COMMISSION DECISION (EU, Euratom) 2018/559

of 6 April 2018

laying down implementing rules for Article 6 of Decision (EU, Euratom) 2017/46 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,

Having regard to Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission ([1]), and in particular Article 6 thereof,

Whereas:

(1) With the adoption of Decision (EU, Euratom) 2017/46, there is a need for the Commission to review, update and consolidate the implementing rules linked to the repealed Commission Decision C(2006) 3602 on the security of communication and information systems used by the Commission.

(2) The member of the Commission responsible for security, in full compliance with the internal rules of procedures, has been empowered to establish implementing rules in line with Article 13 of Decision (EU, Euratom) 2017/46 ([2]).

(3) The implementing rules of Decision C(2006) 3602 should therefore be repealed,

HAS ADOPTED THIS DECISION:

CHAPTER 1

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. The subject matter and scope of this Decision are provided in Article 1 of Decision (EU, Euratom) 2017/46.

2. The provisions in this Decision apply to all communication and information systems (CISs). However, the responsibilities defined in this Decision shall not apply to CISs handling EU classified information. The relevant responsibilities for these systems shall be determined by the system owner and the Commission Security Authority in line with Commission Decision (EU, Euratom) 2015/444 ([3]).

3. Chapter 2 of this Decision presents an overview of the practical implementation of the organisation and responsibilities relating to IT security. Chapter 3 of this Decision presents an overview of the processes relating to Article 6 of Decision (EU, Euratom) 2017/46.

Article 2

Definitions

The definitions in Article 2 of Decision (EU, Euratom) 2017/46 apply to this Decision. For the purposes of this Decision the following definitions shall also apply:

1. 'Crypto Approval Authority' (CAA) is a function assumed by the Commission Security Authority that falls under the authority of the Director-General for Human Resources and Security;

([1]) OJ L 6, 11.1.2017, p. 40.
([2]) Commission Decision C(2017) 7428 final of 8 November 2017 granting an empowerment to adopt implementing rules, standards and guidelines relating to the security of communication and information systems in the European Commission.
([3]) 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).

2. 'External network connection' means any electronic communications connection between the Commission's internal network and any other network, including the internet. This definition excludes third party networks that are provided under contract to be part of the Commission's internal network.

3. 'Key escrow' means a procedure for storing copies of cryptographic keys with one or more separate parties, ensuring the segregation of duties, to enable their recovery in case the operational copy is lost. Keys may be split into two or more parts, each of which is lodged with a different party to ensure that no single party possesses the entire key.

4. 'RASCI' is an abbreviation for a responsibility assignment based on the following attribution indicators:

(a) 'responsible' (R) means having the obligation to act and take decisions to achieve required outcomes;

(b) 'accountable' (A) means being answerable for actions, decisions and performance;

(c) 'supports' (S) means having the obligation to work with the person responsible to complete the task;

(d) 'consulted' (C) means being sought for advice or opinion;

(e) 'informed' (I) means being kept up to date with relevant information.

CHAPTER 2

ORGANISATION AND RESPONSIBILITIES

Article 3

Roles and responsibilities

The roles and responsibilities relating to Articles 4 to 8 of this Decision are defined in the Annex in accordance with the RASCI model.

Article 4

Alignment with the Commission's information security policy

1. The Directorate-General for Human Resources and Security shall review the Commission's IT security policy and related standards and guidelines to ensure that they are in line with the Commission's general security policies, in particular Commission Decision (EU, Euratom) 2015/443 ([1]) and Decision (EU, Euratom) 2015/444.

2. Upon request by other Commission departments, the Directorate-General for Human Resources and Security may review their IT security policies or other IT security documentation to ensure their consistency with the Commission's information security policy. The head of the Commission department concerned shall ensure that any inconsistencies are addressed.

3. Under its responsibility for the security of information, the Directorate-General for Human Resources and Security shall cooperate with the Directorate-General for Informatics to ensure that the IT security processes take full account of the classification and principles of security laid down in Decision (EU, Euratom) 2015/443, in particular Articles 3 and 9.

CHAPTER 3

IT SECURITY PROCESSES

Article 5

Encrypting technologies

1. The use of encrypting technologies for the protection of EU classified information (EUCI) shall comply with Decision (EU, Euratom) 2015/444.

