for them. Each document destroyed shall be listed in a destruction certificate, signed by the TRÈS SECRET UE/EU TOP SECRET control officer and by the officer witnessing the destruction, who shall be TRÈS SECRET UE/EU TOP SECRET cleared. A note to this effect shall be made in the logbook. The registry shall keep the destruction certificates, together with the distribution sheet, for a period of ten years [SVII(31)].	Surplus copies and documents no longer needed must be destroyed [SVII(31)]. TRÈS SECRET UE/EU TOP SECRET documents, including all classified waste resulting from the preparation of TRÈS SECRET UE/EU TOP SECRET documents such as spoiled copies, working drafts, typed notes and carbon paper, shall be destroyed, under the supervision of a TRÈS SECRET UE/EU TOP SECRET officer, by burning, pulping, shredding or otherwise reducing into an unrecognisable and non-reconstitutable form [SVII(31)].
SECRET: This classification shall be	The compromise of assets marked SECRET UE would be likely to:	Member States: authorised persons (origi-	The classification SECRET UE shall be applied to SECRET UE documents, and	Declassification and downgrading rests solely with the originator, or the SG/HR or	Surplus copies and documents no longer needed must be destroyed [SVII(31)].

Classification	When	Who	Markings	Downgrading/Declassification/Destruction	
				Who	When
applied only to information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of its Member States [SII(2)].	— raise international tensions — seriously damage relations with friendly governments — threaten life directly or seriously prejudice public order or individual security or liberty — cause serious damage to the operational effectiveness or security of Member States or other contributors' forces, or to the continuing effectiveness of highly valuable security or intelligence operations — cause substantial material damage to EU or one of its Member States financial, monetary, economic and commercial interests.	nators) [SIII(2)]; GSC and EU decentralised agencies: authorised persons (originators) [SIII(2)], Directors General, SG/HR and DSG. Originators shall specify a date or period when the contents may be downgraded or declassified. Otherwise they shall keep the documents under review every five years at the latest, in order to ensure that the original classification is necessary [SVII(1)].	where applicable introduce the defence marking — ESDP, by mechanical means and by hand [SIII(8)]. The EU classifications shall appear at the top and bottom centre of each page, and each page shall be numbered. Each document shall bear a reference number and a date; this reference number shall appear on each page. If they are to be distributed in several copies, each one shall bear a copy number, which will appear on the first page, together with the total number of pages. All annexes and enclosures shall be listed on the first page [SVII(1)].	DSG, who shall inform of the change any subsequent addressees to whom they have sent or copied the document [SVII(9)]. SECRET UE documents shall be destroyed by the registry responsible for those documents, under the supervision of a security cleared person. SECRET UE documents that are destroyed shall be listed on signed destruction certificates to be retained by the Registry, together with the destruction forms, for at least three years [SVII(32)].	SECRET UE documents, including all classified waste resulting from the preparation of SECRET UE documents such as spoiled copies, working drafts, typed notes and carbon paper, shall be destroyed by burning, pulping, shredding or otherwise reducing into an unrecognisable and non-reconstitutable form [SVII(31),(32)].
CONFIDENTIEL UE: This classification shall be applied to information and material the unauthorised disclosure of would harm the essential interests of the European Union or of one or more of its Member [SII(3)].	The compromise of assets marked CONFIDENTIEL UE would be likely to: — materially damage diplomatic relations, that is, cause formal protest or other sanctions — prejudice individual security or liberty — cause damage to the operational effectiveness or security of Member States or other contri-	Member States: authorised persons (originators) [SIII(2)]; GSC and EU decentralised agencies: authorised persons (originators) [SIII(2)], Directors General, SG/HR and DSG. Originators shall specify a date or period when the contents may be downgraded or declassified. Otherwise they shall	The classification CONFIDENTIEL UE shall be applied to CONFIDENTIEL UE documents, and where applicable introduce the defence-marking — ESDP, by mechanical means and by hand or by printing on pre-stamped, registered paper [SII (8)]. The EU classifications shall appear at the top and bottom centre on each page, and each page shall be numbered.	Declassification and downgrading rests solely with the originator or the SG/HR or DSG, who shall inform of the change any subsequent addressees to whom they have sent or copied the document [SVII(31)]. CONFIDENTIEL UE documents shall be destroyed by the registry respon-sible for those documents, under the supervision of a cleared person. Their destruction shall	Surplus copies and documents no longer needed must be destroyed [SVII(31)]. CONFIDENTIEL UE documents, including all classified waste resulting from the preparation of CONFIDENTIEL UE documents such as spoiled copies, working drafts, typed notes and carbon paper, shall be destroyed by burning, pulping, shredding or otherwise reducing into an unrecognisable

