Title: Information Security Policy			
Number ECDC/IP/63		Checked by Procedure coordinator: 30.05.2011	
Consultation: Legal Advisor 26.11.2010 ISSC 29.02.2011 SMT 29.03.2011			
Author Catalin Butiseaca		Date and signature 16.05.2011	
Reviewer: Head of PHC, Karl Ekdahl		Date and signature 2011-05-17	
Approval : Director, Marc Sprenger		Date and signature 17/5/11	
Consultation or adoption by other bodies (if applicable)			
Date issued (effective date):		30.05.2011	
Review date: max 2 years from effective date		29.05.2013	
Log of revisions			
Rev #	Issue date	Author	

CONTENTS

1. PURPOSE

This policy provides for security measures, for the protection of the ECDC's information systems and the information processed. The measures taken may be technical, physical, procedural or organizational. They must serve to diminish the likelihood of threats, to diminish their impact when they do materialize, to identify all security incidents as quickly as possible and to restore the situation to normal within the required time limit.

2. SCOPE

This policy applies to all ECDC information systems and applications.

3. BACKGROUND

Information Security Policy was developed as part of ECDC overall security requirements. It is also a requirement of the European Data Protection supervisor.

The following documents were used as guidelines:

COMMISSION DECISION of 16 August 2006 C(2006) 3602 concerning the security of information systems used by the European Commission

Implementing rules for COMMISSION DECISION C(2006) 3602 of 16.8.2006 concerning the security of information systems used by the European Commission

4. DESCRIPTION

This policy has the following main objectives:

- To safeguard ECDC information from unauthorised disclosure;
- To safeguard ECDC information handled in communications and information systems and networks, against threats to its confidentiality, integrity and availability;
- In the event of failure, to assess the damage caused, limit its consequences and adopt the necessary remedial measures.

5. DEFINITIONS

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

- "Information" means data in a form that allows it to be communicated, recorded or processed.
- "Information system" means a set of equipment, methods and procedures, and where relevant also persons, personnel, organised to perform information processing functions.
- "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.
- "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.
- "Risk" means the degree of danger that a threat might materialise if one or more vulnerability in an information system were to be exploited.
- "Availability" means the capacity of an information system to perform a task under defined conditions as regards schedules, deadlines and performance.
- "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.
- "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.
- "Non-repudiation" means the possibility of determining with certainty that an action or event is attributable to a process or person.
- "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.
- "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.
- "Information systems security policy" means the current provisions governing information security and their detailed implementing rules.
- "Security plan" means a document describing the measures required to meet the security requirements of an information system.
- "Security incident" means an event identified as having a prejudicial effect on the security of an information system.
- "Personal data" means personal data as defined in Article 2(a) of Regulation (EC) No 45/2001.
- "Processing of personal data" means the processing of personal data as defined in Article 2(b) of Regulation (EC) No 45/2001.

6. INFORMATION SYSTEMS SECURITY RISK MANAGEMENT

The aim of the information systems security risk management process is to identify and implement a set of effective and affordable security measures for an information system. The process is the responsibility of the system owner and must be applied to all information systems classified as SPECIFIC (as described in Annex 1). This process consists of the following steps: risk identification, risk assessment, risk treatment, risk acceptance and risk communication.

- Risk identification — must be performed by identifying the threats to and vulnerabilities of the system based on its characteristics.
- Risk assessment — must be performed by taking into account the required level of security needs derived from the business impact assessment and the levels of identified threats and system vulnerabilities. Risk assessment gives an overview of all risks and calculates the highest risks based on security needs, threat occurrence likelihood and vulnerability level.
- Risk treatment — risks must then be treated through a combination of prevention controls, detection controls, avoidance tactics and/or transfer to another organisation. For a given risk level and a selected environment, corresponding security measures available in the ECDC information systems security policy must be used where available, but additional requirements and measures may always be selected if justified by the risk assessment and based on the rule of proportionality (additional requirements and measures must be proportional to the risk).
- Risk acceptance — residual risks, for which the selected controls will not be feasible or will not provide complete treatment, must be formally accepted using criteria documented in the security plan. These acceptance criteria are based on maximum acceptable risk levels for all or specific security needs specified by business impact assessment or legal, regulatory or contractual requirements.
- Risk communication — the information systems security risk management process must be documented and the security requirements and measures, including any accepted residual risks, must be formally approved by the system owner and communicated to relevant stakeholders.

