COMMISSION DECISION

of 16 August 2006 C(2006) 3602

concerning the security of information systems used by the European Commission

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 Atomic Energy Community, and in particular Article 131 thereof,

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

Whereas:

(1) Information systems play an essential role in the compilation, input, processing, storage and distribution of information.

(2) Information systems can be open to accidental and wilful, tangible and intangible threats.

(3) There ought to be a frame of reference to allow the definition of common principles, procedures, priorities and responsibilities, and a framework for the expression of security needs, so that each information system can be protected in a way appropriate to the actual degree of risk to which it is exposed.

(4) The security of information systems must include measures relating to technical and physical security, procedural measures and organisational measures.

(5) The generally horizontal nature of information systems means that security measures involve, at various levels, a number of departments, including the Commission's horizontal departments.

(6) The management and implementation of measures aimed at ensuring the security of information systems are the responsibility of each Directorate-General and department, and of each body using the Commission's information systems.

(7) The Commission has particular responsibility for, on the one hand, protecting the information and information systems held by its Directorates-General and, on the other, for fulfilling its obligation to provide information to the other Institutions, to the Member States, to citizens and to its numerous partners.

(8) There should be uniform rules to ensure that all of the Commission's information systems are equally protected against threats, regardless of the Directorate-General or department that holds them and independent of the place of work where they are located.

(9) With regard to the systems management of the security of information systems, the Commission may apply internationally recognised standards such as the ISO/IEC 27001 standard. The Commission may also take into account the results of research it carries out direct or funds under its framework programmes for research and development, and also work carried out by the European Network and Security Information Agency established by Regulation (EC) No 460/2004 of the European Parliament and of the Council[1].

(10) Management of risks linked to the security of information systems is complementary to the management of risks linked to the Commission's internal control systems and procedures. It also complements the specific risk management procedure made up of impact and ex ante assessments of the Commission's legislative proposals and main programmes which have an impact on the budget[2].

(11) This Decision applies without prejudice 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[3], Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[4], and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)[5].

(12) Section 25 of the Commission's provisions on security, annexed to Decision 2001/844/EC, ECSC, Euratom[6], contains rules relating to the security of information systems, particularly those relating to EU classified information. These rules must be extended to cover all information systems so as to protect the integrity, availability and confidentiality of these systems and the information they process.

(13) It is necessary to update Decision No C(95) 1510 on the security of information systems in the light of technological developments and changes in the Commission's organisation. For the sake of clarity, it should be replaced by this Decision,

---

1 OJ L 77, 13.3.2004, p. 1.

2 SEC (2005) 1327/4 of 25 October 2005: "Communication to the Commission of Ms Grybauskaité in agreement with the President and Vice-President Kallas - Towards an effective and coherent risk management in the Commission services"

3 OJ L 145, 31.5.2001, p. 43.

4 OJ L 8, 12.1.2001, p. 1.

5 OJ L 201, 31.7.2002, p. 37.

6 OJ L 317, 3.12.2001, p. 1.

HAS DECIDED AS FOLLOWS:

Article 1

Subject matter

1. This Decision provides for security measures for the protection of the Commission's information systems and the information processed therein against threats to the availability, integrity and confidentiality of these systems and information.

2. The measures taken may be technical, physical, procedural or organisational. they must serve to diminish the likelihood of threats, to diminish their impact when they do materialise, to identify all security incidents as quickly as possible and to restore the situation to normal within the required time limit.

3. They must be proportionate to the danger in terms of costs and functional or technical restrictions.

Article 2

Scope

The security measures provided for by this Decision shall apply to the Commission's information systems and concern all of its Directorates-General and departments in all places of work, including the Joint Research Centre and the delegations in third countries, offices linked administratively to the Commission[7] and all Executive Agencies or other bodies using the Commission's information systems. They shall also apply to any form of teleworking.

They shall be applicable to officials and other servants of the Communities, persons under contract to the Commission and subcontractors who have access to and use the Commission's information systems.

