DECISIONS

COMMISSION DECISION (EU, Euratom) 2017/46

of 10 January 2017

on the security of communication and information systems in the European Commission

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 249 thereof,

Having regard to the Treaty establishing the European Atomic Energy Community,

Whereas:

(1) The Commission's communication and information systems are an integral part of the functioning of the Commission and IT security incidents can have a serious impact on the Commission's operations as well as on third parties, including individuals, businesses and Member States.

(2) There are many threats that can harm the confidentiality, integrity or availability of the Commission's communication and information systems and of the information processed therein. These threats include accidents, errors, deliberate attacks and natural events, and need to be recognised as operational risks.

(3) Communication and information systems need to be provided with a level of protection commensurate with the likelihood, impact and nature of the risks to which they are exposed.

(4) IT security in the Commission should ensure that the Commission's CISs protect the information they process and they function as they need to, when they need to, under the control of legitimate users.

(5) The IT security policy of the Commission should be implemented in a manner which is consistent with the policies on security in the Commission.

(6) The Security Directorate of the Directorate-General for Human Resources and Security has the general responsibility for security in the Commission under the authority and responsibility of the Member of the Commission responsible for security.

(7) The Commission's approach should take into account EU policy initiatives and legislation on network and information security, industry standards and good practices, to comply with all relevant legislation and to allow interoperability and compatibility.

(8) Appropriate measures should be developed and implemented by the Commission departments responsible for communication and information systems and IT security measures for protecting communication and information systems should be coordinated across the Commission to ensure efficiency and effectiveness.

(9) Rules and procedures for access to information in the context of IT security, including IT security incident handling, should be proportionate to the threat to the Commission or its staff and compliant with the principles laid down in Regulation (EC) No 45/2001 of the European Parliament and of the Council [1], on the protection of individuals with regard to the processing of personal data by the Union institutions and bodies and on the free movement of such data and taking account of the principle of professional secrecy, as provided in Article 339 of the TFEU.

[1] 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 (OJ L 8, 12.1.2001, p. 1).

(10) The policies and rules for communication and information systems processing EU classified information (EUCI), sensitive non-classified information, and unclassified information are to be fully in line with Commission Decisions (EU, Euratom) 2015/443 ([1]) and (EU, Euratom) 2015/444 ([2]).

(11) There is a need for the Commission to review and update the provisions on the security of communication and information systems used by the Commission.

(12) The Commission Decision C(2006) 3602 should therefore be repealed,

HAS ADOPTED THIS DECISION:

CHAPTER 1

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This decision applies to all communication and information systems (CISs) which are owned, procured, managed or operated by or on behalf of the Commission and all usage of those CISs by the Commission.

2. This decision sets out the basic principles, objectives, organisation and responsibilities regarding the security of those CISs, and in particular for Commission departments owning, procuring, managing or operating CISs and including CISs provided by an internal IT service provider. When a CIS is provided, owned, managed or operated by an external party on the basis of a bilateral agreement or contract with the Commission, the terms of the agreement or contract shall comply with this decision.

3. This decision applies to all Commission departments and Executive Agencies. When a Commission CIS is used by other bodies and institutions on the basis of a bilateral agreement with the Commission, the terms of the agreement shall comply with this decision.

4. Notwithstanding any specific indications concerning particular groups of staff, this decision shall apply to the Members of the Commission, to Commission staff falling under the scope of the Staff Regulations of Officials of the European Union (the 'Staff Regulations') and the Conditions of Employment of Other Servants of the Union (the 'CEOS') ([3]), to national experts seconded to the Commission ('SNEs') ([4]), to external service providers and their staff, to trainees and to any individual with access to CIS in the scope of this decision.

5. This Decision shall apply to the European Anti-Fraud Office (OLAF) in so far as this is compatible with Union legislation and Commission Decision 1999/352/EC, ECSC, Euratom ([5]). In particular, measures provided for in this Decision, including instructions, inspections, inquiries and equivalent measures, may not apply to the CIS of the Office where this is not compatible with the independence of the Office's investigative function and/or the confidentiality of information obtained by the Office in the exercise of this function.