Classification	When	Who	Markings	Downgrading/Declassification/Destruction	
				Who	When
	butors' forces, or to the effectiveness of valuable security or intelligence operations — substantially undermine the financial viability of major organisations — impede the investigation or facilitate the commission of serious crime — work substantially against EU or Member States financial, monetary, economic and commercial interests — seriously impede the development or operation of major EU policies — shut down or otherwise substantially disrupt significant EU activities.	keep the documents under review every five years at the latest, in order to ensure that the original classification is necessary [SIII(10)].	Each document shall bear a reference number and a date. All annexes and enclosures shall be listed on the first page [SVII(1)].	be recorded in accordance with national regulations and, in the case of GSC or EU decentralised agencies, according to instructions from the SG/HR or DSG [SVII(33)].	and non-reconstitutable form [SVII(31),(33)].
RESTREINT UE: This classification shall be applied to information and material the unauthorised disclosure of which could be disadvantageous to the interests of the EU or of one or more of its Member States [SII(4)].	The compromise of assets marked RESTREINT UE would be likely to: — adversely affect diplomatic relations — cause substantial distress to individuals — make it more difficult to maintain the operational effectiveness or security of Member States or other contributors' forces — cause financial loss or	Member States: authorised persons (originators) [SIII(2)]; GSC and EU decentralised agencies: authorised persons (originators) [SIII(2)], Directors General, SG/HR and DSG. Originators shall specify a date or period when the contents may be downgraded or declassified. Otherwise they shall keep the documents under	The classification RESTREINT UE shall be applied to RESTREINT UE documents, and where applicable introduce the defence marking — ESDP, by mechanical or electronic means [SII(8)]. The EU classifications shall appear at the top and bottom centre on each page, and each page shall be numbered. Each document shall bear a	Declassification and downgrading rests solely with the originator, or the SG/HR or DSG, who shall inform of the change any subsequent addressees to whom they have sent or copied the document [SIII(9)]. RESTREINT UE documents shall be destroyed by the registry responsible for those documents, in accordance with national regulations and, in the case of GSC or EU	Surplus copies and documents no longer needed must be destroyed [SVII(31)].

▼B

Classification	When	Who	Markings	Downgrading/Declassification/Destruction	
				Who	When
	facilitate improper gain or advantage for individuals or companies — breach proper undertakings to maintain the confidence of information provided by third parties — breach statutory restrictions on disclosure of information — prejudice the investigation or facilitate the commission of crime — disadvantage EU or Member States in commercial or policy negotiations with others — impede the effective development or operation of EU policies — undermine the proper management of the EU and its operations.	review every five years at the latest, in order to ensure that the original classification is necessary [SIII(10)].	reference number and a date [SVII(1)].	decentralised agencies, according to instructions from the SG/HR or DSG [SVII (34)].	

▼B

Appendix 4

Guidelines for release of EU classified information to third States or international organisations

Level 1 Cooperation

PROCEDURES

1. The authority to release EU classified information to countries that are not signatories of the Treaty on European Union or to other international organisations whose security policy and regulations are comparable to EU's lies with the Council.

2. The Council may delegate the decision to release classified information. Its delegation will state the nature of the information that may be released and its level of classification, which will normally be no higher than CONFIDENTIEL UE.

3. Subject to the conclusion of a security agreement, requests for the release of EU classified information will be made to the Secretary-General/High Representative by the security bodies of the States or international organisations concerned, which shall state the purposes for which this release is intended and the nature of the classified information to be released.

   Requests may also be made by a Member State or EU decentralised agency, that regard the release of EU classified information as desirable; they will state the aims and the benefit to EU of such a release, specifying the nature and classification of the information to be released.

4. The request will be considered by the GSC, which:

   — shall seek the opinions of the Member State or, as appropriate, the decentralised EU agency originating the information to be released,

   — shall establish the necessary contacts with the security bodies of the beneficiary countries or international organisations to verify whether their security policy and regulations are such as to guarantee that the classified information released will be protected in accordance with these security regulations,

   — shall seek the technical opinions of the Member States' National Security Authorities as to the confidence that can be placed in the beneficiary States or international bodies.