2. The decisions on the use of encrypting technologies for the protection of non-EUCI data shall be taken by the system owner of each CIS, taking into account both the risks that are intended to be mitigated through encryption and the risks that it introduces.

3. Prior approval from the CAA is required for all uses of encrypting technologies, unless the encryption is used only to protect the confidentiality of non-EUCI data in transit and uses standard network communications protocols.

([1]) Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).

4. With the exception noted in paragraph 3 of this Article, Commission departments shall ensure that back-ups of any decryption keys are stored in key escrow for the purpose of recovering stored data in the event that the decryption key is not available. The recovery of encrypted data using back-ups of decryption keys shall be carried out only when authorised in line with the standard defined by the CAA.

5. Requests for approval for the use of encrypting technologies shall be formally documented and shall include details of the CIS and data to be protected, the technologies to be used and the related security operating procedures. These requests for approval shall be signed by the system owner.

6. Requests for approval for the use of encrypting technologies shall be evaluated by the CAA in line with the published standards and requirements.

Article 6

IT security inspections

1. The Directorate-General for Human Resources and Security shall undertake IT security inspections in order to verify whether IT security measures comply with the Commission's IT security policies and to check the integrity of these control measures.

2. The Directorate-General for Human Resources and Security may perform an IT security inspection:

(a) on its own initiative;

(b) on request from the Information Security Steering Board (ISSB);

(c) on a request received from a system owner;

(d) further to a security incident; or

(e) further to the identification of a high risk to a particular system.

3. Data owners may request an IT security inspection before storing their information in a CIS.

4. The results of an inspection shall be documented in a formal report to the system owner, and copied to the LISO, that includes findings and recommendations for improving the CIS's compliance with the IT security policy. The Directorate-General for Human Resources and Security shall report significant issues and recommendations to the ISSB.

5. The Directorate-General for Human Resources and Security shall monitor the implementation of the recommendations.

6. Where appropriate, IT security inspections shall include the inspection of services, premises and equipment provided to the system owner, including both internal and external service providers.

Article 7

Access from external networks

1. The Directorate-General for Human Resources and Security shall lay down the rules in a standard on authorising access between Commission CISs and external networks.

2. The rules shall distinguish different types of external network connections and lay down appropriate security rules for each type of connection, including whether a prior authorisation for the connection is required from the relevant authority as noted in paragraph 4 of this Article.

3. If required, authorisation shall be granted on the basis of a formal request and approval process. The approval shall be valid for a specified duration and shall be obtained before the connection is activated.

4. The Directorate-General for Human Resources and Security shall have the overall responsibility for authorising requests, but may delegate the responsibility for authorising some types of connection at its own discretion in line with Article 17(3) of Decision (EU, Euratom) 2015/443 and subject to the conditions laid down under (8).

5. The authorising entity may impose additional security requirements as a prerequisite for approval, in order to protect the Commission's CIS and networks from the risks of unauthorised access or other security breaches.

6. The Directorate-General for Informatics is the standard provider of network services for the Commission. Any other Commission department operating a network that is not provided by the Directorate-General for Informatics shall first obtain the agreement of the ISSB. The Commission department shall document the business justification for the request and demonstrate that the network controls are sufficient to meet the requirements for controlling incoming and outgoing flows of information.

7. The system owner of a CIS shall determine the security requirements for external access to that CIS and shall ensure the implementation of appropriate measures to protect its security, with the support of the LISO.

8. The security measures implemented for external network connections shall be based on the principles of need-to-know and least privilege, which ensure that individuals only receive the information and access rights that they need to perform their official duties for the Commission.

9. All external network connections shall be filtered and monitored to detect potential security breaches.

10. Where connections are established to allow the outsourcing of a CIS, the authorisation shall be conditional on the successful completion of the procedure described in Article 8.

Article 8

Outsourcing of CISs

1. For the purposes of this Decision, a CIS is considered to be outsourced when it is provided on the basis of a contract with a third party contractor, under which the CIS is housed on non-Commission premises. This includes the outsourcing of individual or multiple CISs or other IT services, data centres on non-Commission premises, and the handling of Commission data sets by external services.

2. The outsourcing of a CIS shall take into account the sensitivity or classification of the information handled as follows:

(a) CISs handling EUCI shall be accredited in accordance with Decision (EU, Euratom) 2015/444, and the Commission Security Accreditation Authority (SAA) shall be consulted in advance. Systems handling EUCI shall not be outsourced.