Article 2

Definitions

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

(1) 'Accountable' means to be answerable for actions, decisions and performance.

([1]) Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).
([2]) Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).
([3]) Laid down by Council Regulation (EEC, Euratom, ECSC) No 259/68 of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (Conditions of Employment of Other Servants) (OJ L 56, 4.3.1968, p. 1).
([4]) Commission Decision of 12 November 2008 laying down rules on the secondment to the Commission of national experts and national experts in professional training (C(2008) 6866 final).
([5]) Commission Decision 1999/352/EC, ECSC, Euratom of 28 April 1999 establishing the European Anti-fraud Office (OLAF) (OJ L 136, 31.5.1999, p. 20).

(2) 'CERT-EU' is the Computer Emergency Response Team for the EU institutions and agencies. Its mission is to support the European Institutions to protect themselves against intentional and malicious attacks that would hamper the integrity of their IT assets and harm the interests of the EU. The scope of CERT-EU's activities covers prevention, detection, response and recovery.

(3) 'Commission department' means any Commission Directorate-General or service, or any Cabinet of a Member of the Commission.

(4) 'Commission Security Authority' refers to the role laid down in Decision (EU, Euratom) 2015/444.

(5) 'Communication and information system' or 'CIS' means any system enabling the handling of information in electronic form, including all assets required for its operation, as well as infrastructure, organisation, personnel and information resources. This definition includes business applications, shared IT services, outsourced systems, and end-user devices.

(6) 'Corporate Management Board' (CMB) provides the highest level of corporate management oversight for operational and administrative issues in the Commission.

(7) 'Data owner' means the individual responsible for ensuring the protection and use of a specific data set handled by a CIS.

(8) 'Data set' means a set of information which serves a specific business process or activity of the Commission.

(9) 'Emergency procedure' means a predefined set of methods and responsibilities for responding to urgent situations in order to prevent a major impact on the Commission.

(10) 'Information security policy' means a set of information security objectives, which are or have to be established, implemented and checked. It comprises, but is not limited to, Decisions (EU, Euratom) 2015/444 and (EU, Euratom) 2015/443.

(11) 'Information Security Steering Board' (ISSB) means the governance body that supports the Corporate Management Board in its IT-security-related tasks.

(12) 'Internal IT service provider' means a Commission department providing shared IT services.

(13) 'IT security' or 'security of CIS' means the preservation of confidentiality, integrity and availability of CISs and the data sets that they process.

(14) 'IT security guidelines' consist of recommended but voluntary measures that help support IT security standards or serve as a reference when no applicable standard is in place.

(15) 'IT security incident' means an event that could adversely affect the confidentiality, integrity or availability of a CIS.

(16) 'IT security measure' means a technical or organisational measure aimed at mitigating IT security risks,

(17) 'IT security need' means a precise and unambiguous definition of the levels of confidentiality, integrity and availability associated with a piece of information or an IT system with a view to determining the level of protection required.

(18) 'IT security objective' means a statement of intent to counter specified threats and/or satisfy specified organisational security requirements or assumptions.

(19) 'IT security plan' means the documentation of the IT security measures required to meet the IT security needs of a CIS.

(20) 'IT security policy' means a set of IT security objectives, which are or have to be established, implemented and checked. It comprises this decision and its implementing rules.

(21) 'IT security requirement' means a formalised IT security need through a predefined process.

(22) 'IT security risk' means an effect that an IT security threat might induce on a CIS by exploiting a vulnerability. As such, an IT security risk is characterised by two factors: (1) uncertainty, i.e. the likelihood of an IT security threat to cause an unwanted event; and (2) impact, i.e. the consequences that such an unwanted event may have on a CIS.

(23) 'IT security standards' means specific mandatory IT security measures that help enforce and support the IT security policy.

(24) 'IT security strategy' means a set of projects and activities which are designed to achieve the objectives of the Commission and which have to be established, implemented and checked.