5. The GSC will forward the request and the Security Office's recommendation to the Council for a decision.

SECURITY REGULATIONS TO BE APPLIED BY BENEFICIARIES

6. The Secretary-General/High Representative will notify the beneficiary States or international organisations of the Council's decision to authorise the release of EU classified information, forwarding as many copies of these security regulations as are considered necessary. If the request was made by a Member State, this State will notify the beneficiary of the authorised release.

   The decision to release will come into force only when the beneficiaries give a written assurance that they will:

   — use the information for no other than the agreed purposes,

   — protect the information in accordance with these security regulations and in particular the special provisions set out below.

7. *Personnel*

   (a) The number of officials having access to the EU classified information will be strictly limited, based on the need-to-know principle, to those persons whose duties require such access.

   (b) All officials or nationals authorised to have access to information classified CONFIDENTIEL UE or above shall hold either a security certificate at the appropriate level or the equivalent security clearance, either one being issued by their own State's government.

▼B

8. *Transmission of documents*

   (a) The practical procedures for the transmission of documents will be decided by agreement on the basis of the provisions of Section VII of the Council Security Regulations. They will in particular specify the registries to which EU classified information is to be forwarded.

   (b) If the classified information whose release is authorised by the Council includes TRÈS SECRET UE/EU TOP SECRET, the beneficiary State or international organisation shall set up a central EU registry and, if necessary, EU subregistries. These registries will be governed by the provisions of Section VIII of these security regulations.

9. *Registration*

   As soon as a registry receives a EU document classified CONFIDENTIEL UE or above, it will list the document in a special register held by the organisation, with columns for the date received, particulars of the document (date, reference and copy number), its classification, title, the recipient's name or title, the date of return of the receipt and the date the document is returned to the EU originator or is destroyed.

10. *Destruction*

   (a) EU classified documents will be destroyed in accordance with the instructions set out in Section VI of these security regulations. Copies of the destruction certificates for SECRET UE and TRÈS SECRET UE/EU TOP SECRET documents will be sent to the EU registry that has forwarded the documents.

   (b) EU classified documents will be included in emergency destruction plans for the beneficiary bodies own classified documents.

11. *Protection of documents*

   Every step will be taken to prevent unauthorised persons from having access to EU classified information.

12. *Copies, translations and extracts*

   No photocopies or translation may be made of a document classified CONFIDENTIEL UE or SECRET UE, or extracts taken, without the authorisation of the Head of the security organisation concerned, who will register and check those copies, translations or extracts and stamp them as necessary.

   The reproduction or translation of a TRÈS SECRET UE/EU TOP SECRET document may be authorised only by the originating authority, which will specify the number of copies authorised; if the originating authority cannot be determined, the request will be referred to the GSC Security Office.

13. *Breaches of security*

   When a breach of security involving a EU classified document has taken place or is suspected, the following action should be taken immediately, subject to the conclusion of a security agreement:

   (a) carry out an investigation to establish the circumstances of the breach of security;

   (b) notify the GSC Security Office, the National Security Authority and the originating authority, or clearly state that the latter has not been notified if this has not been done;

   (c) take action to minimise the effects of the breach of security;

   (d) reconsider and implement measures to prevent any recurrence;

   (e) implement any measures recommended by the GSC Security Office to prevent a recurrence.

14. *Inspections*

   The GSC Security Office will be permitted, by agreement with the States or international organisations concerned, to carry out an assessment of the effectiveness of measures for the protection of the EU classified information released.

15. *Reporting*

   Subject to the conclusion of a security agreement, as long as the State or international organisation holds EU classified information, it should submit a

▼B

yearly report, by a date specified when the authorisation to release the information is given, confirming that these security regulations have been complied with.

▼B

Appendix 5

Guidelines for release of EU classified information to third States or international organisations

Level 2 Cooperation

PROCEDURES

1. The authority to release EU classified information to third States or international organisations whose security policy and regulations are markedly different from EU's lies with the Council. In principle, it is restricted to information classified up to and including SECRET UE; it excludes national information specifically reserved to Member States and categories of EU classified information protected by special markings.

2. The Council may delegate the decision: in delegating it will, within the constraints defined in paragraph 1, state the nature of the information that may be released and its level of classification, which will be no higher than RESTREINT UE.