(b) The system owner of a CIS handling non-EUCI information shall implement proportionate measures to address the security needs in line with the relevant legal obligations or the sensitivity of the information, taking into account the risks of outsourcing. The Directorate-General for Human Resources and Security may impose additional requirements.

(c) Outsourced development projects shall take into account the sensitivity of the developed code and any test data used during development.

3. The following principles shall apply to outsourced CIS in addition to those laid down in Article 3 of Decision (EU, Euratom) 2017/46:

(a) outsourcing arrangements shall be designed to avoid dependency on specific suppliers;

(b) outsourcing security arrangements shall minimise the possibilities for third party staff to access or modify Commission information;

(c) third party staff that have access to an outsourced CIS shall provide confidentiality agreements;

(d) the outsourcing of a CIS shall be indicated in the inventory of CISs.

4. The system owner with the participation of the data owner shall:

(a) assess and document the risks relating to outsourcing;

(b) lay down relevant security requirements;

(c) consult with the system owners of all other connected CISs to ensure that their security requirements are included;

(d) ensure that appropriate security requirements and rights are included in the outsourcing contract;

(e) fulfil any other requirements laid down in the detailed procedure as noted in paragraph 8 of this Article.

These actions shall be completed before the contract or other agreement is signed for the outsourcing of one or more CISs.

5. System owners shall manage the risks relating to outsourcing during the lifetime of the CIS in order to meet the defined security requirements.

6. System owners shall ensure that third party contractors are obliged to immediately notify the Commission of all IT security incidents affecting an outsourced Commission CIS.

7. The system owner is responsible for ensuring the compliance of the CIS, the outsourcing contract and the security arrangements with the Commission's rules on information security and IT security.

8. The Directorate-General for Human Resources and Security shall lay down the detailed standard related to the responsibilities and activities set out in points (1) to (7) in accordance with Article 10 below.

CHAPTER 4

MISCELLANEOUS AND FINAL PROVISIONS

Article 9

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 10

Standards

1. The provisions of this Decision shall, where necessary, be further detailed in standards and/or guidelines to be adopted in line with Decision (EU, Euratom) 2017/46 and with Decision C(2017) 7428. IT security standards and guidelines shall provide further details on these implementing rules and Decision (EU, Euratom) 2017/46 for specific security domains according to ISO 27001:2013 Annex A. These standards and guidelines are based on industry best practices and are selected to suit the Commission's IT environment.

2. Standards shall, where necessary, be developed according to ISO 27001:2013 Annex A in the following domains:

(1) organisation of information security;

(2) human resources security;

(3) asset management;

(4) access control;

(5) cryptography;

(6) physical and environmental security;

(7) operational security;

(8) communications security;

(9) system acquisition, development and maintenance;

(10) supplier relationships;

(11) information security incident management;

(12) information security aspects of business continuity management;

(13) compliance.

3. The ISSB shall approve the standards mentioned under paragraph 1 and 2 of this Article before their adoption.

4. The implementing rules to Decision C(2006) 3602 related to the scope of this Decision are hereby repealed.

5. The standards and guidelines adopted under Decision C(2006) 3602 of 16 August 2006 shall remain in effect, insofar as they do not conflict with these implementing rules, until they are repealed or replaced by standards or guidelines to be adopted under Article 13 of Decision (EU, Euratom) 2017/46.

Article 11

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, 6 April 2018.

For the Commission,
On behalf of the President,
Günther OETTINGER
Member of the Commission

ANNEX

ROLES AND RESPONSIBILITIES (RASCI)

The RASCI model assigns roles to entities using the following abbreviations:

(a) R — Responsible;

(b) A — Accountable;

(c) S — Supporting;

(d) C — Consulted;

(e) I — Informed.

Role / Process	ISSB	HR (DS)	Commission Departments	System Owner	Data Owner	LISO	DIGIT	Contractors
Alignment with the Commission's information security policy		**R/A**	**S**				**S**	
Encrypting technologies		**C**	**A**	**R**	**I**	**C**		
IT Security Inspections	**I**	**A/R**		**S**	**I**	**I**	**S**	
Access from external networks	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Outsourcing of CISs		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] The ISSB is consulted in relation to the operation of internal networks by any Commission department other than the Directorate-General for Informatics.

[2] The system owner of a CIS being outsourced shall be responsible, and the system owner of any other CIS with which an outsourced CIS interconnects shall be consulted.