(25) 'IT security threat' means a factor that can potentially lead to an unwanted event which may result in harm to a CIS. Such threats may be accidental or deliberate and are characterised by threatening elements, potential targets and attack methods.

(26) 'Local Informatics Security Officer' or 'LISO' means the officer who is responsible for IT security liaison for a Commission department.

(27) 'Personal data', 'processing of personal data', 'controller' and 'personal data filing system' shall have the same meaning as in Regulation (EC) No 45/2001, and in particular Article 2 thereof.

(28) 'Processing of information' means all functions of a CIS with respect to data sets, including creation, modification, display, storage, transmission, deletion and archiving of information. Processing of information can be provided by a CIS as a set of functionalities to users and as IT services to other CIS.

(29) 'Professional secrecy' means the protection of business data information of the kind covered by the obligation of professional secrecy, in particular information about undertakings, their business relations or their cost components as laid down in Article 339 of the TFEU.

(30) 'Responsible' means having the obligation to act and take decisions to achieve required outcomes.

(31) 'Security in the Commission' means the security of persons, assets and information in the Commission, and in particular the physical integrity of persons and assets, the integrity, confidentiality and availability of information and communication and information systems, as well as the unobstructed functioning of Commission operations.

(32) 'Shared IT service' means the service a CIS provides to other CISs in the processing of information.

(33) 'System owner' is the individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of a CIS.

(34) 'User' means any individual who uses functionality provided by a CIS, whether inside or outside the Commission.

Article 3

Principles for IT security in the Commission

1. IT security in the Commission shall be based on the principles of legality, transparency, proportionality and accountability.

2. IT security issues shall be taken into account from the start of the development and implementation of Commission CISs. In order to do so, the Directorate-General for Informatics and the Directorate-General for Human Resources and Security shall be involved for their respective areas of responsibility.

3. Effective IT security shall ensure appropriate levels of:

(a) authenticity: the guarantee that information is genuine and from bona fide sources;

(b) availability: the property of being accessible and usable upon request by an authorised entity;

(c) confidentiality: the property that information is not disclosed to unauthorised individuals, entities or processes.

(d) integrity: the property of safeguarding the accuracy and completeness of assets and information;

(e) non-repudiation: the ability to prove an action or event has taken place, so that this event or action cannot subsequently be denied;

(f) protection of personal data: the provision of appropriate safeguards in regard to personal data in full compliance with Regulation (EC) No 45/2001;

(g) professional secrecy: the protection of information of the kind covered by the obligation of professional secrecy, in particular information about undertakings, their business relations or their cost components as laid down in Article 339 of the TFEU.

4. IT security shall be based on a risk management process. This process shall aim at determining the levels of IT security risks and defining security measures to reduce such risks to an appropriate level and at a proportionate cost.

5. All CIS shall be identified, assigned to a system owner and recorded in an inventory.

6. The security requirements of all CIS shall be determined on the basis of their security needs and of the security needs of the information they process. CIS that provide services to other CIS may be designed to support specified levels of security needs.

7. IT security plans and IT security measures shall be proportionate to the security needs of the CIS.

The processes related to these principles and activities shall be further detailed in implementing rules.

CHAPTER 2

ORGANISATION AND RESPONSIBILITIES

Article 4

Corporate Management Board

The Corporate Management Board shall take the overall responsibility for the governance of IT security as a whole within the Commission.

Article 5

Information Security Steering Board (ISSB)

1. The ISSB shall be chaired by the Deputy Secretary-General responsible for IT security governance in the Commission. Its members shall represent business, technology and security interests across the Commission departments and include representatives of the Directorate-General for Informatics, the Directorate-General for Human Resources and Security, the Directorate-General for Budget, and, on a 2-year rotating basis, representatives of four other Commission departments involved where IT security is a major concern for their operations. Membership is at senior management level.

2. The ISSB shall support the Corporate Management Board in its IT-security-related tasks. The ISSB shall take the operational responsibility for the governance of IT security as a whole within the Commission.