Article 3

Definitions

For the purposes of this Decision the following definition shall apply:

1) "Information" means data in a form that allows it to be communicated, recorded or processed.

2) "EU classified information" means all information classified EU RESTRICTED, EU CONFIDENTIAL, EU SECRET or EU TOP SECRET under point 4.2a of the provisions on security annexed to Decision 2001/844/EC, ECSC, Euratom.

[7] OLAF, EPSO, OPOCE, OIL, OIB and PMO.

3) “Information system” means a set of equipment, methods and procedures, and where relevant also persons, personnel, organised to perform information processing functions.

4) “Threat” means a potential for the accidental or deliberate compromise of security involving loss of one or more of the properties of confidentiality, integrity and availability of information systems or the information contained therein.

5) “Vulnerability” means a weakness or lack of safeguards that might facilitate or permit the materialisation of a threat to an information system or the information contained therein.

6) “Risk” means the degree of danger that a threat might materialise if one or more vulnerabilities in an information system were to be exploited.

7) “Availability” means the capacity of an information system to perform a task under defined conditions as regards schedules, deadlines and performance.

8) “Integrity” means the guarantee that the information system and processed information can be altered only by deliberate and legitimate action and that the system will produce the expected result accurately and in full.

9) “Confidentiality” means the reserved character of information or of all or part of an information system (such as algorithms, programmes and documentation) to which access is limited to authorised persons, bodies and procedures.

10) “Non-repudiation” means the possibility of determining with certainty that an action or event is attributable to a process or person.

11) “Security need” means a precise and unambiguous definition of the levels of confidentiality, integrity and availability associated with a piece of information or an information system with a view to determining the level of protection required.

12) “Security requirement” means the specifications in terms of functions or level of assurance relating to the security measures to be implemented in an information system to ensure that it meets the security needs.

13) “Information systems security policy” means the current provisions governing information security and their detailed implementing rules.

14) “Security plan” means a document describing the measures required to meet the security requirements of an information system.

15) “Security incident” means an event identified as having a prejudicial effect on the security of an information system.

16) “Personal data” means personal data as defined in Article 2(a) of Regulation (EC) No 45/2001.

17) “Processing of personal data” means the processing of personal data as defined in Article 2(b) of Regulation (EC) No 45/2001.

17) "User" means any person to whom this Decision applies.

18) "Directorate-General" means any Directorate-General or departments or any other administrative body to which Article 2 refers.

19) "Data owner" means any user who as owner of the information ensures the consistency and validity of the data.

20) "System security officer" (SSO) means an officer designated by the information system owner to advise the owner on the security of the information system.

Article 4

Compliance of users with the information systems security policy

1. The Directorates-General shall take the necessary steps, with the aid of the Security Directorate, to ensure that their staff, including subcontractors and contractors, are made aware of the information systems security policy.

2. Each new user must be informed of the information systems security policy.

3. By accessing the Commission's IT resources for the first time users are deemed to undertake to comply with the information systems security policy.

4. Use of the Commission's information systems in breach of the information systems security policy or for illegal purposes may give rise to disciplinary proceedings.

5. The rules on use and access by users are described in Annex III.

Article 5

Protection of personal data

1. The information systems security policy must guarantee a high level of protection of personal data and the processing thereof in accordance with Regulation (EC) No 45/2001, particularly Articles 21 to 23 and 35 to 37.

Article 6

Use of encrypting technologies

1. The use of encrypting technologies by Directorates-General must be approved in advance by the Security Directorate.

2. Directorates-General shall put in place means of recovering stored data where the necessary decryption key is not available.

3. Where need is duly established, the recovery of encrypted data shall be carried out by officials of the Security Directorate with the authorisation of its Director or by the Local Information Security Officer (LISO), following procedures that protect classified information and personal data.

Article 7

Security incidents

1. When a security incident covered by this Decision is detected in a Directorate-General, the Local Information Security Officer (LISO) shall be informed. LISOs shall at once inform their superiors and the Security Directorate.