7. SCOPE OF INFORMATION SYSTEMS SECURITY POLICY.

Provide a list of high-level information systems security policy objectives. These policy objectives are based on industry best practices and are selected to suit the IT environment of the ECDC.

These objectives must - in principle - be targeted in all information systems unless the system owner - after a risk analysis - decides not to select them. This decision shall then be adequately justified and documented.

The standards, which shall be applied to target the above policy objectives, shall be selected to meet the requirements identified by a risk assessment and risk treatment process, using the principle of proportionality to mitigate - at an appropriate level - the threats and will be

implemented using a phased approach. Each standard shall specify conditions, security needs and/or risk levels under which the security controls must be implemented for information systems classified at the STANDARD level.

Additional objectives and/or stronger security controls may be decided and implemented as part of the risk management process under the responsibility of the system owner for 'SPECIFIC' information systems.

8. BREACH OF COMPLIANCE

Compliance with the ECDC information systems security policy is mandatory for all staff, personnel, external consultants and contractors who have access to and use the ECDC's information systems and the information they process.

Any overruling of security measures or deviations from mandatory policies and standards, must be documented, justified and approved by ISSC before any action is taken, and the ICT Security Officer and Legal Section must be informed.

Breaches of compliance may be referred to the Legal Section for further legal or disciplinary consideration.

9. HIGH-LEVEL INFORMATION SYSTEMS SECURITY POLICY OBJECTIVES

9.1. ORGANISATION OF INFORMATION SECURITY

Management must demonstrate commitment to and involvement in information systems security, provide clear direction and take responsibility.

Effective coordination and communication must be established between all stakeholders in the domain of information systems security.

Information systems security responsibilities are laid down in Annex 1.

ECDC must develop and maintain contact with local authorities (e.g.: police, fire and intelligence services) to ensure a quick response should any unlawful or harmful incidents occur.

ICT Security Officer should maintain appropriate contacts with special interest groups, forums or professional associations within information systems security, in order to obtain current information and advice on good practice, security alerts, technology, products and emerging threats and vulnerabilities.

9.2. ASSET MANAGEMENT

9.2.1. Responsibility for information systems assets

All information systems assets, whether physical or logical, must be identified, indicating their value to the ECDC. All information systems must have a designated owner, accountable for their security protection, and a designated person in charge of the implementation and maintenance of appropriate controls.

With reference to the "ECDC/IP/26 – Use of ICT equipment at ECDC", computer and communication systems are intended to be used for business purposes only. Incidental personal use is nonetheless permissible if the use does not consume more than a trivial amount of resources that could otherwise be used for business purposes, does not interfere with worker productivity, does not pre-empt any business activity, and does not cause distress, legal problems, or morale problems for other employees. Offensive material that might cast ECDC in a bad light, including sexist, racist, violent, or other content, is strictly forbidden from all ECDC personal computers.

With the reference to the "ECDC-ADM-024 Notification Process for newcomers and staff in place (arrival, change, departure)", upon termination of their employment, contract or agreement, all ECDC staff, such as Temporary Agents, Contract Agents, Seconded National Experts, trainees, interims, third party users, external consultants and contractors, must return all ECDC assets in their possession: for example security tokens granted to teleworkers, laptops, PDAs, iPhones, mobile phones or USB sticks.

9.2.2. *Identification of security needs for confidentiality, integrity and availability*

Information and related information systems must be categorised on the basis of their security needs, i.e. levels of confidentiality, integrity and availability, using a systematic process based on their value to the ECDC, criticality and sensitivity. These levels, which must be periodically reviewed, allow the need for, priorities for and degree of security protection to be determined as described in Annex 2. Procedures for information labelling and handling throughout its whole life-cycle, including disposal, must be developed and implemented in accordance with the classification scheme.

9.3. HUMAN RESOURCES SECURITY

9.3.1. *Prior to employment*

The security roles and responsibilities of ECDC staff, contractors and third-party users must be defined, documented and communicated to the people concerned. The job description and the objectives must state these roles and responsibilities for ECDC staff; contracts must state them for contractors, and service level agreements must state them for third-party users.

