II

(Acts whose publication is not obligatory)

COMMISSION

COMMISSION DECISION
of 29 November 2001
amending its internal Rules of Procedure

(notified under document number C(2001) 3031)

(2001/844/EC, ECSC, Euratom)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Community, and in particular Article 218(2) thereof,

Having regard to the Treaty establishing the European Coal and Steel Community, and in particular Article 16 thereof,

Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 131 thereof,

Having regard to the Treaty on European Union, and in particular Article 28(1) and Article 41(1) thereof,

HAS DECIDED AS FOLLOWS:

Article 1

The Commission's provisions on security, the text of which is annexed to this Decision, are hereby added to the Commission's Rules of Procedure as an annex.

Article 2

This Decision shall enter into force on the day of its publication in the *Official Journal of the European Communities*.

It shall apply from 1 December 2001.

Done at Brussels, 29 November 2001.

For the Commission
The President
Romano PRODI

ANNEX

COMMISSION PROVISIONS ON SECURITY

Whereas:

(1) In order to develop Commission activities in areas which require a degree of confidentiality, it is appropriate to establish a comprehensive security system applicable to the Commission, the other institutions, bodies, offices and agencies established by virtue or on the basis of the EC Treaty or the Treaty on European Union, the Member States, as well as any other recipient of European Union classified information, hereafter referred to as 'EU classified information'.

(2) In order to safeguard the effectiveness of the security system thus established, the Commission will make EU classified information available only to those outside bodies which offer guarantees that they have taken all measures necessary to apply rules strictly equivalent to these provisions.

(3) These provisions are taken without prejudice to Regulation No 3 of 31 July 1958 implementing Article 24 of the Treaty establishing the European Atomic Energy Community [1], to Council Regulation (EC) No 1588/90 of 11 June 1990 on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities [2] and to Commission Decision C (95) 1510 final of 23 November 1995 on the protection of informatics systems.

(4) The Commission's security system is based on the principles put forward in Council Decision 2001/264/EC of 19 March 2001 adopting the Council's security regulations [3] with a view to ensuring a smooth functioning of the decision-making process of the Union.

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

(6) The Commission recognises the need to create its own concept of security, taking into consideration all elements of security and the specific character of the Commission as an institution.

(7) These provisions are taken without prejudice to Article 255 of the Treaty and to Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents [4];

Article 1

The Commission's rules on security are set out in the Annex.

Article 2

1. The Member of the Commission responsible for security matters shall take appropriate measures to ensure that, when handling EU classified information, the rules referred to in Article 1 are respected within the Commission by Commission officials and other servants, by personnel seconded to the Commission, as well as within all Commission premises, including its Representations and Offices in the Union and its Delegations in third countries and by contractors external to the Commission.

2. Member States, other institutions, bodies, offices and agencies established by virtue or on the basis of the Treaties shall be allowed to receive EU classified information on the condition that they ensure that, when EU classified information is handled, rules strictly equivalent to those referred to in Article 1 are respected within their services and premises, in particular by:

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

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

[1] OJ L 17/58, 6.10.1958, p. 406/58.
[2] OJ L 151, 15.6.1990, p. 1.
[3] OJ L 101, 11.4.2001, p. 1.
[4] OJ L 145, 31.5.2001, p. 43.

Article 3

Third states, international organisations and other bodies shall be allowed to receive EU classified information on the condition that they ensure that, when such information is handled, rules strictly equivalent to those referred to in Article 1 are respected.

Article 4

In keeping with the basic principles and minimum standards of security contained in Part I of the Annex, the Member of the Commission responsible for security matters may take measures in accordance with Part II of the Annex.

Article 5

As from the date of their application, these provisions shall replace:

(a) Commission Decision C (94) 3282 of 30 November 1994 on the security measures applicable to classified information produced or transmitted in connection with activities of the European Union;

(b) Commission Decision C (99) 423 of 25 February 1999 relating to the procedures whereby officials and other employees of the European Commission may be allowed access to classified information held by the Commission.

Article 6

As from the date of application of these provisions, all classified information held by the Commission until that date, with the exception of Euratom classified information, shall:

(a) if created by the Commission, be considered to be reclassified 'EU RESTRICTED' by default, unless its author decides to give it another classification by 31 January 2002. In such case the author shall inform all addressees of the document concerned;

(b) if created by authors outside the Commission, retain its original classification and thus be treated as EU classified information of the equivalent level, unless the author agrees to declassification or downgrading of the information.

ANNEX

RULES ON SECURITY

Contents

-

PART I: BASIC PRINCIPLES AND MINIMUM STANDARDS OF SECURITY

1. INTRODUCTION

These provisions lay down the basic principles and minimum standards of security to be respected in an appropriate manner by the Commission in all its places of employment, as well as by all recipients of EUCI, so that security is safeguarded and each may be assured that a common standard of protection is established.

2. GENERAL PRINCIPLES

The Commission's security policy forms an integral part of its general internal management policy and is thus based on the principles governing its general policy.

These principles include legality, transparency, accountability and subsidiarity (proportionality).

Legality indicates the need to stay strictly within the legal framework in executing security functions and the need to conform to the legal requirements. It also means that responsibilities in the domain of security have to be based on proper legal provisions. The provisions in the Staff Regulations fully apply, notably its Article 17 on the obligation of staff to exercise discretion with regard to Commission information and its Title VI on disciplinary measures. Finally it means that breaches of security within the responsibility of the Commission have to be dealt with in a manner consistent with Commission policy on disciplinary actions and with its policy on cooperation with Member States in the area of criminal justice.

Transparency indicates the need for clarity regarding all security rules and provisions, for balance between the different services and the different domains (physical security versus information protection etc.) and the need for a consistent and structured security awareness policy. It also defines a need for clear written guidelines for implementing security measures.

Accountability means that responsibilities in the domain of security will be clearly defined. Moreover it indicates the need to test regularly whether these responsibilities have been correctly executed.

Subsidiarity, or proportionality, means that security shall be organised on the lowest possible level and as close as possible to the Directorates General and services of the Commission. It also indicates that security activities shall be limited to only those elements that really need it. And finally it means that security measures shall be proportional to the interests to be protected and to the actual or potential threat to these interests, allowing for a defence which causes the least possible disruption.

3. FOUNDATIONS OF SECURITY

The foundations of sound security are:

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

1. The collection and recording of intelligence on espionage, sabotage, terrorism and other subversive activities, and

2. Providing information and advice to its governments, and through it, to the Commission, on the nature of the threats to security and the means of protection against them.

(b) Within each Member State, and within the Commission, a technical INFOSEC authority (IA) 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 and the appropriate services of the European institutions to order to establish and recommend, as appropriate:

1. What persons, information and resources need to be protected, and

2. Common standards of protection.

(d) Close cooperation between the Commission Security Office and the security services of the other European institutions and with the NATO Office of Security (NOS).

4. PRINCIPLES OF INFORMATION SECURITY

4.1. **Objectives**

Information security has the following principal objectives:

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

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

(c) To safeguard Commission premises 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.

4.2. **Definitions**

Throughout these rules:

(a) The term 'EU classified information' (EUCI) means any information and material, an unauthorised disclosure of which could cause varying degrees of prejudice to 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.

(b) The term 'document' means 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.

(c) The term 'material' means 'document' as defined in b) and also any item of equipment, either manufactured or in the process of manufacture.

(d) The term 'need to know' means the need of an individual employee to have access to EU classified information in order to be able to perform a function or a task.

(e) 'Authorisation' means a decision by the President of the Commission to grant an individual access to EUCI up to a specific level, on the basis of a positive result of a security screening (vetting), carried out by a National Security Authority under national law.

(f) The term 'classification' means the allocation of an appropriate level of security to information the unauthorised disclosure of which might cause a certain degree of prejudice to Commission or to Member State interests.

(g) The term 'downgrading' (déclassement) means a reduction in the level of classification.

(h) The term 'declassification' (déclassification) means the removal of any classification.

(i) The term 'originator' means the duly authorised author of a classified document. Within the Commission, Heads of departements may authorize their staff to originate EUCI.

(j) The term 'Commission departments' means Commission departments and services, including the cabinets, in all places of employment, including Joint Research Centre, Representations and Offices in the Union and Delegations in third countries.

4.3. **Classification**

(a) 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 to 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 to avoid both overclassification and underclassification.

(b) The classification system is the instrument for giving effect to these principles; a similar system of classification shall 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.

(c) Responsibility for classifying information lies solely with the originator of that information.

(d) The level of classification may solely be based on the content of that information.

(e) Where a number of items of information is grouped together, the classification level to be applied to the whole shall at least be as high as the highest classification. A collection of information may however be given a higher classification than its constituent parts.