2. Solely for the purposes of verifying and investigating security incidents in information systems in order to determine their causes, impact and remedies, the Director of the Security Directorate shall authorise officials of the Directorate to access all necessary information, where necessary using the appropriate means and in proportion to the seriousness of the event, after obtaining the specific agreement of the Director-General of the Directorate-General for Personnel and Administration, and after consulting the Data Protection Officer. Access to classified information shall be given in accordance with the rules governing such information.

Article 8

Security needs of information and information systems

1. The security needs of the information systems and the information processed therein shall be expressed in terms of their level of confidentiality, integrity and availability. The security requirements shall be determined on the basis of these needs.

2. The levels of confidentiality, integrity and availability are defined in Annex I.

Article 9

Responsibilities and organisation

1. Responsibility for the security of information systems shall lie with different parties, particularly the following:

   a) the Directorate-General for Informatics, in respect of its management and coordination of IT and telecommunications technology intended for the use of the other Directorates-General;

   b) the Security Directorate, in respect of the drawing up and updating of the detailed rules for implementing this Decision, in respect of support and monitoring of the implementation of the information systems security policy, and in respect of advice given to other Directorates-General and departments;

c) all Directorates-General and departments, in respect of the implementation of security measures for the information systems for which they are responsible.

2. The responsibilities of the different parties for the security of information systems and the organisation to be put in place at the Commission are defined in Annex II.

Article 10

Detailed implementing rules

1. The detailed rules for implementing this Decision shall be decided and updated by the Director-General of the Directorate-General for Personnel and Administration, acting on proposals from the Security Directorate, after consulting the Directorates-General in accordance with Article 23 of the Commission's Rules of Procedure, and after informing the European Data Protection Supervisor in accordance with Article 28(1) of Regulation (EC) No 45/2001.

2. The drafting and updating of the detailed implementing rules shall take account of the following:

a) new obligations by which the Commission may be bound,

b) developments in IT and electronic communications technology, particularly the results of research work carried out or financed by the Commission,

c) the experience accumulated in the application of the information systems security policy,

d) specific situations in Directorates-General and departments such as the European Anti-Fraud Office, delegations, representations and external offices,

e) internationally recognised norms and standards applicable in the field of information systems security,

f) work carried out by the European Network and Information Security Agency.

3. The detailed implementing rules may be supplemented by measures of a technical, physical, procedural or organisational nature adopted by the Director-General of the Directorate-General for Personnel and Administration in consultation with departments having a legitimate interest.

Article 11

Transitional provisions

1. Any new information system must from the design stage take account of the information systems security policy.

2. The information systems security policy shall be incorporated into operational information systems within a time limit agreed jointly by the Directorate-General concerned and the Security Directorate.

Article 12

Repeal

Decision C (95) 1510 of 23 November 1995 is hereby repealed.

Done at Brussels, 16 August 2006

For the Commission

Member of the Commission

ANNEX I
Confidentiality, integrity and availability

A. IDENTIFICATION OF THE LEVEL OF CONFIDENTIALITY OF INFORMATION AND INFORMATION SYSTEMS

1. Without prejudice to the gradings provided for by the provisions on security, information systems and the information processed therein shall be protected to ensure that only authorised persons or those with a need to know may access them or receive information from them.

2. In order to define appropriate security measures, information systems and the information processed therein shall be identified according to their level of confidentiality on the basis of the likely consequences that unauthorised disclosure might have for the interests of the Commission, the other Institutions, the Member States or other parties.

3. The levels referred to in point 2 are as follows:

   – "PUBLIC": information system or information whose public disclosure would not damage the interests of the Commission, the other Institutions, the Member States or other parties;

   – "LIMITED": information system or information reserved for a limited number of persons on a need to know basis and whose disclosure to unauthorised persons would be prejudicial to the Commission, other Institutions, Member States or other parties, but not to an extent serious enough to merit classification as laid down in paragraph 16.1 of the provisions on security. An additional marking may be attached for information at this level of security identifying the categories of persons or bodies who are the recipients of the information or authorised to access it.