3. The ISSB shall recommend the Commission's IT security policy for adoption by the Commission.

4. The ISSB shall review and report biannually to the Corporate Management Board on governance matters as well as on IT-security-related issues, including serious IT security incidents.

5. The ISSB shall monitor and review the overall implementation of this decision and report on it to the Corporate Management Board.

6. On the proposal of the Directorate-General for Informatics, the ISSB shall review, approve and monitor the implementation of the rolling IT security strategy. The ISSB shall report on it to the Corporate Management Board.

7. The ISSB shall monitor, evaluate and control the corporate information risk treatment landscape and shall have the power to issue formal requirements for improvements wherever necessary.

The processes related to these responsibilities and activities shall be further detailed in implementing rules.

Article 6

The Directorate-General for Human Resources and Security

In relation to IT security, the Directorate-General for Human Resources and Security has the following responsibilities. It shall:

(1) assure alignment between the IT security policy and the Commission's information security policy;

(2) establish a framework for the authorisation of the use of encrypting technologies for the storage and communication of information by CISs;

(3) inform the Directorate-General for Informatics about specific threats which could have a significant impact on the security of CISs and the data sets that they process;

(4) perform IT security inspections to assess the compliance of the Commission's CISs with the security policy, and report the results to the ISSB;

(5) establish a framework for the authorisation of access and the associated appropriate security rules to Commission CISs from external networks and develop the related IT security standards and guidelines in close cooperation with the Directorate-General for Informatics;

(6) propose principles and rules for the outsourcing of CISs in order to maintain appropriate control of security of the information;

(7) develop the related IT security standards and guidelines in relation to Article 6, in close cooperation with the Directorate-General for Informatics.

The processes related to these responsibilities and activities shall be further detailed in implementing rules.

Article 7

The Directorate-General for Informatics

In relation to the overall IT security of the Commission, the Directorate-General for Informatics has the following responsibilities. It shall:

(1) develop IT security standards and guidelines, except as provided in Article 6, in close cooperation with the Directorate-General for Human Resources and Security, in order to assure consistency between the IT security policy and the Commission's information security policy, and propose them to the ISSB;

(2) assess the IT security risk management methods, processes and outcomes of all Commission departments and report on this regularly to the ISSB;

(3) propose a rolling IT security strategy for revision and approval by the ISSB and further adoption by the Corporate Management Board, and propose a programme, including the planning of projects and activities implementing the IT security strategy;

(4) monitor the execution of the Commission's IT security strategy and report on this regularly to the ISSB;

(5) monitor the IT security risks and IT security measures implemented in CISs and report on this regularly to the ISSB;

(6) report regularly on the overall implementation and compliance with this decision to the ISSB;

(7) after consulting with the Directorate-General for Human Resources and Security, request system owners to take specific IT security measures in order to mitigate IT security risks to Commission's CISs;

(8) ensure that there is an adequate catalogue of the Directorate-General for Informatics IT security services available for the system owners and data owners to fulfil their responsibilities for IT security and to comply with the IT security policy and standards;

(9) provide adequate documentation to system and data owners and consult with them, as appropriate, on the IT security measures implemented for their IT services in order to facilitate compliance with the IT security policy and support the system owners in IT risk management;

(10) organise regular meetings of the LISOs network and supporting LISOs in carrying out their duties;

(11) define the training needs and coordinate training programmes on IT security in cooperation with the Commission departments, and develop, implement and coordinate awareness-raising campaigns on IT security in close cooperation with the Directorate-General for Human Resources;

(12) ensure that system owners, data owners and other roles with IT security responsibilities in Commission departments are made aware of the IT security policy;

(13) inform the Directorate-General for Human Resources and Security on specific IT security threats, incidents and exceptions to the Commission's IT security policy notified by the system owners which could have a significant impact on security in the Commission;

(14) in respect of its role as an internal IT service provider, deliver to the Commission a catalogue of shared IT services that provide defined levels of security. This shall be done by systematically assessing, managing and monitoring IT security risks to implement the security measures in order to reach the defined security level.