(f) Classifications shall be assigned only when necessary and for as long as necessary.

4.4. **Aims of security measures**

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 that contain it.

(d) Ensure that classified information is disseminated solely on the basis of the need-to-know principle that 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.

5. ORGANISATION OF SECURITY

5.1. **Common minimum standards**

The Commission shall ensure that common minimum standards of security are observed by all recipients of EUCI, inside the institution and under its competence, e.g. by all departments 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.

The Commission shall only allow access of EUCI to outside bodies under the condition that they ensure that, when EUCI is handled, provisions at least strictly equivalent to these minimum standards are respected.

5.2. **Organisation**

Within the Commission security is organised on two levels:

(a) On the level of the Commission as a whole there is a Commission Security Office with a Security Accreditation Authority (SAA) also acting as Crypto Authority (CrA) and as TEMPEST Authority, and with an INFOSEC Authority (IA) and one or more Central EUCI Registries, each with one or more Registry Control Officer (RCO).

(b) On the level of the Commission departments, security is the responsibility of one or more Local Security Officers (LSO), one or more Central Informatics Security Officers (CISO), Local Informatics Security Officers (LISO) and Local EU Classified Information Registries with one or more Registry Control Officers.

(c) The central security bodies will provide operational guidance to the local security bodies.

6. SECURITY OF PERSONNEL

6.1. **Clearance of personnel**

All persons who require access to information classified EU CONFIDENTIAL 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.

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

(d) To be granted access to EU TOP SECRET information;

(e) Occupying positions involving regular access to a considerable volume of EU SECRET information;

(f) Whose duties give them special access to secure 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.

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.

6.2. **Records of personnel clearances**

All Commission departments handling EU classified information or housing secure 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 Local Security Officer of the Commission department shall hold record of the clearances within his or her domain.

6.3. **Security instruction of personnel**

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. Such personnel are required to certify in writing that they have read and fully understand the present security provisions.

6.4. **Management responsibilities**

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

6.5. **Security status of personnel**

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 secure communication or information systems, and the Commission Security Office is 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.

7. PHYSICAL SECURITY

7.1. **Need for protection**

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. 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.

7.2. **Checking**

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.

7.3. **Security of buildings**

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

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

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.

7.4. **Contingency plans**

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

8. SECURITY OF INFORMATION

Information security (INFOSEC) relates to the identification and application of security measures to protect EU classified 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 classified information by unauthorised users, to prevent the denial of access to EU classified information to authorised users, and to prevent corruption or unauthorised modification or deletion of EU classified information.

9. COUNTER-SABOTAGE AND CONTROL OF OTHER FORMS OF MALICIOUS WILFUL DAMAGE

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 be asked to provide intelligence regarding espionage, sabotage, terrorism and other subversive activities.

10. RELEASE OF CLASSIFIED INFORMATION TO THIRD STATES OR INTERNATIONAL ORGANISATIONS

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

If the Commission 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 provisions for EU classified information, or such higher standards as may be required by the third party releasing the information. Mutual checks may be arranged.

The above principles shall be implemented in accordance with the detailed provisions set out in Part II, Section 26, and Appendixes 3, 4 and 5.

PART II: THE ORGANISATION OF SECURITY IN THE COMMISSION

11. THE MEMBER OF THE COMMISSION RESPONSIBLE FOR SECURITY MATTERS

The Member of the Commission responsible for security matters shall:

(a) Implement the Commission's security policy;

(b) Consider security problems referred to him by the Commission or its competent bodies;

(c) Examine questions involving changes in the Commission security policy, in close liaison with the National Security (or other appropriate) Authorities of the Member States (hereinafter 'NSA').

In particular, the Member of the Commission responsible for security matters shall be responsible for:

(a) Co-ordinating all matters of security relating to Commission activities;

(b) Addressing to the designated authorities of the Member States requests for the NSA to provide security clearances for personnel employed in the Commission in accordance with Section 20;

(c) Investigating or ordering an investigation into any leakage of EU classified information that, on prima facie evidence, has occurred in the Commission;

(d) Requesting the appropriate security authorities to initiate investigations when a leakage of EU classified information appears to have occurred outside the Commission, and co-ordinating the enquiries when more than one security authority is involved;

(e) Carrying out periodic examinations of the security arrangements for the protection of EU classified information;

(f) Maintaining close liaison with all security authorities concerned in order to achieve overall co-ordination of security;

(g) Keeping the Commission security policy and procedures constantly under review and, as required, preparing appropriate recommendations. In this regard, the Member of the Commission responsible for security matters shall present to the Commission the annual inspection plan prepared by the Commission Security Service.

12. THE COMMISSION SECURITY POLICY ADVISORY GROUP

A Commission Security Policy Advisory Group shall be set up. It shall consist of the Member of the Commission responsible for security matters or his/her delegate, who shall have the chair, and of representatives of the NSA of each Member State. Representatives of other European institutions may also be invited. Representatives of relevant EC and EU decentralised agencies may also be invited to attend when questions concerning them are discussed.

The Commission Security Policy Advisory Group shall meet at the request of its chair or any of its members. The Group shall have the task to examine and assess all relevant security issues, and to present recommendations to the Commission as appropriate.

13. THE COMMISSION SECURITY BOARD

A Commission Security Board shall be set up. It shall consist of the Secretary General, who shall have the chair, and of the Directors General of the Legal Service, Administration and Personnel, External Relations, Justice and Home Affairs and Joint Research Centre and of the Heads of the Internal Audit Service and the Commission Security Office. Other Commission officials may be invited. Its remit is to assess security measures within the Commission and to make recommendations in this domain to the Member of the Commission responsible for security matters.

14. THE COMMISSION SECURITY OFFICE

In order to fulfil the responsibilities mentioned in Section 11 the Member of the Commission responsible for security matters shall have the Commission Security Office at his or her disposal for co-ordinating, supervising and implementing security measures.

The Head of the Commission Security Office shall be the principal adviser to the Member of the Commission responsible for security matters on security matters and shall act as secretary to the Security Policy Advisory Group. In this regard he or she shall direct the updating of the security regulations and co-ordinate security measures with the competent authorities of the Member States and, as appropriate, with international organisations linked to the Commission by security agreements. To that effect, he/she shall act as a liaison officer.

The Head of the Commission Security Office shall be responsible for the accreditation of IT systems and networks within the Commission. The Head of the Commission Security Office shall decide, in agreement with the relevant NSA, on the accreditation of IT systems and networks involving the Commission on the one hand, and on the other hand any other recipient of EU classified information.

15. SECURITY INSPECTIONS

Periodic inspections of the security arrangements for the protection of EU classified information shall be carried out by the Commission Security Office.

The Commission Security Office may be assisted in this task by the security services of other EU institutions holding EUCI or by Member State National Security Authorities [1].

At the request of a Member State an inspection of EUCI can be conducted by its NSA within the Commission, jointly with the Commission Security Service and in mutual agreement.

[1] Without prejudice to the Vienna Convention of 1961 on diplomatic relations and the Protocol on the privileges and immunities of the European Communities of 8 April 1965.

16. CLASSIFICATIONS, SECURITY DESIGNATORS AND MARKINGS

16.1. **Levels of classification** [1]

Information is classified at the following levels (see also, Appendix 2):

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.

EU SECRET: 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.

EU CONFIDENTIAL: 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.

EU RESTRICTED: 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.

No other classifications are permitted.

16.2. **Security designators**

To set limits to the validity of a classification (for classified information signifying automatic downgrading or declassification) an agreed security designator may be used. This designator shall either be 'UNTIL …..(time/date)' or 'UNTIL ….(event)'.

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

Security designators shall only be used in combination with a classification.

16.3. **Markings**

A marking may be used for specifying the field covered by the document or a particular distribution on a need-to-know basis, or (for non-classified information) to signify the end of an embargo.

A marking is not a classification and must not be used in lieu of one.

The ESDP 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.

16.4. **Affixing of classification**

Classification shall be affixed as follows:

(a) On EU RESTRICTED documents, by mechanical or electronic means;

(b) On EU CONFIDENTIAL documents, by mechanical means or by hand or by printing on pre-stamped, registered paper;

(c) On EU SECRET and EU TOP SECRET documents, by mechanical means or by hand.

16.5. **Affixing of security designators**

Security designators shall be affixed directly under the classification, by the same means as those for affixing classifications.

[1] See a comparative table of EU, NATO, WEU and Member States' security classifications in Appendix 1.

17. CLASSIFICATION MANAGEMENT

17.1. **General**

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.

The responsibility for classifying information and for any subsequent downgrading or declassification rests solely with the originator.