Prior to commencing work, all applicants for employment or award of contracts (e.g. consultants, contractors, third-party users, maintenance technicians, etc.) must submit to background verification checks in line with the relevant laws and regulations. These checks must be proportional to business requirements, the security levels of the information and information systems to be accessed, and the perceived risks (e.g. taking up references, checking career history/qualifications and confirming identity).

9.3.2. *During employment*

All ECDC staff and, where relevant, contractors and third-party users must receive appropriate training in security awareness, policies and procedures, to the extent required by their duties.

9.3.3. *Termination or change of employment*

Responsibilities related to job change or employment termination must be defined for management and ECDC staff and contractors, and procedures must be established to manage the return of assets owned by the ECDC and the removal of access rights.

9.4. PHYSICAL AND ENVIRONMENTAL SECURITY

9.4.1. *Secure areas*

Security perimeters with appropriate barriers and entry controls must be used to protect areas that contain information and information processing facilities.

Secure areas must be protected by appropriate entry controls to ensure that only authorised personnel are allowed access. Work in secure areas must follow specific security rules.

Physical security for offices, rooms and facilities must be designed and installed. Access points such as delivery and loading areas and other points where unauthorised persons may enter the premises must be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.

Physical protection against damage from natural or man-made disaster must be designed and applied proportionally to the risk.

9.4.2. Equipment security

Equipment must be protected from physical and environmental threats and from opportunities for unauthorised access. Power and telecommunications cabling carrying data or supporting information services must be protected from threats arising from interception or damage.

Equipment must be correctly maintained to ensure its continued availability and integrity.

Equipment, information or software must not be taken off-site without prior authorisation. Adequate protection must be applied to off-site equipment, taking into account the different risks of working outside the ECDC's premises.

All items of equipment containing storage media, either must be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or sending back for repair, or must be securely destroyed.

9.5. COMMUNICATIONS AND OPERATIONS MANAGEMENT

9.5.1. Operational procedures and responsibilities

Operating procedures must be documented, maintained and made available to all personnel who need them.

Changes to information processing facilities, to systems and to the provision of services must be planned, tested, documented, communicated and approved.

Duties and areas of responsibility must be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of information systems. Development, test and operational facilities must be separated to reduce the risks of unauthorised access or changes to the operational system.

9.5.2. Third-party service delivery management

Services delivered by third parties involving accessing, processing, communicating or managing the ECDC's information or information processing facilities or adding products

or services to information processing facilities must have appropriate integrated security controls. These security controls, the service definition and the delivery levels must be documented in service delivery agreements so as to ensure they are properly implemented, operated and maintained by the third party.

The services, reports and records provided by the third party must be managed by designated ECDC personnel, regularly monitored and reviewed, and audits must be carried out regularly.

9.5.3. System planning and acceptance

The use of resources must be monitored and tuned, and projections made of future capacity requirements to ensure the required system performance.

Acceptance criteria for new information systems, upgrades, and new versions must be established. Suitable tests of the system(s) must be carried out during development and prior to acceptance to ensure that all relevant security policies and requirements are met before the system is authorised and used.

9.5.4. Protection against viruses and malware

Viruses and malicious software constitutes a present and frequent threat because it may have impact on business operations. For that reason, strong controls preventing, detecting, suppressing and countering viruses and malicious software must be implemented to adequately protect ECDC information system assets.

9.5.5. Back-up

To maintain the integrity and availability of information and information processing facilities, backups of information and software must be made. They must be regularly tested, including the timely restoration of information. System owners must define which information and which machines are to be backed up, the frequency of backup, and the method of backup.

Information must be retained for as long as required by legal regulations. Other information must be destroyed when no longer needed.

ICT section is responsible for preparing and periodically updating contingency plans to restore service for all ECDC applications identified as critical and essentials. ICT section is responsible for preparing and periodically updating network service contingency plans.

9.5.6. Network security management

Network infrastructure must be adequately managed and controlled, in order to protect it from threats, and to ensure the security of the network itself and of the systems and applications using the network, including information in transit. All information travelling over ECDC computer networks that has not been specifically identified as the property of

other parties will be treated as though it is an ECDC asset. ECDC will prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information. In addition, ECDC will protect information belonging to third parties that have been entrusted to ECDC in a manner consistent with its sensitivity and in accordance with all applicable agreements.