B. IDENTIFICATION OF THE LEVELS OF INTEGRITY AND AVAILABILITY OF INFORMATION AND INFORMATION SYSTEMS

1. Information systems and the information processed therein shall also be identified according to their level of integrity and availability on the basis of the likely consequences that a loss of integrity or availability might have for the interests of the Commission, other Institutions, Member States or other parties.

2. The levels referred to in point 1 are as follows:

   – "MODERATE" shall apply to information or information systems the loss of whose integrity or availability might threaten the internal working of the Commission; cases would include the non-application of the Commission's Rules of Procedure without any outside impact or with limited outside impact, a threat to the achievement of the objectives of an action plan, or the appearance of significant organisational and operational problems within the Commission without any outside impact;

– "CRITICAL" shall apply to information or information systems the loss of whose integrity or availability might threaten the position of the Commission with regard to other Institutions, Member States or other parties; cases would include damage to the image of the Commission or of other Institutions in the eyes of the Member States or the public, a very serious prejudice to legal or natural persons, a budget overrun or a substantial financial loss with very serious adverse consequences for the Commission's finances;

– "STRATEGIC" shall apply to information or information systems the loss of whose integrity or availability would be unacceptable to the Commission, to other Institutions, to Member States to other parties because it might, for example, lead to the halting of the Commission's decision-making process, an adverse effect on important negotiations involving catastrophic political damage or financial losses, or the undermining of the Treaties or their application.

C. SECURITY REQUIREMENTS OF INFORMATION SYSTEMS

1. The security requirements of information systems shall be determined on the basis of their security needs and the security needs of the information they process. The rules and recommendations governing such determination shall be defined in the detailed implementing rules.

2. For inventory and reporting purposes, information systems shall be classified in terms of their security requirements as defined in the preceding paragraph as follows:

   – "STANDARD": where the security requirements are met by the security measures provided by the basic infrastructure of the Commission's information systems, which infrastructure shall be defined in the detailed implementing rules;

   – "SPECIFIC": where the security requirements make it necessary for measures to be put in place that complement or replace the security measures provided by the infrastructure of the Commission's information systems.

3. Accreditation of information systems processing classified information shall be governed by Section 25 of the provisions on security annexed to Decision No 2001/844/EC, ECSC, Euratom.

ANNEX II
Responsibilities of the different parties for the security of information systems

A. THE DIRECTORATES-GENERAL

1. Les directions générales sont responsables de la mise en œuvre de la politique de sécurité des systèmes d'information pour les systèmes d'information qui sont sous leur responsabilité. Elles sont responsables des activités liées à la gestion de cette mise en œuvre.

2. The Directorates-General shall draw up, implement and manage the security plans for their information systems. These plans shall be recorded in a register.

3. They shall define and plan guidelines, human resources, budgetary resources and IT resources for the activities associated with their responsibilities for the security of information systems.

4. The Directorates-General may delegate all or part of the implementation and management of their security plans to horizontal departments such as the Directorate-General for Informatics. In such cases, the Directorates-General shall ensure that the department in question applies the necessary security measures. In order to record the terms of the delegation, a Service Level Agreement shall be drawn up between the parties defining in particular measures for monitoring implementation.

5. The Directorates-General shall inform in good time the Directorate-General for Informatics, the Local Informatics Security Officers, the Local Informatics Security Officers of the other Directorates-General and the Security Directorate of any alteration to the architecture of their systems that is likely to affect information systems that are not under their responsibility.

6. They shall periodically carry out a review of the security requirements of their information systems on the basis of security needs.

7. They shall draw up, implement and develop the relevant measures for their information systems in accordance with their security requirements in order to give them appropriate protection.

8. They shall establish, maintain and test contingency and back-up plans tailored to security needs.

9. They shall ensure that the obligation to comply with the Commission's information systems security policy is clearly mentioned in each contract they conclude with contractors.

B. LOCAL INFORMATICS SECURITY OFFICERS (LISOS)

1. Each Director-General or Head of Service shall appoint at least one Local Informatics Security Officer (LISO). LISOs should not be members of the IRM team and should report directly to the Director-General, Head of Service or Director of

Resources. There shall consequently be no hierarchical link between LISOs and the Security Directorate.