Officials and other employees of the Commission shall classify, downgrade or declassify information on instruction from or with the agreement of their Head of department.

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.

The number of persons authorised to originate EU TOP SECRET documents shall be kept to a minimum, and their names kept on a list drawn up by the Commission Security Office.

17.2. **Application of classifications**

The classification of a document shall be determined by the level of sensitivity of its contents in accordance with the definition at Section 16. It is important that classification is correctly and sparingly used. This applies especially to EU TOP SECRET classification.

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

A practical guide for the classification is contained in Appendix 2.

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

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.

Public access shall remain governed by Regulation (EC) No 1049/2001.

17.3. **Downgrading and declassification**

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 originator 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.

If possible, originators shall specify on classified documents a date, period or event 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.

18. PHYSICAL SECURITY

18.1. **General**

The main objectives of physical security measures are to prevent an unauthorised person from gaining access to EU classified information and/or material, to prevent theft and degradation of equipment and other property and to prevent harassment or any other type of aggression of staff, other employees and visitors.

18.2. **Security requirements**

All premises, areas, buildings, 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.

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 (e.g. 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.

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;

(c) Prevent those who do not have a need to know from having access to EU classified information.

18.3. **Physical security measures**

18.3.1. *Security areas*

Areas where information classified EU CONFIDENTIAL 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 EU CONFIDENTIAL 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 EU CONFIDENTIAL 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 Services in which EU CONFIDENTIAL 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 that 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.

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.

18.3.2. *Administrative area*

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 EU RESTRICTED and non-classified information shall be handled and stored in such areas.

18.3.3. *Entry and exit controls*

Entry and exit into and from Class I and Class II security areas shall be controlled by a pass or personal recognition system applicable to all staff normally working in these areas. 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.

18.3.4. *Guard patrols*

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 2 hours.

18.3.5. *Security containers and strong rooms*

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

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

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

— Class C: Service furniture suitable for storage of EU RESTRICTED information only.

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

18.3.6. *Locks*

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 Service furniture only.

18.3.7. *Control of keys and combinations*

Keys of security containers shall not be taken out of the Commission buildings. Combination settings of security containers shall be committed to memory by persons needing to know them. For use in an emergency, the Local Security Officer of the Commission department 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.

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

(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 twelve months.

18.3.8. *Intrusion detection devices*

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.

18.3.9. *Approved equipment*

The Commission Security Office shall maintain up-to-date lists by type and model of the security equipment that they have approved for the protection of classified information under various specified circumstances and conditions. The Commission Security Office shall base these lists, *inter alia*, on information from NSAs.

18.3.10. *Physical protection of copying and telefax machines*

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

18.4. **Protection against overlooking and eavesdropping**

18.4.1. *Overlooking*

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.

18.4.2. *Eavesdropping*

Services or areas in which information classified EU SECRET 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 Commission Security Office after consultation, as necessary, with NSAs.

18.4.3. *Introduction of electronic and recording equipment*

It is not permitted to introduce mobile phones, private computers, recording devices, cameras and other electronic or recording devices into security areas or technically secure areas without prior authorisation from the Head of the Commission Security Office.

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 Commission Security Office may request assistance from experts from NSAs.

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

18.5. **Technically secure areas**

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.

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 general rule, the installation of communication lines in technically secure areas is not permitted without prior authorisation from the appropriate authority.

19. GENERAL RULES ON THE NEED TO KNOW PRINCIPLE AND EU PERSONAL SECURITY CLEARANCES

19.1. **General**

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

The responsibility for determining 'need-to-know' shall rest with the department in which the person concerned is to be employed.

Requesting the clearance of personnel shall be the responsibility of each department.

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

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

Persons other than officials or other employees, such as external contractors, experts or consultants, with whom it may be necessary to discuss, or to whom it may be necessary to show, EU classified information, must have a EU personal security clearance as regards EU classified information and be briefed as to their responsibility for security.

Public access shall remain governed by Regulation (EC) No 1049/2001.

19.2. **Specific rules on access to EU TOP SECRET information**

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

All persons who are required to have access to EU TOP SECRET information shall be designated by the Member of the Commission responsible for security matters and their names kept in the appropriate EU TOP SECRET registry. The Commission Security Office will create and maintain this registry.

Before having access to EU TOP SECRET information, all persons shall sign a certificate to the effect that they have been briefed on Commission security procedures and that they fully understand their special responsibility for safeguarding 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.

In the case of persons having access to 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.

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

19.3. **Specific rules on access to EU SECRET and EU CONFIDENTIAL information**

All persons who are to have access to EU SECRET or EU CONFIDENTIAL information shall first be screened to the appropriate grading.

All persons who are to have access to EU SECRET or EU CONFIDENTIAL information shall be acquainted with the appropriate security provisions and shall be aware of the consequences of negligence.

In the case of persons having access to EU SECRET or EU CONFIDENTIAL 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.

19.4. **Specific rules on access to EU RESTRICTED information**

Persons with access to EU RESTRICTED information will be made aware of these security rules and of the consequences of negligence.

19.5. **Transfers**

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.

When a member of staff is transferred to another post involving the handling of EU classified material the Local Security Officer will brief him accordingly.

19.6. **Special instructions**

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 and with representatives of special interest groups;

(c) The threat presented by the activities of intelligence services that 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.

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.

There are no Commission security provisions concerning private travel to any destination by personnel cleared for access to EU classified information. The Commission Security Office shall, however, acquaint the officials and other servants falling within their responsibility with travel regulations to which they may be subjected.

20. SECURITY CLEARANCE PROCEDURE FOR COMMISSION OFFICIALS AND OTHER EMPLOYEES

(a) Only Officials and other employees of the Commission or persons working within the Commission 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 Commission, shall have access to such information.

(b) In order to have access to information classified as 'EU TOP SECRET', 'EU SECRET' and 'EU CONFIDENTIAL', the persons referred to in paragraph (a) above must have been authorised, in accordance with the procedure referred to in paragraphs (c) and (d) of this Section.

(c) 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 (i) to (n).

(d) The Head of the Commission Security Office shall be responsible for granting the authorisations referred to in paragraphs (a), (b) and (c).

(e) He/she 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 (i) to (n).

(f) The Commission Security Office shall maintain an up to date list of all sensitive posts, provided by the relevant Commission departments, and of all persons who have been granted a (temporary) authorisation.

(g) 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 in accordance with the procedure referred to in paragraph (e).

(h) Authorisation shall be withdrawn by the Head of the Commission Security Office where he/she 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 Head of the Commission Security Office, and to the competent national authority.

(i) Security screening shall be carried out with the assistance of the person concerned and at the request of the Head of the Commission Security Office. The competent national authority for screening is the one of the Member State of which the person subject to authorisation is a national. Where the person concerned is not a national of an EU Member State, the Head of the Commission Security Office will request a security screening from the EU Member State in which the person is domiciled or usually resident.

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

(k) The Head of the Commission Security Office 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.

(l) 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.

(m) Where the competent national authorities of the Member State give a positive opinion, the Head of the Commission Security Office may grant the person concerned authorisation.

(n) A negative opinion by the competent national authorities shall be notified to the person concerned, who may ask to be heard by the Head of the Commission Security Office. Should he consider it necessary, the Head of the Commission Security Office may ask the competent national authorities for any further clarification they can provide. If the negative opinion is confirmed, authorisation shall not be granted.

(o) All persons granted authorisation within the meaning of paragraphs (d) and (e) 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 persons shall sign a declaration acknowledging receipt of the instructions and give an undertaking to obey them.

(p) The Head of the Commission Security Office 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.

(q) Exceptionally, if required by the service, the Head of the Commission Security Office 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 (i).

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

21. PREPARATION, DISTRIBUTION, TRANSMISSION, COURRIER PERSONAL SECURITY AND EXTRA COPIES OF TRANSLATIONS AND EXTRACTS OF EU CLASSIFIED DOCUMENTS

21.1. **Preparation**

1. The EU classifications shall be applied as established in Section 16 and for EU CONFIDENTIAL and above 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 EU TOP SECRET and EU SECRET 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 EU CONFIDENTIAL and above.

2. Documents classified EU CONFIDENTIAL 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.

3. The provisions regulating the computerised production of classified documents are set out in Section 25.

21.2. **Distribution**

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

2. EU TOP SECRET documents shall be circulated through EU TOP SECRET registries (see Section 22.2). In the case of 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.

3. Documents classified EU SECRET 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.

4. Every document classified EU CONFIDENTIAL and above shall, on arriving at or leaving a DG or service, be recorded by the departments' Local EUCI 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 (see Section 22.1).