3. Subject to the conclusion of a security agreement, requests for the release of EU classified information will be made to the Secretary-General/High Representative by the security bodies of the States or international organisations concerned, which will state the purposes for which this release is intended and the nature and classification of the information to be released.

   Requests may also be made by a Member State or EU decentralised agency that regard the release of EU classified information as desirable; they will state the aims and the benefit to EU of such a release, specifying the nature and classification of the information to be released.

4. The request will be considered by the GSC, which:

   — shall seek the opinions of the Member State or, as appropriate, the EU decentralised agency originating the information to be released,

   — shall establish preliminary contacts with the security bodies of the beneficiary States or international organisations to find out information on their security policy and regulations, and in particular to draw up a table comparing the classifications applicable in the EU and in the State or organisation concerned,

   — shall arrange for a meeting of the Council Security Committee or, under a silent procedure if necessary, enquire from the Member States' National Security Authorities with a view to obtaining the Security Committee's technical opinion.

5. The Council Security Committee's technical opinion will be on the following:

   — the confidence that can be placed in the beneficiary States or international organisations with a view to assessing the security risks incurred by the EU or its Member States,

   — an assessment of the beneficiaries' ability to protect classified information released by EU,

   — proposals as to practical procedures for the handling of the EU classified information (for example providing expurgated versions of a text) and documents transmitted (retaining or deleting EU classification headings, specific markings, etc.),

   — downgrading or declassification by the originating authority before the information is released to the beneficiary countries or international organisations ([1]).

6. The Secretary-General/High Representative will forward to the Council for a decision, the request and the Council Security Committee's technical opinion obtained by the GSC Security Office.

([1]) This entails the originating authority's application of the procedure defined in paragraph 9, Section III, in the case of all copies circulated within EU.

▼B

SECURITY REGULATIONS TO BE APPLIED BY BENEFICIARIES

7. The Council's decision to authorise the release of EU classified information will be brought to the attention of the beneficiary countries or international organisations by the Secretary-General/High Representative, together with a table comparing the classifications applicable within the EU and the States or organisations concerned. If the request was made by a Member State, this State will notify the beneficiary of the authorised release.

   The decision to release will come into force only when the beneficiaries give a written assurance that they will:

   — use the information for no other than the agreed purposes,

   — protect the information in accordance with the regulations laid down by the Council.

8. The following rules of protection will be established unless the Council, having obtained the Council Security Committee's technical opinion, decides on a particular procedure for the handling of EU classified documents (deleting mention of the EU classification, specific marking, etc.).

   The rules will be adapted in that case.

9. *Personnel*

   (a) The number of officials having access to EU classified information must be strictly limited, based on the need-to-know principle, to those persons whose duties require such access.

   (b) All officials or nationals authorised to have access to the classified information released by EU shall have a national security clearance or authorisation for access, in the case of national classified information, to an appropriate level equivalent to that of the EU, as defined in the comparative table.

   (c) These national security clearances or authorisations will be forwarded to the Secretary-General/High Representative for information.

10. *Transmission of documents*

   (a) The practical procedures for the transmission of documents will be agreed between the GSC Security Office and the security bodies of the recipient States or international organisations based on its rules set out in Section VII of these Regulations. They will in particular specify the precise addresses to which the documents must be forwarded as well as the courier or mail services used for the transmission of the EU classified information.

   (b) Documents classified CONFIDENTIEL UE and higher will be transmitted under double cover. The inner envelope will be marked 'UE' together with the security classification. A receipt form will be enclosed for each classified document. The receipt form, which will not itself be classified, will quote only the particulars of the document (its reference, date, copy number) and its language, not the title.

   (c) The inner envelope will then be placed in the outer envelope, which will carry a package number for receipting purposes. The outer envelope will not bear a security classification.

   (d) A receipt showing the package number will always be given to the couriers.

11. *Registration on arrival*

   The addressee State's NSA or its equivalent in the State receiving on behalf of its government the classified information forwarded by the EU, or the security bureau of the recipient international organisation, will open a special register to record EU classified information on its receipt. The Register will contain columns indicating the date received, particulars of the document (date, reference and copy number), its classification, title, the addressee's name or title, the date of return of the receipt and the date of return of the document to EU or its destruction.

12. *Return of documents*

   When the recipient returns a classified document to the Council, or the Member State which released it, it will proceed as indicated in paragraph 10.