The related processes and more detailed responsibilities shall be further defined in implementing rules.

Article 8

Commission departments

In relation to IT security in their department, each Head of Commission department shall:

(1) formally appoint a system owner, who is an official or a temporary agent, for each CIS who will be responsible for IT security of that CIS and formally appoint a data owner for each data set handled in a CIS who should belong to the same administrative entity which is the Data Controller for data sets subject to Regulation (EC) No 45/2001;

(2) formally designate a Local Informatics Security Officer (LISO) who can perform the responsibilities independently from system owners and data owners. A LISO can be designated for one or more Commission departments

(3) ensure that appropriate IT security risk assessments and IT security plans have been made and implemented

(4) ensure that a summary of IT security risks and measures is reported on a regular basis to the Directorate-General for Informatics;

(5) ensure, with the support of the Directorate-General for Informatics, that appropriate processes, procedures and solutions are in place to ensure efficient detection, reporting and resolution of IT security incidents relating to their CISs;

(6) launch an emergency procedure in case of IT security emergencies;

(7) hold ultimate accountability for IT security including the responsibilities of the system owner and data owner;

(8) own the risks relating to their CISs and data sets;

(9) resolve any disagreements between data owners and system owners and in case of continued disagreement bring the issue before the ISSB for resolution;

(10) ensure that IT security plans and IT security measures are implemented and the risks are adequately covered.

The processes related to these responsibilities and activities shall be further detailed in implementing rules.

Article 9

System owners

1. The system owner is responsible for the IT security of the CIS, and reports to the Head of the Commission department.

2. In relation to IT security, the system owner shall:

(a) ensure the compliance of the CIS with the IT security policy;

(b) ensure that the CIS is accurately recorded in the relevant inventory;

(c) assess IT security risks and determine the IT security needs for each CIS, in collaboration with the data owners and in consultation with the Directorate-General for Informatics;

(d) prepare a security plan, including, where appropriate, details of the assessed risks and any additional security measures required;

(e) implement appropriate IT security measures, proportionate to the IT security risks identified and follow recommendations endorsed by the ISSB;

(f) identify any dependencies on other CISs or shared IT services and implement security measures as appropriate based on the security levels proposed by those CISs or shared IT services;

(g) manage and monitor IT security risks;

(h) report regularly to the head of the Commission department on the IT security risk profile of their CIS and report to the Directorate-General for Informatics on the related risks, risk management activities and security measures taken;

(i) consult the LISO of the relevant Commission department(s) on aspects of IT Security;

(j) issue instructions for users on the use of the CIS and associated data as well as on the responsibilities of users related to CIS;

(k) request authorisation from the Directorate-General for Human Resources and Security, acting as the Crypto Authority, for any CIS that uses encrypting technology.

(l) consult the Commission Security Authority in advance concerning any system processing EU classified information;

(m) ensure that back-ups of any decryption keys are stored in an escrow account. The recovery of encrypted data shall be carried out only when authorised in accordance with the framework defined by the Directorate-General for Human Resources and Security;

(n) respect any instructions from the relevant Data Controller(s) concerning the protection of personal data and the application of data protection rules on security of the processing;

(o) notify the Directorate-General for Informatics of any exceptions to the Commission's IT security policy including relevant justifications;

(p) report any unresolvable disagreements between the data owner and the system owner to the head of the Commission department, communicate IT security incidents to the relevant stakeholders in a timely manner as appropriate according to their severity as laid down in Article 15;

(q) for outsourced systems, ensure that appropriate IT security provisions are included in the outsourcing contracts and that IT security incidents occurring in the outsourced CIS are reported in accordance with Article 15;

(r) for CIS providing shared IT services, ensure that a defined security level is provided, clearly documented and security measures are implemented for that CIS in order to reach the defined security level.

3. System owners may formally delegate some or all of their IT security tasks but they remain responsible for the IT security of their CIS

The processes related to these responsibilities and activities shall be further detailed in implementing rules.