21.3. **Transmission of EU classified documents**

21.3.1. *Packaging, receipts*

1. Documents classified EU CONFIDENTIAL 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.

2. Only a Registry Control Officer (see Section 22.1), 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 (see Section 22.1) 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.

3. 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.

4. 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.

5. For documents classified EU CONFIDENTIAL and above, couriers and messengers shall obtain receipts against the package numbers.

21.3.2. *Transmission within a building or group of buildings*

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.

21.3.3. *Transmission within a country*

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

2. Whenever a messenger service is used for the transmission of a 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 EU TOP SECRET documents remain under the direct supervision of a responsible official at all times.

3. Exceptionally, 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 EU TOP SECRET documents;

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

   (c) Under no circumstances does the official leave the EU TOP SECRET documents unattended;

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

4. Within a given country, EU SECRET and EU CONFIDENTIAL 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.

5. The Commission Security Office will prepare instructions on the personal carrying of EU classified documents based on these rules. The bearer shall be required to read and sign these instructions. In particular, the instructions shall 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 18;

   (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.

21.3.4. *Transmission from one State to another*

1. Material classified EU CONFIDENTIAL and above shall be conveyed by EU diplomatic or military courier services.

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

3. The Member of the Commission responsible for security matters 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. The Commission Security Office will prepare instructions covering the personal carriage of material classified up to and including EU SECRET internationally by persons other than diplomatic and military couriers. The instructions shall require that:

   (a) The bearer has the appropriate security clearance;

   (b) A record is held in the appropriate department 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 Member 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 rules 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 18;

(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 (e.g. in aircraft, trains, etc.).

4. 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.

21.3.5. *Transmission of EU restricted documents*

No special provisions are laid down for the conveyance of EU RESTRICTED documents, except that they should be such as to ensure that they can not fall into any unauthorised person's hands.

21.4. **Courier personnel security**

All couriers and messengers employed to carry EU SECRET and EU CONFIDENTIAL documents shall be appropriately security cleared.

21.5. **Electronic and other means of technical transmission**

1. 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 25.

2. Only accredited communications centres and networks and/or terminals and systems may transmit information classified EU CONFIDENTIAL and EU SECRET.

21.6. **Extra copies and translations of and extracts from EU classified documents**

1. Only the originator may authorise the copy or translation of EU TOP SECRET documents.

2. If persons without EU TOP SECRET clearance require information which, although contained in a EU TOP SECRET document, does not have that classification, the Head of the EU TOP SECRET Registry (see Section 22.2) 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.

3. Documents classified EU SECRET and lower may be reproduced and translated by the addressee, within the framework of these security provisions 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.

22. EUCI REGISTRIES, MUSTERS, CHECKS, ARCHIVE STORAGE AND DESTRUCTION OF EUCI

22.1. **Local EUCI Registries**

1. Within the Commission, in each department, as required, one or more Local EUCI Registries shall be responsible for the registration, reproduction, dispatch, archiving and destruction of documents classified EU SECRET and EU CONFIDENTIAL.

2. When a department does not have a Local EUCI Registry, the Local EUCI Registry of Secretariat General will act as its EUCI Registry.

3. Local EUCI Registries shall report to the Head of department from whom they receive their instructions. The Head of these registries shall be Registry Control Officer (RCO).

4. They shall be subject to the supervision of the Local Security Officer as far as the application of the provisions regarding the handling of EUCI documents and compliance with the corresponding security measures is concerned.

5. Officials assigned to the Local EUCI Registries shall be authorised to have access to EUCI in accordance with Section 20.

6. Under the authority of the relevant Head of department the Local EUCI Registries 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.

7. The Local EUCI Registries shall keep a register of the following particulars:

   (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 department;

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

8. The general rules provided for in Section 21 shall apply to the Local EUCI Registries of the Commission, unless modified by the specific rules laid down in this Section.

22.2. **The EU TOP SECRET Registry**

22.2.1. *General*

1. A Central EU TOP SECRET Registry ensures the recording, handling and distribution of EU TOP SECRET documents in accordance with these security provisions. The head of the EU TOP SECRET Registry will be the EU TOP SECRET Registry Control Officer.

2. The Central EU TOP SECRET Registry will act as the main receiving and despatching authority in the Commission, with other EU institutions, Member States, international organisations and third States with which the Commission has agreements on security procedures for the exchange of classified information.

3. When necessary, sub-registries shall be established, to be responsible for the internal management of EU TOP SECRET documents; they shall keep up-to-date records of the circulation of each document held on the Sub-Registry's charge.

4. EU TOP SECRET sub-registries shall be set up as specified in Section 22.2.3 in response to long term needs and shall be attached to a central EU TOP SECRET Registry. If there is a need to consult EU TOP SECRET documents only temporarily and occasionally, these documents may be released without setting up a EU TOP SECRET sub-registry, provided rules are laid down to ensure that they remain under the control of the appropriate EU TOP SECRET registry and that all physical and personnel security measures are observed.

5. Sub-registries may not transmit EU TOP SECRET documents directly to other sub-registries of the same Central EU TOP SECRET Registry without express approval by the latter.

6. All exchanges of EU TOP SECRET documents between sub-registries not attached to the same central registry shall be routed through the Central EU TOP SECRET Registries.

22.2.2. *The Central EU TOP SECRET Registry*

As the Control Officer, the head of the Central EU TOP SECRET Registry shall be responsible for:

(a) The transmission of EU TOP SECRET documents in accordance with the provisions defined in Section 21.3;

(b) Maintaining a list of all its dependent 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 EU TOP SECRET documents distributed by the Central Registry;

(d) Maintaining a record of EU TOP SECRET documents held and distributed;

(e) Maintaining an up-to-date list of all Central 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 EU TOP SECRET documents held within the registry in accordance with regulations contained in Section 18.

22.2.3. *EU TOP SECRET sub-registries*

As the Control Officer, the head of an EU TOP SECRET sub-registry shall be responsible for:

(a) The transmission of EU TOP SECRET documents in accordance with provisions contained in Section 21.3;

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

(c) The distribution of 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 EU TOP SECRET documents held or circulating under his control or which have been passed to other EU TOP SECRET registries and holding all corresponding receipts;

(e) Maintaining an up-to-date list of EU TOP SECRET registries with whom he is authorised to exchange EU TOP SECRET documents, together with the names and signatures of their Control Officers and authorised deputies;

(f) The physical safeguarding of all EU TOP SECRET documents held within the sub-registry in accordance with the rules laid down in Section 18.

22.3. **Inventories, musters and checks of EU classified documents**

1. Every year, each EU TOP SECRET Registry as referred to in this Section shall carry out an itemised inventory of EU TOP SECRET documents. A document is deemed to have been accounted for if the registry physically musters the document, or holds a receipt from the 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. They shall forward the findings of the annual inventories to the Member of the Commission responsible for security matters, by 1 April each year at the latest.

2. EU TOP SECRET Sub-registries shall forward the findings of their annual inventory to the Central Registry to which they are answerable, on a date specified by the latter.

3. EU classified documents below the level of EU TOP SECRET shall be subject to internal checks according to instructions from the Member of the Commission responsible for security matters.

4. 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.

22.4. **Archive storage of EU classified information**

1. EUCI shall be stored under conditions that comply with all relevant requirements listed in Section 18.

2. To minimise storage problems, the Control Officers of all registries shall be authorised to have EU TOP SECRET, EU SECRET and EU CONFIDENTIAL 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 EU TOP SECRET document is reported to the originator;

   (d) Rolls of film, or other type of support, contain only documents of the same EU TOP SECRET, EU SECRET or EU CONFIDENTIAL classification;

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

   (f) Original documents that have been microfilmed or otherwise stored are destroyed, in accordance with the rules set out in Section 22.5.

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

22.5. **Destruction of EU classified documents**

1. 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) 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 EU TOP SECRET Control Officer and by the Officer witnessing the destruction, who shall be 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) EU TOP SECRET documents, including all classified waste resulting from the preparation of EU TOP SECRET documents such as spoiled copies, working drafts, typed notes, floppy disks, shall be destroyed, under the supervision of a EU TOP SECRET Registry Control Officer, by burning, pulping, shredding or otherwise reducing into an unrecognisable and non-reconstitutable form.

2. EU SECRET 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 1 (c). EU SECRET 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.

3. EU CONFIDENTIAL 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 1 (c). Their destruction shall be recorded according to instructions from the Member of the Commission responsible for security matters.

4. EU RESTRICTED documents shall be destroyed by the registry responsible for those documents or by the user, in accordance with instructions from the Member of the Commission responsible for security matters.

22.6. **Destruction in emergencies**

1. The Commission departments 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. It shall promulgate instructions deemed necessary to prevent EU classified information from falling into unauthorised hands.