2. LISOs must be sufficiently available, have appropriate experience in the security of information systems and have the management skills necessary to carry out their role efficiently.

3. Within their Directorate-General, LISOs

– shall oversee the development of the security plans approved by the Director-General and monitor their implementation,

– shall contribute to the dissemination of the information systems security policy within their Directorate-General by proposing specific awareness-raising and training programmes,

– shall ensure that an inventory of all information systems is kept and updated, with a description of the security needs and a grading of the requirements,

– shall advise and report to their superiors, the system owners, IT service providers and project leaders on information systems security matters,

– shall ensure that IT service providers and system suppliers put in place in the information infrastructures or systems the security measures required under security plans.

– shall collaborate with the Local Security Officer (LSO) defined in the provisions on security annexed to Decision No 2001/844/EC, ECSC, Euratom,

– shall collaborate with the Data Protection Coordinator (DPC) defined in SEC (2002) 1043,

– shall be the main contacts of the Security Directorate concerning the security of information systems and take part in this capacity in meetings organised by it.

4. Without prejudice to the provisions on security annexed to Decision No 2001/844/EC, ECSC, Euratom, LISOs may take part in the checks carried out whenever a security incident occurs that may threaten one or several information systems used by their Directorate-General in order to determine its causes and impact and to identify containing and corrective measures.

C. SYSTEM OWNERS

1. System owners shall bear responsibility for the security of their information system. They shall define the security needs of the information system and the information processed therein. To this end, they shall take note of the needs expressed by data owners and users.

2. In matters of information systems security, they shall consult the Local Informatics Security Officer of their Directorate-General or the Systems Security Officer (SSO) that they may have appointed for this purpose.

3. They shall approve the identification of the security requirements and security measures.

4. They shall request accreditation from the Security Accreditation Authority (SAA) for any information system that requires accreditation in order to apply the provisions on security[8]. They shall ensure that their information system complies with the decisions of the Security Accreditation Authority.

C.A DATA OWNERS

5. Data owners shall ensure the consistency and validity of the information in the local domain in which the information system is used. They shall define the security needs of the data for which they are responsible and inform system owners of these needs.

C.B SYSTEM SECURITY OFFICERS (SSOS)

6. They shall ensure that the security of the system is consistent with the principles of this Decision and implement the necessary security policies in this respect.

7. They shall coordinate their activities with those of the LISOs.

8. They shall elaborate the definition, implementation and verification of the security needs of the system for which they are responsible.

9. They shall report to the information system owner on all security matters.

D. PROJECT LEADERS

1. Project leaders shall bear responsibility for the installation and hand-over of the information system to the system owner. They shall specify the security requirements on the basis of the security needs defined by the latter, in the light of a risk assessment if necessary. They shall define the architecture, apply the Commission's ordinary security measures and define and implement specific security measures. They shall ensure that those measures are put in place in the information system or in the infrastructures that support it, whether local or centralised.

2. They shall cooperate with the INFOSEC, Crypto and TEMPEST authorities defined in the provisions on security annexed to Decision 2001/844/EC, ECSC, Euratom in the drafting of the documents required for the accreditation procedure and the compliance of the system with the decisions of the Security Accreditation Authority.

3. They shall ensure that the design, installation and implementation of the project are in accordance with the security requirements of the information system and the information systems security policy.

---

[8] Accreditation is defined in point 25.2 of the provisions on security annexed to Decision 2001/844/EC, ECSC, Euratom.

E. SYSTEM SUPPLIERS

1. System suppliers shall construct and ensure the maintenance and development of the information system in accordance with the security requirements drawn up by the project leader and approved by the system owner.

2. They shall define the technical architecture in collaboration with the Directorate-General for Informatics, and draw up technical specifications for the implementation of the security requirements as defined by the project leader.

