Publications Office

Information Security Management

Publications Office Minimum Security Requirements

Type	Minimum Security Requirements	Status	Final
Version	4.2.3	Date	09/02/2021
Reference	MSR	Language	EN

References

Version	Name
2021-2022	EC IT SECURITY STRATEGY
CD 2017/46	COMMISSION DECISION (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission

Revision history

Version	Name
1.0.0	Initial release
4.2.3	Update

Table of contents

1. INTRODUCTION

1.1. Legal Context

The Commission's communication and information systems (CIS) 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. […]. The goal of IT security in the Commission is to ensure that the Commission's CISs will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.

This high level goal of IT security is extracted from the Commission Decision (EU, Euratom) 2017/46 [1]. It is further refined in the Implementing Rules and detailed in accompanying standards and guidelines as presented in the following sections of this document.

The Commission Decision 2017/46, has been adopted on 10 January 2017, replacing the former Commission Decision 2006/3602. Together with its implementing rules it defines the Commission's IT security policy. The decision lays down the principles of IT security within the Commission, its applicability and the roles and responsibilities of the key stakeholders involved in the Commission's IT security governance. It applies to all Communication and Information Systems (CISs) which are owned, procured, managed or operated by or on behalf of the Commission.

Specifically, this decision sets out the basic principles, objectives, organisation and responsibilities regarding the security of the CISs, and in particular for Commission departments owning, procuring, managing or operating CISs, 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 [1].

The Implementing Rules C(2017) 8841 of Commission decision 2017/46 [2] have been adopted on 13 December 2017, replacing the former implementing rules of Commission Decision 2006/3602. The provisions in this decision apply to all CIS[1].

The Implementing Rules lay down the main processes involved in IT security within the Commission, covering all the essential parts of the lifecycle of a CIS, and specify more detailed roles and responsibilities of the stakeholders involved in the Commission wide IT security governance. Specifically, the Commission Decision 2017/8841 sets out the main tasks in each core IT security process and assigns clear responsibilities regarding these IT systems.

[1] 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 in line with Decision (EU, Euratom) 2015/444 by the System Owner and the Commission Security Authority.

1.2. Subject matter and scope of this document

Due to the complexity of the subject matter, the Implementing Rules of Commission Decision 2017/46 do not include all detailed procedures and rules. These are published in the related IT Security standards and guidelines [3]. Some IT Security standards have been updated, others may be under revision. For each standard it is stipulated that until the update is available, the IT security standards adopted pursuant to Article 10 of Commission Decision 2006/3602 shall remain in effect insofar as they do not conflict with the new decision. Additional guidance is also published in some domains as IT security guidelines.

In this context, Publications Office specified a set of minimum IT security requirements for the design, development, operation, management and support of existing or procured CISs, based on the Commission's existing IT security standards and guidelines. Although the IT security requirements presented in the following sections set out the IT security baseline for all CIS owned, procured, managed or operated by or on behalf of the Publications Office, this document constitutes a brief reference guide to the Commission's IT security standards and guidelines and does not, under any circumstance, substitue them.

The following requirements apply to all IT Systems in the Commission, either hosted on-premises or in the Cloud, providing the minimum set of requirements with which the Publications Office CIS shall also comply. Mandatory requirements are subject to compliance verification. Some requirements specified in the standards are recommended, hence not subject to compliance verification, which means they shall be used as a guidance and they are based on market best practices. These recommended requirements shall be under consideration to become mandatory in the future. Exceptions must be handled in accordance with Article 8.3.d.iv of Commission Decision (EU, Euratom) 2017/8841 (Implementing Rules for Commission Decision (EU, Euratom) 2017/46.

The Publications Office list of minimum security requirements are categorised based on the specific IT security domains indicated in the title of each section, whereas each sub-section provides a brief presentation of the related IT security standards and/or guidelines along with the corresponding reference to the original document. Taking into consideration that the IT security standards adopted pursuant to Article 10 of Commission Decision 2006/3602 shall remain in effect insofar as they do not conflict with the new decision, they are also included in the list of minimum security requirements for the CIS procured, owned or managed by the Publications Office.