2. The arrangements for the safeguarding and/or destruction of EU SECRET and EU CONFIDENTIAL material in a crisis shall under no circumstances adversely affect the safeguarding or destruction of EU TOP SECRET material, including the enciphering equipment, whose treatment shall take priority over all other tasks.

3. The measures to be adopted for the safeguarding and destruction of enciphering equipment in an emergency shall be covered by specific instructions.

4. Instructions need to be available on the spot in a sealed envelope. Means/tools for destruction must be available.

23. SECURITY MEASURES FOR SPECIFIC MEETINGS HELD OUTSIDE THE COMMISSION PREMISES AND INVOLVING EU CLASSIFIED INFORMATION

23.1. **General**

When Commission or other important meetings are held outside the Commission premises 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 shall be taken. These measures concern only the protection of EU classified information; other security measures may have to be planned.

23.2. **Responsibilities**

23.2.1. *The Commission Security Office*

The Commission Security Office shall cooperate with the competent authorities of the Member State on whose territory the meeting is being held (the host Member State), in order to ensure the security of the Commission's or other important meetings and for the security of the 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 Commission's communications system for the receipt and transmission of EU classified messages. The host Member State will be requested to provide access if required to secure telephone systems.

The Commission Security Office shall 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 (MSO) and delegations as necessary.

Each delegation to a meeting shall be asked to 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 Commission Security Office representative as required.

23.2.2. *Meeting Security Officer (MSO)*

A Meeting Security Officer shall 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 the MSO shall in general relate to:

(a) 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;

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

(c) Constant coordination with the competent authorities of the host Member State and with the Commission Security Office;

(d) The inclusion of security instructions in the meeting dossier with due regard for the requirements set out in these security rules and any other security instructions considered necessary

23.3. **Security measures**

23.3.1. *Security areas*

The following security areas shall be established:

(a) A Class II security area, consisting of a drafting room, the Commission 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.

23.3.2. *Passes*

The MSO shall 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.

The security instructions for the meeting shall 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.

Apart from badge-holding participants, as few people as possible shall be admitted to the meeting place. The MSO shall only allow national delegations to receive visitors during the meeting upon their request. 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 shall be filled in. Visitors shall be accompanied at all times by a security guard or by the person being visited. The visitor's pass form shall 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.

23.3.3. *Control of photographic and audio equipment*

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 MSO.

23.3.4. *Checking of briefcases, portable computers and packages*

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 MSO considers it necessary, more stringent measures for the inspection of briefcases and packages may be laid down.

23.3.5. *Technical security*

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

23.3.6. *Delegations' documents*

Delegations shall be made responsible for taking EU classified documents to and from meetings. They shall 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.

23.3.7. *Safe custody of documents*

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

23.3.8. *Inspection of offices*

The Meeting Security Officer shall arrange for the Commission 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/she shall take the appropriate measures.

23.3.9. *Disposal of EU classified waste*

All waste shall be treated as EU classified, and waste-paper baskets or bags should be given to the Commission and delegations for its disposal. Before leaving the premises they have been assigned, the Commission and delegations shall take their waste to the Meeting Security Officer, who shall arrange for its destruction according to the rules.

At the end of the meeting, all documents held but no longer wanted by the Commission or delegations shall be treated as waste. A thorough search of Commission and delegations' premises shall be made before the security measures adopted for the meeting are lifted. Documents for which a receipt was signed shall, as far as applicable, be destroyed as prescribed in Section 22.5.

24. BREACHES OF SECURITY AND COMPROMISE OF EU CLASSIFIED INFORMATION

24.1. **Definitions**

A breach of security occurs as the result of an act or omission contrary to a Commission security provision that might endanger or compromise EU classified information.

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.

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.

24.2. **Reporting breaches of security**

All persons who are required to handle EU classified information shall be thoroughly briefed on their responsibilities in this domain. They shall report at once any breach of security that may come to their notice.

When a Local Security Officer or Meeting Security Officer discovers or is informed of a breach of security relating to EU classified information or of the loss or disappearance of EU classified material, he or she shall take timely action in order to:

(a) Safeguard evidence;

(b) Establish the facts;

(c) Assess and minimise the damage done;

(d) Prevent a recurrence;

(e) 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.

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 to the Commission Security Office.

Cases involving EU RESTRICTED information need to be reported only when they present unusual features.

On being informed that a breach of security has occurred, the Member of the Commission responsible for security matters 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 shall also be reported.

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

24.3. **Legal action**

Any individual who is responsible for compromising EU classified information shall be liable to disciplinary action according to the relevant rules and regulations, particularly title VI of the Staff Regulations. Such action shall be without prejudice to any further legal action.

In appropriate cases, on the basis of the report mentioned in Section 24.2, the Member of the Commission responsible for security matters shall take all necessary steps in order to allow the competent national authorities to start criminal law procedures.

25. PROTECTION OF EU CLASSIFIED INFORMATION HANDLED IN INFORMATION TECHNOLOGY AND COMMUNICATIONS SYSTEMS

25.1. **Introduction**

25.1.1. *General*

The security policy and requirements shall apply to all communications and information systems and networks (hereinafter systems) handling information classified EU CONFIDENTIAL and above. They shall be applied as a supplement to Commission Decision C (95) 1510 final of 23 November 1995 on the protection of informatics systems.

Systems handling EU RESTRICTED 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 IT security policy applied by the Commission has the following elements:

— It forms an integral part of security in general, and complements all elements of information security, personnel security and physical security;

— Division of responsibilities between technical system owners, owners of EUCI stored or handled in technical systems, IT security specialists and users;

— Description of security principles and requirements of each IT system;

— Approval of these principles and requirements by a designated authority;

— Taking into account the specific threats and vulnerabilities in the IT area.

25.1.2. *Threats to, and vulnerabilities of systems*

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.

EU classified and unclassified information handled in systems in a concentrated form designed for rapid retrieval, communication and use is vulnerable to many threats. 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.

25.1.3. *Main purpose of security measures*

The main purpose of the security measures stated in this section is to provide protection against unauthorised disclosure of EU classified 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 by the Commission Security Office, along with appropriate special security procedures and techniques particularly designed for each system.

25.1.4. *System-specific security requirement statement (SSRS)*

For all systems handling information classified EU CONFIDENTIAL and above, a System-specific security requirement statement (SSRS) shall be required to be produced by its Technical System Owner (TSO, see Section 25.3.4) and the Information Owner (see Section 25.3.5) in cooperation with input and assistance as required from the project staff and from the Commission Security Office (as INFOSEC Authority -IA, see Section 25.3.3) and approved by the Security Accreditation Authority (SAA, see Section 25.3.2).

An SSRS shall also be required where the availability and integrity of the EU RESTRICTED or unclassified information is deemed critical by the Security Accreditation Authority (SAA).

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.

25.1.5. *Security modes of operation*

All systems handling information classified EU CONFIDENTIAL 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.

25.2. **Definitions**

'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.

'Central Information Security Officer' (CISO) shall mean the official in a central IT service who coordinates and supervises security measures for centrally organised systems.

'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.

'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.

'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.

'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.

'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.

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

'Information Owner' (IO) shall mean the authority (Head of department) that has the responsibility for creating, processing and the use of information, including for deciding who shall be allowed to access this information.

'Information Security' (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.

'IT Area' shall mean: an area that 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.

'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.

'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.

'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 TSO.

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

'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.

'Local Informatics Security Officer' (LISO) shall mean the official in a Commission department who is responsible for coordinating and supervising security measures within his domain.

'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.

'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.

'Security Operating Procedures' shall mean the procedures produced by the Technical Systems Owner defining the principles to be adopted on security matters, the operating procedures to be followed and personnel responsibilities.

'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.

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.

'A System Specific Security Requirement Statement' (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 Commission 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.

'Technical Systems Owner' (TSO) shall mean the authority responsible for the creation, maintenance, operation and closing down of a system.

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

25.3. **Security responsibilities**

25.3.1. *General*

The advisory responsibilities of the Commission Security Policy Advisory Group, defined in Section 12, include INFOSEC issues. This Group shall organise its activities in such a way that it can provide expert advice on the above issues.

The Commission Security Office shall be responsible for issuing detailed INFOSEC provisions, based on the provisions in this chapter.

In case of problems regarding security (incidents, breaches, etc.), immediate action shall be taken by the Commission Security Office.

The Commission Security Office shall have an INFOSEC Unit.

25.3.2. *The Security accreditation authority (SAA)*

The Head of the Commission Security Office shall be the Security Accreditation Authority (SAA) for the Commission. The SAA is responsible in the general area of security and in the specialised areas of INFOSEC, Communication security, Crypto security and Tempest security.