3. They shall provide operating manuals and instructions.

F. SYSTEM MANAGERS

1. System managers shall manage the operation of the information system on behalf of the system owner. They may manage the specific security measures direct, or subcontract their management to IT service providers. In the latter case, they shall conclude a Service Level Agreement with the IT service providers to ensure that the security measures for which they are responsible are implemented.

2. They shall ensure that the information necessary to meet the need for non-repudiation and to monitor the proper performance of the Service Level Agreement are preserved and accessible.

G. IT SERVICE PROVIDERS

1. IT service providers shall provide system owners with a range of structured and managed IT resources such as electronic communications networks, equipment and software.

2. The functions of IT service providers shall be carried out in particular by units at the Directorate-General for Informatics, some Commission departments, information resource managers (IRMs) or by subcontracted external services.

3. IT service providers shall be responsible for the security management of the resources they provide.

4. They shall implement the security measures specified in Service Level Agreements concluded with system managers, the security plans and the agreements reached with other service providers.

5. They shall keep an exhaustive inventory of the IT resources they manage. For each such resource the inventory must state the security requirements that are to be met.

6. They shall inform the relevant system managers and LISOs of any security incidents that occur.

7. They shall implement the necessary containment and corrective security measures when a security incident occurs, in collaboration with the Security Directorate and the LISO.

8. They shall maintain the level of security of their IT resources by applying the information systems security policy.

9. They shall evaluate the impact on security of changes made to IT resources. They shall inform the relevant LISOs of changes to the level of security. They shall also inform the Commission's IT community and the Security Directorate if the change is likely to have an impact on Commission information systems that are outside their control.

10. They shall ensure that any new software or equipment to be installed is safe for the information systems and information processed therein.

11. They shall monitor the availability of IT resources.

12. They shall put in place contingency and back-up plans for the IT resources they manage.

13. They shall install, or cause to be installed, physical security measures to protect the equipment for which they are responsible, the choice of measure being based on the security requirements that the equipment must meet.

14. They shall ensure that the information necessary to meet the need for non-repudiation is preserved and accessible.

15. They may appoint a security manager, whose task shall be to coordinate activities associated with the operational management of the security of the services provided.

H. LOCAL INFORMATION RESOURCE MANAGERS (IRMS)

1. Local information resource managers (IRMs) shall be responsible for the provision of IT resources in their Directorate-General. They may also carry out certain of the security functions mentioned in this Annex, depending on the Directorate-General in question. In general, they shall be the IT service provider for their Directorate-General as regards local resources and their staff shall manage the security of those resources accordingly.

I. THE SECURITY DIRECTORATE

1. The Security Directorate shall be responsible for coordinating all activities relating to the implementation of this Decision. It shall ensure that the activities are consistent and that this Decision is implemented in accordance with the provisions on security.

2. It shall draw up in collaboration with the LISOs the detailed implementing rules for this Decision, to be adopted in accordance with the procedure indicated in Article 10.

3. In accordance with the provisions on security, it shall act as the Security Accreditation Authority (SAA), the INFOSEC Authority (IA), the Crypto Authority (CrA) and the TEMPEST Authority (TA).

4. It shall organise training, awareness-raising and support activities in cooperation with the units in charge of general and IT training at the Commission in order to ensure the implementation and application of this Decision.

5. It shall ensure that the information systems security policy is taken into account when the Directorate-General for Informatics and the other Directorates-General draw up IT strategy.

6. It shall advise and assist Directorates-General in the implementation of the information systems security policy and during the drawing up, implementation and monitoring of the security plans.

7. It may ensure that the security plans comply with the information systems security policy.

8. It shall advise and assist system owners and project leaders during the drafting of the documents necessary for accreditation and during the process of bringing information systems into line with the decisions taken by the Security Accreditation Authority.

9. It shall maintain close cooperation with LISOs. It shall assist and support them in the performance of their tasks. It shall organise a meeting with them at least once a year.

10. It shall maintain cooperation with the national security authorities of the Member States and with the security authorities of the other European Institutions concerning the implementation of this Decision.