Article 10

Data owners

1. The data owner is responsible for the IT security of a specific data set to the Head of the Commission department and is accountable for the confidentiality, integrity and availability of the data set.

2. In relation to this data set, the data owner shall:

(a) ensure that all data sets under his or her responsibility are appropriately classified in accordance with Decision (EU, Euratom) 2015/443 and (EU, Euratom) 2015/444;

(b) define the information security needs and inform the relevant system owners of these needs;

(c) participate in the CIS risk assessment;

(d) report any unresolvable disagreements between the data owner and the system owner to the head of the Commission department;

(e) communicate IT security incidents as provided for in Article 15.

3. Data owners may formally delegate some or all of their IT security tasks but they maintain their responsibilities as defined in this Article.

The processes related to these responsibilities and activities shall be further detailed in implementing rules.

Article 11

Local Informatics Security Officers (LISOs)

In relation to IT security, the LISO shall:

(a) proactively identify and inform system owners, data owners and other roles with IT security responsibilities in Commission department(s) about the IT security policy;

(b) liaise on IT-security-related issues in Commission department(s) with the Directorate-General for Informatics as part of the LISO network;

(c) attend the regular LISO meetings;

(d) maintain an overview of the information security risk management process and of the development and implementation of information system security plans;

(e) advise data owners, system owners and heads of Commission departments on IT-security-related issues;

(f) cooperate with the Directorate-General for Informatics in disseminating good IT security practices and propose specific awareness-raising and training programmes;

(g) report on IT security, identify shortfalls and improvements to the Head of the Commission department(s).

The processes related to these responsibilities and activities shall be further detailed in implementing rules.

Article 12

Users

1. In relation to IT security, users shall:

(a) comply with the IT security policy and the instructions issued by the system owner on the use of each CIS;

(b) communicate IT security incidents as provided for in Article 15.

2. Use of the Commission's CIS in breach of the IT security policy or instructions issued by the system owner may give rise to disciplinary proceedings.

The processes related to these responsibilities and activities shall be further detailed in implementing rules

CHAPTER 3

SECURITY REQUIREMENTS AND OBLIGATIONS

Article 13

Implementation of this Decision

1. The adoption of the implementing rules on Article 6, and of the related standards and guidelines, will be subject to an empowerment decision by the Commission in favour of the Member of the Commission responsible for security matters.

2. The adoption of all other implementing rules in relation to this decision, and of the related IT security standards and guidelines, will be subject to an empowerment decision by the Commission in favour of the Member of the Commission responsible for informatics.

3. The ISSB shall approve the implementing rules, standards and guidelines mentioned under paragraphs 1 and 2 above prior to their adoption.

Article 14

Obligation to comply

1. Compliance with the provisions outlined in the IT security policy and standards is mandatory.

2. Non-compliance with the IT security policy and standards may trigger liability to disciplinary action in accordance with the Treaties, the Staff Regulations and the CEOS, to contractual sanctions and/or to legal action under national laws and regulations.

3. The Directorate-General for Informatics shall be notified of any exceptions to the IT security policy.

4. In the event the ISSB decides there is a persistent unacceptable risk to a CIS of the Commission, the Directorate-General for Informatics in cooperation with the system owner shall propose mitigating measures to the ISSB for approval. These measures may, amongst others, include reinforced monitoring and reporting, service limitations and disconnection.

5. The ISSB shall impose the implementation of approved mitigating measures wherever necessary. The ISSB may also recommend to the Director-General of the Directorate-General for Human Resources and Security to open an administrative enquiry. The Directorate-General for Informatics shall report to the ISSB on every situation when mitigating measures are imposed.

The processes related to these responsibilities and activities shall be further detailed in implementing rules

Article 15

IT security incident handling

1. The Directorate-General for Informatics is responsible for providing the principal operational IT security incident response capability within the European Commission.