The SAA shall be responsible for ensuring the compliance of systems with the Commission'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.

The jurisdiction of the Commission SAA shall cover all systems in operation within the premises of the Commission. When different components of a system come under the jurisdiction of the Commission SAA and other SAAs, all parties concerned may appoint a joint accreditation board under the coordination of the Commission SAA.

25.3.3. *The INFOSEC Authority (IA)*

The Head of the Commission Security Office INFOSEC Unit is the INFOSEC Authority for the Commission. 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 rules 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.

25.3.4. *The Technical Systems Owner (TSO)*

The responsibility for the implementation and operation of controls and special security features of a system lies with the owner of that system, the Technical Systems Owner (TSO). For centrally owned systems a Central Informatics Security Officer (CISO) shall be nominated. Each department shall, as appropriate, nominate a Local Informatics Security Officer (LISO). The responsibility of a TSO includes the creation of the Security Operating Procedures (SecOPs) and extends throughout the life cycle of a system from the project concept stage to final disposal.

The TSO shall specify the security standards and practices to be met by the supplier of the system.

The TSO may delegate a part of its responsibilities where appropriate to a Local Informatics Security Officer. A single person may perform the various INFOSEC functions.

25.3.5. *The Information Owner (IO)*

The Information Owner (IO) shall be responsible for EUCI (and other information) that is to be introduced, processed and produced in technical systems. He shall define the requirements for access to this information in systems. He may delegate this responsibility to an Information Manager or to a Database Manager within his domain.

25.3.6. *Users*

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

25.3.7. *INFOSEC training*

INFOSEC education and training shall be available to all staff needing it.

25.4. **Non technical security measures**

25.4.1. *Personnel security*

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 Commission procedures.

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

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.

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 or other employee.

The security settings of a system shall only be changed by at least two authorised personnel working in conjunction.

25.4.2. *Physical security*

IT and remote terminal/workstation areas (as defined in Section 25.2) in which information classified EU CONFIDENTIAL 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, as appropriate.

25.4.3. *Control of access to a system*

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.

When no longer used for this purpose, the access control information and material shall be destroyed pursuant to the provisions in Section 25.5.4.

25.5. **Technical security measures**

25.5.1. *Security of information*

It shall be incumbent upon the originator of the information to identify and classify all information-bearing documents, whether they are 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.

It shall be incumbent upon the Commission departments and their 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.

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.

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.

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.

Re-usable 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 in accordance with a procedure approved by the SAA (see 25.5.4).

25.5.2. *Control and accountability of information*

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

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.

Where output is generated from a system handling EU classified information, and transmitted to a remote terminal/workstation area from an IT area, procedures, agreed by the SAA shall be established for controlling and logging the output. For EU SECRET and above, such procedures shall include specific instructions for accountability of the information.

25.5.3. *Handling and control of removable computer storage media*

All removable computer storage media classified EU CONFIDENTIAL 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.

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 rules.

25.5.4. *Declassification and destruction of computer storage media*

Computer storage media used for recording EU classified information may be downgraded or declassified in accordance with a procedure to be approved by the SAA.

Computer storage media that have held EU TOP SECRET or special category information shall not be declassified and reused.

If computer storage media cannot be declassified or is not reusable, it shall be destroyed in accordance with the above mentioned procedure.

25.5.5. *Communications security*

The Head of the Commission Security Office is the Crypto Authority.

When EU classified information is transmitted electro-magnetically, 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.

When cryptographic methods are required to provide confidentiality, integrity and availability such methods and its associated products shall be specifically approved for the purpose by the SAA as Crypto Authority.

During transmission, the confidentiality of information classified EU SECRET and above shall be protected by cryptographic methods or products approved by the Member of the Commission responsible for security matters after having consulted the Commission Security Policy Advisory Group. During transmission, the confidentiality of information classified EU CONFIDENTIAL or EU RESTRICTED shall be protected by cryptographic methods or products approved by the Commission Crypto Authority after having consulted the Commission Security Policy Advisory Group.

Detailed rules applicable to the transmission of EU classified information shall be set out in specific security instructions approved by the Commission Security Office after having consulted the Commission Security Policy Advisory Group.

Under exceptional operational circumstances, information classified EU RESTRICTED, EU CONFIDENTIAL and EU SECRET may be transmitted in clear text provided each occasion is explicitly authorised and duly registered by the Information Owner. 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.

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.

25.5.6. *Installation and radiation security*

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.

Systems handling information classified EU CONFIDENTIAL and above shall be protected in such a way that their security cannot be threatened by compromising emanations and or conductivity, the study and control of which is referred to as 'Tempest'.

Tempest countermeasures shall be reviewed and approved by the Tempest authority (see 25.3.2).

25.6. **Security during handling**

25.6.1. *Security operating procedures (SecOPs)*

Security Operating Procedures (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 Technical Systems Owner (TSO).

25.6.2. *Software protection/configuration management*

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 shall be verified at regular intervals to ensure their integrity and correct functioning.

New or modified versions of software shall not be used for the handling of EU classified information until verified by the TSO.

25.6.3. *Checking for the presence of malicious software/computer viruses*

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

All computer storage media arriving in the Commission shall be checked for the presence of any malicious software or computer viruses, before being introduced into any system.

25.6.4. *Maintenance*

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 an IT area.

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.

25.7. **Procurement**

25.7.1. *General*

Any security product to be used with the system to be procured shall either have been evaluated and certified, or currently be under evaluation and certification by an appropriate Evaluation or Certification body of one of the EU Member States against internationally acknowledged criteria (such as the Common Criteria for Information Technology Security Evaluation, re ISO 15408). Specific procedures are required to obtain ACPC approval.

In deciding whether equipment, particularly computer storage media, should be leased rather than purchased, it shall 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.

25.7.2. *Accreditation*

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

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

25.7.3. *Evaluation and certification*

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.

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

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 TSO.

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.

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.

25.7.4. *Routine checking of security features for continued accreditation*

The TSO shall establish routine control procedures that shall ensure that all security features of the system are still valid.

The types of change that would give rise to re-accreditation, or requiring the prior approval of the SAA, shall be clearly identified and stated in the SSRS. After any modification, repair or failure that could have affected the security features of the system, the TSO 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.

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 EU TOP SECRET the inspections shall be carried out not less than once annually.

25.8. **Temporary or occasional use**

25.8.1. *Security of microcomputers/personal computers*

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.

This 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).

25.8.2. *Use of privately-owned IT equipment for official Commission work*

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.

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 written authorisation of the Head of the Commission Security Office. This authorisation can only be provided for technical reasons in exceptional cases.

25.8.3. *Use of contractor-owned or nationally-supplied IT equipment for official Commission work*

The use of contractor-owned IT equipment and software in organisations in support of official Commission work may be permitted by the Head of the Commission Security Office. The use of nationally-provided IT equipment and software may also be permitted; in this case, the IT equipment shall be brought under the control of the appropriate Commission inventory. In either case, if the IT equipment is to be used for handling EU classified information, then the 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.

26. RELEASE OF EU CLASSIFIED INFORMATION TO THIRD STATES OR INTERNATIONAL ORGANISATIONS

26.1.1. *Principles regulating the release of EU classified information*

The Commission as a college shall decide on release of EU classified information to third States or international organisations on the basis of:

— The nature and content of such information;

— The recipients' need to know;

— The measure of advantages to EU.

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

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 Commission Security Policy Advisory Group will give the Commission its technical opinion on this point.

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 Commission.

26.1.2. *Levels*

Once the Commission 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.

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.

Each level of cooperation shall determine the procedures and security provisions, detailed in Appendices 3, 4, and 5.

26.1.3. *Security agreements*

Once the Commission has decided that there is a permanent or long-term need for the exchange of classified information between the Commission 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.

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 EU RESTRICTED.

Draft agreements on security procedures or memoranda of understanding, shall be discussed by the Commission Security Policy Advisory Group before they are presented to the Commission for a decision.

The Member of the Commission responsible for security matters shall request all necessary assistance from Member State NSA's 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.