▼B

13. *Protection*

(a) When the documents are not in use, they will be stored in a security container which is approved for the storage of nationally-classified material of the same classification. The container will bear no indication of its contents, which will be accessible only to persons authorised to handle EU classified information. Where combination locks are used, the combination will be known only to those officials in the State or organisation having authorised access to the EU classified information stored in the container and will be changed every six months, or sooner on the transfer of an official, on withdrawal of the security clearance of one of the officials knowing the combination or if there is a risk of compromise.

(b) EU classified documents will be removed from the security container only by those officials cleared for access to the EU classified documents and having need to know. They will remain responsible for the safe custody of those documents as long as they are in their possession and, in particular, for ensuring that no unauthorised person has access to the documents. They will also ensure that the documents are stored in a security container when they have finished consulting them and outside working hours.

(c) No photocopies may be made of a document classified CONFIDENTIEL UE or above, nor extracts taken, without the authorisation of the GSC Security office.

(d) The procedure for the rapid and total destruction of the documents in an emergency should be defined and confirmed with the GSC Security office.

14. *Physical security*

(a) When not in use, security containers used for storage of EU classified documents shall be kept locked at all times.

(b) When it is necessary for maintenance or cleaning staff to enter or work in a room which houses such security containers, they shall be escorted at all times by a member of the State's or organisation's security service or by the official more specifically responsible for supervising the security of the room.

(c) Outside normal working hours (at night, at weekends and on public holidays) the security containers containing EU classified documents shall be protected either by a guard or by an automatic alarm system.

15. *Breaches of security*

When a breach of security involving a EU classified document has taken place or is suspected, the following action should be taken immediately:

(a) forward a report immediately to the GSC Security Office or the NSA of the Member State that has taken the initiative in forwarding documents (with a copy to the GSC Security Office);

(b) conduct an enquiry, on completion of which a full report will be submitted to the security body (see (a) above). The requisite measures to remedy the situation should then be adopted.

16. *Inspections*

The GSC Security Office will be permitted, by agreement with the States or international organisations concerned, to carry out an assessment of the effectiveness of measures for the protection of the EU classified information released.

17. *Reporting*

As long as the State or organisation holds EU classified information, it shall submit a yearly report, by a date specified when the authorisation to release the information is given, confirming that these security regulations have been complied with.

▼B

Appendix 6

Guidelines for release of EU classified information to third States or international organisations

Level 3 Cooperation

PROCEDURES

1. From time to time, the Council may wish to cooperate in certain special circumstances with States or organisations that cannot give the assurances required by these security regulations, but that cooperation may call for the release of EU classified information. Such release will be exclusive of national information specifically reserved to Member States.

2. In such special circumstances, requests for cooperation with EU, whether from third States or international organisations or whether proposed by the Member States or, where applicable, EU decentralised agencies, will first be considered as to substance by the Council, which will, where necessary, seek the opinions of the Member State or decentralised agency originating the information. The Council will consider the wisdom of releasing classified information, assess the beneficiaries' need to know and decide on the nature of the classified information that may be communicated.

3. If the Council is in favour, it will be the responsibility of the Secretary-General/High Representative to convene the Council Security Committee or to enquire from the National Security Authorities of Member States, if appropriate under a silence procedure, in order to obtain the Security Committee's technical opinion.

4. The Council Security Committee's technical opinion will be on the following:

   (a) an evaluation of the security risks incurred by EU or its Member States;

   (b) classification of the information that may be released, where appropriate, in view of its nature;

   (c) the downgrading or declassification of the information by the originating authority before it is released to the countries or international organisations concerned ([1]);

   (d) procedures for handling the documents to be released (see paragraph 5 below);

   (e) the possible methods of transmission (use of public postal services, public or secure telecommunications systems, diplomatic bag, cleared couriers, etc.).

5. The documents released to the States or organisations covered in this Appendix will, in principle, be prepared without reference to the source or a EU classification. The Council Security Committee may recommend:

   — the use of a specific marking or codename,

   — the use of a specific system of classification linking the sensitivity of the information to the control measures required of the beneficiary methods of transmission of the documents (see examples in paragraph 14).

6. The GSC Security Office will submit the Security Committee's technical opinion to the Council, where necessary attaching the proposed delegations of authority required for the performance of the task, particularly in urgent circumstances.

7. Once the Council has approved the release of EU classified information and the practical implementing procedures, the GSC Security Office will establish the necessary contact with the security body of the State or organisation concerned to facilitate the application of the security measures envisaged.