For more detailed information, the reader is encouraged to retrieve the original documents of referenced IT security standards and guidelines any other related documentation as indicated in the last section of the document.

1.3. Responsibilities of the System Owner

The System Owner is the individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of a CIS.

The **System Owner** is responsible for:

- applying the security requirements to the project and allocating financial, technical and human resources as required for meeting the security requirements of the project.
- ensuring that the security controls are tested and validated during acceptance test phase.
- maintaining the security controls throughout the life cycle of the product or the application.

Where the security functionality in a proposed product does not satisfy specific security requirements, the risk introduced must be evaluated and additional controls must be reconsidered prior to purchasing the product. Where additional functionality is supplied and causes a security risk, this must be disabled and the proposed control structure must be reviewed to determine the additional controls that should be deployed to ensure the secure use of the enhanced functionality.

Design reviews must be conducted at periodic intervals during the development process to assure that the proposed design will satisfy the functional and security requirements.

Decisions not to implement security controls or to implement alternative controls, must be subject to formally documented exemptions describing the residual risks. The exemption approval process must conclude with the System Owner's final decision.

1.4. Responsibilities of the Project Manager

The Project Manager manages the daily progress of the project to deliver the outputs within the agreed constraints.

When delegated by the System Owner, the **Project Manager** is responsible for:

- ensuring that a secure system development lifecycle is applied and that the necessary IT security clauses are included in contracts with external parties.
- ensuring the specification of the IT security requirements.
- applying the security measures based on the Commission’s standards and other regulations and legislation.
- ensuring that the security measures are implemented in the IT system or in the infrastructures that support it.
- ensuring that the design, installation and implementation of the system are in accordance with the IT security requirements of the IT system and the IT security standards.

- the deployment and hand-over of the IT system to the System Owner.
- evaluating the cost of the required IT security measures and may request not to implement measures if approved by the System Owner.

1.5. Responsibilities of the System Supplier

The System Supplier implements the technical architecture and security measures of a system based on the IT security requirements, supports in developing those security requirements and performs appropriate security testing.

When delegated by the System Owner, the **System Supplier** is responsible for:

- defining the technical architecture and drawing up technical specifications for the implementation of the IT security requirement.
- constructing and ensuring the development of the IT system in accordance with the IT security requirement.
- ensuring good quality by performing code reviews and security tests of applications prior to their deployment in production.
- providing operating manuals and instructions for the System Manager who manages and/or operates the IT system on behalf of the System Owner.

1.6. Responsibilities of the System Security Officer

The System Security Officer advises the System Owner, System Manager and Project Manager on the IT security approach and takes an active role as IT security expert to define IT security requirements and assists in the architecture, design, implementation and verification activities of IT security.

When delegated by the System Owner, the **System Security Officer** is responsible for:

- taking delegated responsibility for the activities in the IT Security Risks Management process:
    - perform, in collaboration with the relevant stakeholders, in particular the Data Owner or other linked System Owners, a business impact assessment to identify the IT security needs based on the required levels of confidentiality, integrity and availability of the IT system.
    - draw up security plans that shall contain the key output of the IT risk management process, in particular, the IT security needs, IT security measures and selection rationale, residual risks, risk acceptance criteria and exceptions with a timespan of their validity.

- supporting the specification of IT security requirements, the definition of IT security architecture, and the implementation and verification of security measures during the IT project.

2. INORMATION CLASSIFICATION

The **confidentiality** of information is assessed according to the damage that unauthorised disclosure may cause to the interests of the Commission, the European Union or one or more of its Member States, or other stakeholders such as businesses and European citizens.

A realistic classification in terms of confidentiality must be aproved by the System Owner.