9.5.7. Media handling

Removable media containing information must be protected against unauthorised access, misuse or corruption and its readability guaranteed during the whole lifetime of the information. Media must be disposed of securely and safely when no longer required. System documentation must be protected against unauthorised access.

9.5.8. Exchange of information

In the absence of a legal framework, the exchange of information (other than public information) and software between ECDC services and external parties must be governed by contractual agreements signed by the system owner and the external party.

9.5.9. Electronic administration services

Information involved in e-administration systems must be protected from fraudulent activity, incomplete transmission, mis-routing and unauthorised disclosure and modification. All identified security requirements must be addressed before giving external users access to the ECDC's information or assets.

The integrity of information being made available on a publicly available system must be protected to prevent unauthorised modification and its availability must be ensured in line with its classification.

9.5.10. Monitoring and logging

Audit logs recording user activities, exceptions and information systems security events must be produced and kept for an agreed period to assist in future investigations or access control monitoring in accordance with Regulation (EC) No 45/2001 on data protection.

With reference to "ECDC/IP/26 – Use of ICT Equipment at ECDC", monitoring use or faults in information processing facilities must be established and the results of the monitoring activities reviewed regularly in accordance with Regulation (EC) No 45/2001 on data protection. When necessary, appropriate action must be taken.

Logging facilities and log information must be protected against tampering and unauthorised access in order to meet the required retention period or requirements to collect and retain evidence in accordance with Regulation (EC) No 45/2001 on data protection.

9.6. ACCESS CONTROL

9.6.1. User access management

With reference to "ECDC/IP/44 Notification Process for newcomers and staff in place (arrival, change, departure)", a formal user registration and de-registration process must be used for granting and revoking access to all information systems and services. Exceptions can be granted for systems and services dedicated to public access. The allocation and use of privileges must be restricted and controlled. The allocation and use of adequate access credentials (e.g. password) must be controlled through a formal management process. Users' access rights must be reviewed at regular intervals (e.g. internal change in job or duties).

9.6.2. Network access control

Each user must only be provided with access to the services or resources that they have been specifically authorised to use. Access to diagnostic and configuration interfaces must be controlled.

For networks extending across the ECDC's boundaries, the capability of users to connect to the network must be restricted in line with the access requirements of the business applications.

Groups of information services, users, and information systems must be segregated on networks, based on the value and classification of information stored or processed in the network, levels of trust or lines of business.

With reference to "ECDC/IP/37 - Internal policy on remote access to ECDC using the VPN ", the capability of users to connect remotely to the ECDC network must be adequately secured in line with the access requirements of the business applications.

9.6.3. Operating system access control

Access to the operating system must be restricted to persons with a need to use it in accordance with a defined access control policy.

The use of system utilities that might be capable of overriding system and application controls must be restricted and tightly controlled. With reference to "ECDC/IP/26 - Use of ICT equipment at ECDC ", installation of software must be controlled.

9.6.4. Application and information access control

Access to information and application system functions must be restricted in accordance with a defined access control policy.

9.6.5. *Mobile computing and teleworking*

With reference to "ECDC/IP/26 – Use of ICT Equipment at ECDC ", mobile computing, using communication facilities and teleworking activities present particular risks that must be mitigated by appropriate security measures.

9.7. INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

9.7.1. *Security requirements of information systems*

System owners must ensure that their security requirements are properly implemented. Therefore, all security requirements must be identified at the requirements phase of a project and justified, agreed and documented as part of the project documentation.

9.7.2. *Correct processing in applications*

Data input to applications must be validated to ensure that this data is correct and appropriate. Validation checks must be incorporated into applications to detect any corruption of information due to processing errors or deliberate acts.

Requirements for ensuring authenticity and protecting integrity of messages exchanged between applications must be identified, and appropriate controls identified and implemented.

Data output from an application must be validated to ensure that the processing of information is correct and appropriate to the circumstances. Test data must be selected carefully and protected and controlled.

9.7.3. *Security in development and support processes*

The implementation of changes must be controlled by the use of change control procedures. Modifications to software packages must be discouraged and limited to necessary changes, and all changes must be strictly controlled. Access to program source code must be restricted.

Software code developed for ECDC services must be reviewed using a formal process in order to guarantee that its functions are implemented in accordance with the specifications and that there is no malicious code.

Outsourced software development must be supervised and monitored and its deliverables formally accepted before installation and usage.