8. As a reference, the GSC Security Office will circulate a table to all the Member States and where appropriate, EU decentralised agencies concerned summarising the nature and classification of the information and

([1]) This entails the originating authority's application of the procedure defined in paragraph 9, Section III, to all copies circulated within EU.

▼B

listing the organisations and countries to which it may be released, as decided by the Council.

9. The NSA of the Member State making the release, or the GSC Security Office, will take all the necessary measures to facilitate any consequent damage assessment and review of procedures.

10. Further reference will be made to the Council whenever the conditions of cooperation are altered.

SECURITY REGULATIONS TO BE APPLIED BY BENEFICIARIES

11. The Council's decision to authorise the release of EU classified information will be brought to the attention of the beneficiary States or international organisations by the Secretary-General/High Representative, together with the detailed rules of protection proposed by the Council Security Committee and approved by the Council. If the request was made by a Member State, this State will notify the beneficiary of the authorised release.

    The decision will come into force only when the beneficiaries give a written assurance that they will:

    — use the information for no other purpose than the cooperation decided by the Council,

    — offer the information the protection required by the Council.

12. *Transmission of documents*

    (a) The practical procedures for the transmission of documents will be agreed between the GSC Security Office and the security bodies of the recipient States or international organisations. They will in particular specify the precise addresses to which the documents must be forwarded.

    (b) Documents classified CONFIDENTIEL UE and higher will be transmitted under double cover. The inner envelope will bear the specific stamp or codename decided upon and a mention of the special classification approved for the document. A receipt form will be enclosed for each classified document. The receipt form, which will not itself be classified, will quote only the particulars of the document (its reference, date, copy number) and its language, not the title.

    (c) The inner envelope will then be placed in the outer envelope, which will carry a package number for receipting purposes. The outer envelope will not bear a security classification.

    (d) A receipt showing the package number will always be given to the couriers.

13. *Registration on arrival*

    The addressee State's NSA or its equivalent in the State receiving the classified information forwarded by EU on behalf of its government, or the security bureau of the recipient international organisation, will open a special register to record EU classified information on its receipt. The Register will contain columns indicating the date received, particulars of the document (date, reference and copy number), its classification, title, the addressee's name or title, the date of return of the receipt and the date of return of the receipt to EU and the date of destruction of the document.

14. *Use and protection of the classified information exchanged*

    (a) Information at the level of SECRET UE will be handled by specifically designated officials authorised to have access to information with this classification. It will be stored in good quality security cabinets that can be opened only by the persons authorised to have access to the information they contain. The areas in which those cabinets are located will be permanently guarded and a system of verification will be set up to ensure that only duly authorised persons are allowed to enter. SECRET UE-level information will be forwarded by diplomatic bag, secure mail services and secure telecommunications. A SECRET UE document may be copied only with the originating authority's written agreement. All copies will be registered and monitored. Receipts will be issued for all operations relating to SECRET UE documents.

▼B

(b) CONFIDENTIEL UE-level information will be handled by duly designated officials authorised to be informed on the subject. Documents will be stored in locked security cabinets in controlled areas.

CONFIDENTIEL UE-level information will be forwarded by diplomatic bag, military mail services and secure telecommunications. Copies may be made by the recipient body, their number and distribution being recorded in special registers.

(c) RESTREINT UE-level information will be handled in premises that are not accessible to unauthorised personnel and stored in locked containers. Documents may be forwarded by public postal services as registered mail in a double envelope and, in emergency situations during operations, by the unprotected public telecommunications systems. The recipients may make copies.

(d) Unclassified information will not call for special protection measures and may be forwarded by mail and public telecommunications systems. The addressees may make copies.

15. *Destruction*

Documents no longer needed must be destroyed. In the case of RESTREINT UE and CONFIDENTIEL UE-level documents, an appropriate note will be entered in the special registers. In the case of SECRET UE-level documents, destruction certificates will be issued and signed by two persons witnessing their destruction.

16. *Breaches of security*

If CONFIDENTIEL UE- or SECRET UE-level information is compromised or there is a suspicion of compromise, the NSA of the State or the head of security in the organisation will conduct an enquiry into the circumstances of the compromise. If the enquiry yields positive results, the originating authority will be notified. The necessary steps will be taken to remedy inadequate procedures or storage methods if they have given rise to the compromise. The Council Secretary-General/High Representative or the NSA of the Member State that released the compromised information may ask the beneficiary for details on the enquiry.