Appendix 1

COMPARISON OF NATIONAL SECURITY CLASSIFICATIONS

EU classification	EU TOP SECRET	EU SECRET	EU CONFIDENTIAL	EU RESTRICTED
NATO classification ([1])				
WEU classification	Focal Top Secret	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
EURATOM classification ([2])	EURATOM Top Secret	EURATOM SECRET	EURATOM Confidential	EURATOM Restricted
Belgium	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Denmark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Germany	STRENG GEHEIM	GEHEIM	VS ([3]) — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Greece	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Spain	Secreto	Reservado	Confidencial	Difusión limitada
France	Très Secret Défense ([4])	Secret Défense	Confidentiel Défense	Diffusion restreinte
Ireland	Top Secret	Secret	Confidential	Restricted
Italy	Segretissimo	Segreto	Riservatissimo	Riservato
Luxembourg	Très Secret	Secret	Confidentiel	Diffusion restreinte
Netherlands	Stg. Zeer Geheim	Stg. Geheim	Stg. Confidentieel	
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Finland	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Sweden	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
United Kingdom	Top Secret	Secret	Confidential	Restricted

([1]) NATO — correspondence with NATO classification levels will be established when the Security Agreement between the Commission and NATO is negotiated.
([2]) Euratom Regulation Number 3 of 31 July 1958 on the protection of Euratom classified information.
([3]) Germany: VS = Verschlusssache.
([4]) France: the classification 'Très Secret Défense', which covers governmental priority issues, may be changed only with the Prime Minister's authorisation.

Appendix 2

PRACTICAL CLASSIFICATION GUIDE

This guide is indicative and may not be construed as modifying the substantial provisions laid down in Sections 16, 17, 20 and 21.

Classification	When	Who	Affixing	Downgrading/declassification/destruction	
				Who	When
EU TOP SECRET: This classification shall be applied only to infomation 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 [16.1].	The compromise of assets classified EU TOP SECRET would be likely to: — Threaten directly the internal stability of the EU or one of its Member States 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.	Duly authorised persons (originators), Directors General, Heads of Service [17.1] Originators shall specify a date, period or event when the contents may be downgraded or declassified. [16.2] Otherwise they shall keep the documents under review every five years at the latest, in order to ensure that the original classification is necessary [17.3].	The classification EU TOP SECRET shall be affixed to EU TOP SECRET documents, and where applicable a security designator, and/or the defence marking — ESDP, by mechanical means and by hand [16.4, 16.5, 16.3]. The EU classifications and security designators 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 [21.1].	Declassification or downgrading rests solely with the originator, who shall inform of the change any subsequent addressees to whom he has sent or copied the document [17.3]. EU TOP SECRET documents shall be destroyed by the Central Registry or sub-registry responsible for them. Each document destroyed shall be listed in a destruction certificate, signed by the EU TOP SECRET Control Officer and by the Officer witnessing the destruction, who shall be 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 distributions sheet, for a period of ten years [22.5].	Surplus copies and documents no longer needed must be destroyed [22.5]. EU TOP SECRET documents, including all classified waste resulting from the preparation of EU TOP SECRET documents such as spoiled copies, working drafts, typed notes and carbon paper, shall be destroyed, under the supervision of a EU TOP SECRET Control Officer, by burning, pulping, shredding or otherwise reducing into an unrecognisable and non-reconstitutable form [22.5].

Classification	When	Who	Affixing	Downgrading/declassification/destruction	
				Who	When
EU SECRET: 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 [16.1].	The compromise of assets classified EU SECRET would be liked to: — 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.	Authorised persons (originators), Directors General, Heads of Service [17.1]. Originators shall specify a date period when the contents may be downgraded or declassified. [16.2] Otherwise they shall keep the documents under review every five years at the latest, in order to ensure that the original classification is necessary [17.3].	The classification EU SECRET shall be affixed to EU SECRET documents, and where applicable a security designator and/or the defence marking — ESDP, by mechanical means and by hand [16.4, 16.5, 16.3]. The EU classifications and security designators 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 [21.1].	Declassification and downgrading rests soley with the originator, who shall inform of the change any subsequent addressees to whom he has sent or copied the document [17.3]. EU SECRET documents shall be destroyed by the registry responsible for those documents, under the supervision of a security cleared person. EU SECRET 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 [22.5].	Surplus copies and documents no longer needed must be destroyed [22.5]. EU SECRET documents, including all classified waste resulting from the preparation of EU SECRET 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 [22.5].

Classification	When	Who	Affixing	Downgrading/declassification/destruction	
				Who	When
EU CONFIDENTIAL: This classification shall be applied to information and material the unauthorised disclosure of which would harm the essential interests of the European Union or of one or more of its Member States [16.1].	The compromise of assets classified EU CONFIDENTIAL 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 contributors' 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.	Authorised persons (originators), Directors General and Heads of Service [17.1]. 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 [17.3].	The classification EU CONFIDENTIAL shall be affixed to EU CONFIDENTIAL documents, and where applicable a security designator and/or the defence-marking — ESDP introduced, by mechanical means and by hand or by printing on pre-stamped, registered paper [16.4, 16.5, 16.3]. 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 reference number and a date. All annexes and enclosures shall be listed on the first page [21.1].	Declassification and downgrading rests solely with the originator, who shall inform of the change any subsequent addressees to whom he has sent or copied the document [17.3]. EU CONFIDENTIAL documents shall be destroyed by the registry responsible for those documents, under the supervision of a cleared person. Their destruction shall be recorded in accordance with national regulations and, in the case of Commission or EU decentralised agencies, according to instructions from the President [22.5].	Surplus copies and documents no longer needed must be destroyed [22.5]. EU CONFIDENTIAL documents, including all classified waste resulting from the preparation of EU CONFIDENTIAL 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 [22.5].

Classification	When	Who	Affixing	Downgrading/declassification/destruction	
				Who	When
EU RESTRICTED: 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 [16.1].	The compromise of assets classified EU RESTRICTED 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 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.	Authorised persons (originators), Directors General, Heads of Service [17.1]. Originators shall specify a date, period or event when the contents may be downgraded or declassified [16.2]. Otherwise they shall keep the documents under review every five years at the latest, in order to ensure that the original classification is necessary [17.3].	The classification EU RESTRICTED shall be affixed to EU RESTRICTED documents, and where applicable a security designator and/or the defence marking — ESDP, by mechanical or electronic means [16.4, 16.5, 16.3]. The EU classification and security designators shall appear at the top of the first page, and each page shall be numbered. Each document shall bear a reference number and a date [21.1].	Declassification rests solely with the originator, who shall inform of the change any subsequent addressees to whom they have sent or copied the document [17.3]. EU RESTRICTED documents shall be destroyed by the registry responsible for the document or by the user, according to instructions from the President [22.5].	Surplus copies and documents no longer needed must be destroyed [22.5].

Appendix 3

Guidelines for the 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 members of the European Union or to other international organisations, whose security policy and regulations are comparable to EU's, lies with the Commission as a college.

2. Pending the conclusion of a security agreement, the Member of the Commission responsible for security matters is competent to examine requests for the release of EU classified information.

3. In doing so he/she:

   — Shall seek the opinions of the originators of the EUCI 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 provisions are such as to guarantee that the classified information released will be protected in accordance with these security provisions;

   — Shall seek the opinion of the Commission Security Policy Advisory Group as to the confidence that can be placed in the beneficiary States or international bodies.

4. The Member of the Commission responsible for security matters shall forward the request and the Commission Security Policy Advisory Group's opinion to the Commission for a decision.

SECURITY PROVISIONS TO BE APPLIED BY BENEFICIARIES

5. The Member of the Commission responsible for security matters shall notify the beneficiary States or international organisations of the Commission's decision to authorise the release of EU classified information.

6. The decision to release shall come into force only when the beneficiaries have given a written assurance that they will:

   — Use the information for no other than the agreed purposes;

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

7. Personnel

   (a) The number of officials having access to the EU classified information shall 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 EU CONFIDENTIAL 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.

8. Transmission of documents

   (a) The practical procedures for the transmission of documents shall be decided by agreement. Pending the conclusion of such an agreement the provisions of Section 21 apply. The agreement shall 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 Commission includes EU TOP SECRET, the beneficiary State or international organisation shall set up a central EU registry and, if necessary, EU sub-registries. These registries shall apply strictly equivalent provisions as those of Section 22 of these security provisions.

9. Registration

   As soon as a registry receives a EU document classified EU CONFIDENTIAL or above, it shall 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 shall be destroyed in accordance with the instructions set out in Section 22 of these security provisions. Copies of the destruction certificates for EU SECRET and EU TOP SECRET documents shall be sent to the EU registry that has forwarded the documents.

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

11. Protection of documents

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

12. Copies, translations and extracts

No photocopies or translation shall be made of a document classified EU CONFIDENTIAL or EU SECRET, or extracts taken, without the authorisation of the head of the security organisation concerned, who shall register and check those copies, translations or extracts and stamp them as necessary.

The reproduction or translation of a EU TOP SECRET document shall be authorised only by the originating authority, which shall specify the number of copies authorised; if the originating authority cannot be determined, the request shall be referred to the Commission Security Service.

13. Breaches of security

When a breach of security involving a EU classified document has taken place or is suspected, the following action shall 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 Commission Security Office, the relevant 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 Commission Security Office to prevent a recurrence.