11. For invitations to tender, the Security Directorate may take part, either at its own request or at the request of the Directorate-General, in the drawing up of technical specifications and selection and award criteria with regard to the security of information systems.

12. It shall monitor the implementation of the information systems security policy. It shall report on the question to the competent authorities at the Commission. In the event of serious infringements, it shall notify the matter as soon as possible to those authorities and, where appropriate, to the Member of the Commission responsible for security matters.

13. Its authorisation shall be required for the connection of electronic communications networks to the Commission's private electronic communication networks.

J. THE DIRECTORATE-GENERAL FOR INFORMATICS

1. The rules and responsibilities laid down for the Directorates-General shall apply mutatis mutandis to the Directorate-General for Informatics.

2. The Directorate-General for Informatics shall set up and maintain an IT infrastructure, including a methodology and dedicated resources for the development of information systems, in accordance with the information systems security policy.

3. It shall ensure the security of the Commission's private electronic communications network and provide secure connections to the network for the Commission’s external sites, contractors and all authorised partners, in cooperation with the Directorates-General concerned.

4. It shall make available architecture, reference configurations and IT software and equipment satisfying the needs of the implementation of the security policy.

5. It shall draw up and implement within the Commission a programme of measures to prevent the exploitation of vulnerabilities in systems, such as measures to combat malicious code. It shall set up corrective measures to prevent the exploitation of vulnerabilities in the software and equipment for which it provides central support.

6. It shall manage the general security mechanisms, such as firewalls, intrusion detection programs, antivirus programs and authentication systems.

7. It shall manage security incidents in cooperation with the Security Directorate.

8. In cooperation with the Security Directorate, the Directorate-General shall keep abreast of the latest technological developments as regards security for all the IT software and equipment for which it provides central support.

9. It may delegate certain tasks and responsibilities to other departments. In such cases, a Service Level Agreement shall be concluded between the Directorate-General for Informatics, the Directorate-General concerned and the Security Directorate in order to define the conditions of the delegation, particularly in terms of the connection of electronic communications networks.

ANNEX III
Rules on the use of and access to the Commission's information systems

A. GENERAL RULES

1. Users shall comply with the information systems security policy and the security plans applicable to them in carrying out their duties.

2. Without prejudice to other obligations resulting from provisions that may apply to them, users shall seek to ensure that the information and IT resources placed at their disposal by the Commission are protected.

3. These rules shall also apply to teleworking.

B. SPECIFIC RULES

1. Without prejudice to Article 17 of the Staff Regulations or other provisions that may apply, users shall seek to ensure that information that is the property of the Commission is not disclosed to unauthorised persons.

2. They shall use all the means for controlling access with which they are provided to prevent the use by unauthorised persons of the resources placed at their disposal or under their control. Among other things, they shall ensure that the information systems placed at their disposal are not accessible during their absence, even when this is for a short time only.

3. With the exception of public access information systems, they shall access only those information systems for which they have been granted explicit authorisation, whether or not the systems are the property of the Commission.

4. They shall not reveal their authentication mechanisms or share them with other persons.

5. They shall use the information systems placed at their disposal or under their control in the way they are intended to be used.

6. They shall not install equipment or software on the IT resources placed at their disposal or under their control.

7. They shall not install equipment or software enabling connections to be made with other electronic communications networks.

8. They shall neither install nor use their own equipment or software to access the information systems covered by this Decision.

9. If users become aware of a vulnerability or event affecting one or several of the Commission's information systems, they shall immediately inform the local information resource manager (IRM) of their Directorate-General or a person appointed by the latter for this function.

10. They shall not seek to test any vulnerabilities in the systems and shall not seek to circumvent the security measures put in place.

11. They shall ensure that visitors under their responsibility do not by their conduct endanger the security of the Commission's information systems, and in particular that they do not connect their own equipment to the Commission's private electronic communications network.

12. Any derogation from these rules must be justified by the needs of the service and explicitly authorised by the LISO and the IT service provider concerned, after informing the Security Directorate, which reserves the right to establish the framework for such derogation.