9.8. INFORMATION SYSTEMS SECURITY INCIDENT MANAGEMENT

9.8.1. Reporting information systems security events and weaknesses

Information systems security events must be reported through designated channels as quickly as possible. In the case of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data processed by ECDC information systems, the system owner needs to inform the ICT Security Officer and Data Protection Officer.

All employees, contractors and third-party users of information systems and services must be required to note and report any observed or suspected security weaknesses in systems or services to ICT Security Officer.

9.8.2. Management of information systems security incidents and improvements

Information systems security incidents must be managed to ensure a quick, effective and orderly response. Mechanisms must be in place to enable the type, volume and cost of information systems security incidents to be quantified and monitored. This information gathered about incidents must be used, either to indicate the need for additional or improved security measures against future recurring or high-impact incidents, or to assist in the information systems security review process.

9.9. BUSINESS CONTINUITY MANAGEMENT

9.9.1. Information systems security aspects of business continuity management

A process must be developed and maintained for business continuity that addresses the information systems security requirements needed for business continuity for the ECDC.

Events that can cause interruptions to business processes must be identified, along with the probability and impact of such interruptions and their consequences for information systems security.

Plans must be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes and other important business processes.

The IT aspects of business continuity plans must be tested and updated regularly to ensure that they are up to date and effective.

9.10. COMPLIANCE

9.10.1. Compliance with legal requirements

All relevant statutory, regulatory and contractual requirements and the ECDC's approach to meeting these requirements must be explicitly defined, documented and kept up to date for each information system and the organisation.

Appropriate procedures must be implemented to ensure compliance with legislative, regulatory and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

9.10.2. Information systems audit consideration

Audit requirements and activities involving checks on operational systems must be carefully planned and agreed to minimise the risk of disruption to business processes. Access to information systems audit tools must be protected to prevent any possible misuse or compromise.

10. ANNEX 1 - CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

10.1. 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 ECDC, Commission and Member States, other Institutions 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 ECDC, Commission, the Member States, other Institutions 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 ECDC, other Institutions, Member States or other parties. An additional marking may be attached for information at this level of security identifying the categories of persons or bodies that are the recipients of the information or authorised to access it.

10.2. 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 ECDC; 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 ECDC 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 ECDC with regard to other Institutions, Member States or other parties; cases would include damage to the image of the

ECDC 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 ECDC's finances;

– "STRATEGIC" shall apply to information or information systems the loss of whose integrity or availability would be unacceptable to the ECDC, to other Institutions, to Member States to other parties because it might, for example, lead to the halting of the ECDC'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.

10.3. 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 ECDC'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 ECDC's information systems.

This policy doesn't cover information systems that process classified information.

11. ANNEX 2 – ROLES AND RESPONSIBILITIES

11.1. ICT SECURITY OFFICER

Shall oversee and monitor the implementation of the Information Security Policy approved by the Director and monitor their implementation,

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 his/her 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 Data Protection Officer,

Shall be the main contact of ISSC concerning the security of information systems and take part in this capacity in meetings organised by it,

11.2. SYSTEM OWNERS

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.

In matters of information systems security, they shall consult the ICT Security Officer.

They shall approve the identification of the security requirements and security measures with the help of Information Security Officer.

11.3. DATA OWNERS

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.

11.4. PROJECT MANAGERS

Project managers 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 ECDC's standard 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 centralized.

11.5. SYSTEM SUPPLIERS - DEVELOPERS

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

They shall define the technical architecture in collaboration with the ICT Section, and draw up technical specifications for the implementation of the security requirements as defined by the project leader.

They shall provide operating manuals and instructions.

11.6. IT SERVICE PROVIDERS – BACKOFFICE & NETWORKING

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

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.

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.

They shall inform the relevant system owners and ICT Security Officer of any security incidents that occur.

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

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

They shall evaluate the impact on security of changes made to IT resources. They shall inform the relevant ICT Security Officer of changes to the level of security. They shall also inform the Head of Section ICT and Project Office if the change is likely to have an impact on ECDC information systems that are outside their control.

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

They shall monitor the availability of IT resources.

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

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.

They shall ensure that the information necessary to meet the need for no repudiation is preserved and accessible.

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.

11.7. ISSC

Together with ICT Security Officer they shall ensure that the design, installation and implementation of the projects are in accordance with the security requirements of the information system and the information systems security policy.

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