14. Inspections

The Commission Security Office shall 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 shall submit a yearly report, by a date specified when the authorisation to release the information is given, confirming that these security provisions have been complied with.

Appendix 4

Guidelines for the 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 originator. The authority to release EUCI created within the Commission lies with the Commission as a college.

2. In principle, it is restricted to information classified up to and including EU SECRET; it excludes classified information protected by special security designators or markings.

3. Pending the conclusion of a security agreement, the Member of the Commission responsible for security matters is competent to examine requests for the release of EU classified information.

4. In doing so he/she:
   — Shall seek the opinions of the originators of the EUCI to be released;
   — Shall establish the necessary contacts with the security bodies of the beneficiary States or international organisations to find out information on their security policy and provisions, 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 Commission Security Policy Advisory Group or, under a silent procedure if necessary, enquire from the member States' National Security Authorities with a view to obtaining the Commission Security Policy Advisory Group's opinion.

5. The Commission Security Policy Advisory Group's opinion shall 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 (providing expurgated versions of a text, for example) and documents transmitted (retaining or deleting EU classification headings, specific markings, etc.);
   — Downgrading or declassification before the information is released to the beneficiary countries or international organisations.

6. The Member of the Commission responsible for security matters shall forward the request and the Commission Security Policy Advisory Group's opinion to the Commission for a decision.

SECURITY RULES TO BE APPLIED BY BENEFICIARIES

7. The Member of the Commission responsible for security matters shall notify the beneficiary States or international organisations of the Commission's decision to authorise the release of EU classified information and of its restrictions.

8. The decision to release shall come into force only when the beneficiaries have given a written assurance that they will:
   — Use the information for no other than the agreed purposes;
   — Protect the information in accordance with the provisions laid down by the Commission.

9. The following rules of protection shall apply unless the Commission, having obtained the Commission Security Policy Advisory Group's technical opinion, decides on a particular procedure for the handling of EU classified documents (deleting mention of the EU classification, specific marking, etc.).

10. Personnel

   (a) The number of officials having access to EU classified information shall 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 the Commission shall have a national security clearance or authorisation for access, to an appropriate level equivalent to that of the EU, as defined in the comparative table;

   (c) These national security clearances or authorisations shall be forwarded to the President for information.

11. Transmission of documents

The practical procedures for the transmission of documents shall be decided by agreement. Pending the conclusion of such an agreement the provisions of Section 21 shall apply. The agreement shall in particular specify the registries to which EU classified information is to be forwarded and the precise addresses to which the documents shall be forwarded as well as the courier or mail services used for the transmission of the EU classified information.

12. 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 Commission, or the security bureau of the recipient international organisation, shall open a special register to record EU classified information on its receipt. The Register shall 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.

13. Return of documents

When the recipient returns a classified document to the Commission, it shall proceed as indicated in the paragraph 'Transmission of documents' above.

14. Protection

(a) When the documents are not in use, they shall be stored in a security container that is approved for the storage of nationally-classified material of the same classification. The container shall bear no indication of its contents, which shall be accessible only to persons authorised to handle EU classified information. Where combination locks are used, the combination shall be known only to those officials in the State or organisation having authorised access to the EU classified information stored in the container and shall 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 shall be removed from the security container only by those officials cleared for access to the EU classified documents and having need-to-know. They shall 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 shall also ensure that the documents are stored in a security container when they have finished consulting them and outside working hours.

(c) No photocopies shall be made of a document classified EU CONFIDENTIAL or above, nor extracts taken, without the authorisation of the Commission Security Office.

(d) The procedure for the rapid and total destruction of the documents in an emergency shall be defined and confirmed with the Commission Security Office.

15. 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.

16. Breaches of security

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

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

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

17. Inspections

The Commission Security Office shall 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.

18. Reporting

Subject to the conclusion of a security agreement, as long as the State or international 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 provisions have been complied with.

Appendix 5

Guidelines for the release of EU classified information to third States or international organisations: Level 3 cooperation

PROCEDURES

1. From time to time, the Commission may wish to cooperate in certain special circumstances with States or organisations that cannot give the assurances required by these security rules, but that cooperation may call for the release of EU classified information.

2. 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 originator. The authority to release EUCI created within the Commission lies with the Commission as a college.

   In principle, it is restricted to information classified up to and including EU SECRET; it excludes classified information protected by special security designators or markings.

3. The Commission shall 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.

4. If the Commission is in favour, the Member of the Commission responsible for security matters
   — Shall seek the opinions of the originators of the EUCI to be released;
   — Shall arrange for a meeting of the Commission Security Policy Advisory Group or, under a silent procedure if necessary, enquire from the Member States' National Security Authorities with a view to obtaining the Commission Security Policy Advisory Group's opinion.

5. The Commission Security Policy Advisory Group's opinion shall be on the following:

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

   (b) The level of classification of the information that may be released;

   (c) Downgrading or declassification before the information is released;

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

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

6. The documents released to the States or organisations covered in this Appendix shall, in principle, be prepared without reference to the source or an EU classification. The Commission Security Policy Advisory Group 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.

7. The President shall forward the Commission Security Policy Advisory Group's opinion to the Commission for a decision.

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

9. The Member of the Commission responsible for security matters shall inform the Member States about the nature and classification of the information, listing the organisations and countries to which it may be released, as decided by the Commission.

10. The Commission Security Office shall take all the necessary measures to facilitate any consequent damage assessment and review of procedures.

    Whenever the conditions of cooperation change, the Commission shall reconsider the issue.

SECURITY PROVISIONS TO BE APPLIED BY BENEFICIARIES

11. The Member of the Commission responsible for security matters shall notify the beneficiary States or international organisations of the Commission's decision to authorise the release of EU classified information, together with the detailed rules of protection proposed by the Commission Security Policy Advisory Group and approved by the Commission.

12. The decision shall come into force only when the beneficiaries have given a written assurance that they will:

— Use the information for no other purpose than the cooperation decided by the Commission;

— Offer the information the protection required by the Commission.

13. Transmission of documents

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

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

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

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

14. Registration on arrival

The addressee State's NSA or its equivalent in the State receiving the classified information forwarded by the Commission on behalf of its government, or the security bureau of the recipient international organisation, shall open a special register to record EU classified information on its receipt. The Register shall 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.

15. Use and protection of the classified information exchanged

(a) Information at the level of EU SECRET shall be handled by specifically designated officials, authorised to have access to information with this classification. It shall 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 shall be permanently guarded and a system of verification shall be set up to ensure that only duly authorised persons are allowed to enter. EU SECRET-level information shall be forwarded by diplomatic bag, secure mail services or by secure telecommunications. An EU SECRET document shall be copied only with the originating authority's written agreement. All copies shall be registered and monitored. Receipts shall be issued for all operations relating to EU SECRET documents;

(b) EU CONFIDENTIAL shall be handled by duly designated officials authorised to be informed on the subject. Documents shall be stored in locked security cabinets in controlled areas;

EU CONFIDENTIAL information shall 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) EU RESTRICTED information shall 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 shall not call for special protection measures and may be forwarded by mail and public telecommunications systems. The addressees may make copies.

16. Destruction

Documents no longer needed shall be destroyed. In the case of EU RESTRICTED and EU CONFIDENTIAL documents, an appropriate note shall be entered in the special registers. In the case of EU SECRET documents, destruction certificates shall be issued and signed by two persons witnessing their destruction.

17. Breaches of security

If EU CONFIDENTIAL or EU SECRET information is compromised or there is a suspicion of compromise, the NSA of the State or the head of security in the organisation shall conduct an enquiry into the circumstances of the compromise. The Commission Security Office shall be notified of its results. The necessary steps shall be taken to remedy inadequate procedures or storage methods if they have given rise to the compromise.

Appendix 6

LIST OF ABBREVIATIONS

ACPC	Advisory Committee on Procurement and Contracts
CrA	Crypto Authority
CISO	Central Informatics Security Officer
COMPUSEC	Computer Security
COMSEC	Communication Security
CSO	Commission Security Office
ESDP	European Security and Defence Policy
EUCI	EU classified information
IA	INFOSEC Authority
INFOSEC	Information Security
IO	Information Owner
ISO	International Organisation for Standardisation
IT	Information Technology
LISO	Local Informatics Security Officer
LSO	Local Security Officer
MSO	Meeting Security Officer
NSA	National Security Authority
PC	Personal Computer
RCO	Registry Control Officer
SAA	Security Accreditation Authority
SecOPS	Security Operating Procedures
SSRS	Specific Security Requirement Statement
TA	Tempest Authority
TSO	Technical Systems Owner