2. The Directorate-General for Human Resources and Security as contributing stakeholders to the IT security incident response shall:

(a) have the right to access summary information for all incident records and full records upon request;

(b) participate in IT security incidents crisis management groups and IT security emergency procedures;

(c) be in charge of relations with law enforcement and intelligence services;

(d) perform forensic analysis regarding cyber-security in accordance with Article 11 of Decision (EU, Euratom) 2015/443;

(e) decide on the need to launch a formal inquiry;

(f) inform the Directorate-General for Informatics of any IT security incidents that may present a risk to other CISs.

3. Regular communications shall take place between the Directorate-General for Informatics and the Directorate-General for Human Resources and Security to exchange information and coordinate the handling of security incidents, in particular any IT security incident that may require a formal inquiry.

4. The incident coordination services of Computer Emergency Response Team for the European institutions, bodies and agencies ('CERT-EU') may be used to support the incident handling process when appropriate and for knowledge sharing with other EU institutions and agencies that may be affected.

5. System owners involved in an IT security incident shall:

(a) immediately notify their Head of Commission Departments, the Directorate-General for Informatics, the Directorate-General for Human Resources, the LISO and, where appropriate, the data owner of any major IT security incidents, in particular those involving a breach of data confidentiality;

(b) cooperate and follow the instructions of the relevant Commission authorities on incident communication, response and remediation.

6. Users shall report all actual or suspected IT security incidents to the relevant IT helpdesk in a timely manner.

7. Data owners shall report all actual or suspected IT security incidents to the relevant IT security incident response team in a timely manner.

8. The Directorate-General for Informatics, with support from the other contributing stakeholders, is responsible for handling any IT security incident detected in relation to Commission CISs that are not outsourced systems.

9. The Directorate-General for Informatics shall inform affected Commission departments about IT security incidents, the relevant LISOs and, where appropriate, the CERT-EU on a need-to-know basis.

10. The Directorate-General for Informatics shall regularly report on major IT security incidents affecting the Commission's CIS to the ISSB.

11. The relevant LISO shall, upon request, have access to IT security incident records concerning the CIS of the Commission department.

12. In case of a major IT security incident, the Directorate-General for Informatics shall be the contact point for the management of the crisis situations by coordinating the IT security incidents crisis management groups.

13. In case of an emergency the Director-General of the Directorate-General for Informatics can decide to launch an IT security emergency procedure. The Directorate-General for Informatics shall develop emergency procedures to be approved by the ISSB.

14. The Directorate-General for Informatics shall report on the execution of emergency procedures to the ISSB and the heads of Commission departments affected.

The processes related to these responsibilities and activities shall be further detailed in implementing rules.

CHAPTER 4

FINAL PROVISIONS

Article 16

Transparency

This Decision shall be brought to the attention of Commission staff and to all individuals to whom it applies, and published in the *Official Journal of the European Union*.

Article 17

Relation to other acts

The provisions of this decision are without prejudice to Decision (EU, Euratom) 2015/443, Decision (EU, Euratom) 2015/444, Regulation (EC) No 45/2001, Regulation (EC) No 1049/2001 of the European Parliament and of the Council ([1]), Commission Decision 2002/47/EC, ECSC, Euratom ([2]), Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council ([3]), Decision 1999/352/EC, ECSC, Euratom.

Article 18

Repeal and transitional measures

Decision C(2006) 3602 of 16 August 2006 is repealed.

The implementing rules and IT security standards adopted pursuant to Article 10 of Decision C(2006) 3602 shall remain in effect insofar as they do not conflict with this decision, until they are replaced by the implementing rules and standards to be adopted under Article 13 of this decision. Any reference to Article 10 of Decision C(2006)3602 shall be read as a reference to Article 13 of this decision.

Article 19

Entry into force

This decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Done at Brussels, 10 January 2017.

For the Commission
The president
Jean-Claude JUNCKER

([1]) 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 (OJ L 145, 31.5.2001, p. 43).
([2]) Commission Decision 2002/47/EC, ECSC, Euratom of 23 January 2002 amending its Rules of Procedure (OJ L 21, 24.1.2002, p. 23).
([3]) Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18.9.2013, p. 1).