Publications Office does not deal with EU CLASSIFIED information (EUCI) in the scope of its daily business, therefore the security requirements for EU CLASSIFIED information are out-of-scope of this document. In exceptional cases where this might be the case, classified information and data will be managed using specific security procedures based on the Commission decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information.

The confidentiality levels for **non-EUCI** are defined as follows:

Confidentiality level	Description
Publicly available (PA)	Information that is, or is ready to be, published[2].
Commission use (CU)	Information that is not for public use and does not fall into higher categories.
Sensitive Non Classified (SNC)	Information that the Commission must protect because of legal obligations or because of its sensitivity. SNC information must be marked[3].

The originator of a document or other information asset must determine the appropriate level based on the definitions above.

According to the security notice of the European Commission on marking and handling fo sensitive non-classified information, SNC is information or material the Commission must protect because of legal obligations laid down in the Treaties or in acts adopted in implementation thereof, and/or because of its sensitivity [4].

Examples of this type of information may include:

- Commission's Acts (decisions, opinions, recommendations, …) and Commission's proposals (for final adoption of the European Parliament and/or the Council) bearing a marking;
- Some documents involved in trade negotiations;
- Some procurement documents, where relevant;
- Personal data, especially the special categories of data defined in Article 10 of Regulation (EU) 2018/1725(4);

[2] Note that many documents are sensitive before they are published, and so the draft documents may need to be protected at a higher level than the final documents after the date of publication.

[3] Security Notice on Marking and handling of sensitive non-classified information.

- Sensitive business information of third parties;
- Evidence in administrative, competition or criminal investigations;
- Certain audit reports, depending on the subject matter;
- Certain security-related documents, depending on the subject matter;
- Certain sensitive documents forming part of the policy and legislation development process, or parts thereof.

Especially for "Sensitive Non Classified Information", appropriate security markings must be applied to documents to indicate relevant restrictions and handling instructions in line with the security notice on marking and handling of sensitive non-classified information. Emails containing SNC information must be protected by approved protection mechanisms such as S-MIME (with external partners).

SNC information may be communicated to external entities with formal permission from the author or Data Owner, with written instructions not to distribute outside a specified audience.

Integrity includes principles such as authenticity and non-repudiation, and relates to the required level of confidence in the accuracy and the source of information. The **availability** rating is used to determine the business continuity requirements. The impact definitions in the table below are related to the impacts for confidentiality.

Integrity / Availability Level	Rating	Impact and Scope
1	Very Low	No or negligible damage to the Commission or other stakeholders.
2	Low	Minor damage to the Commission or other stakeholders[5].
3	Medium	Significant damage to the Commission or other stakeholders.

Integrity and availability are typically addressed in the IT security risk management process (see section 4.1).

[4] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

[5] The stakeholders mentioned at levels 2 and 3 do not include Member States.

3. SECURITY BY DESIGN

The security by design approach is enabled over the entire life cycle of an information system. It is acknowledged as a risk-based approach as the IT security plans need to be consistently done as part of the design phase of a system, to enable security by design. Therefore, it should start with an IT Security risks assessment, data classification and an IT Security plan (see [27] for more details).

The framework used for the IT Security Risk Management Processes, is the *IT Security Risk Management Methodology (ITSRM²)* [21]. The *ITSRM² Security Plan Template Guideline* document can be used as a supporting tool to elaborate the Security Plan [22] (see section 4 for further information on risk management).

The *Guidelines on Secure systems Lifecycle – S²LC* [5] focus on Life-Cycle Processes as part of IT Security in System Development and Operation. These guidelines do not substitute the existing standards. Their role is to position pragmatically all the security requirements mandated in the legal bases in the global life-cycle of any IT System, from its inception to its decommissioning.

Achieving this goal in practice relies on five main principles:

1. Consider security as a global process, not as a product, and consider security measures as processes to implement in an organized way; for example, encryption is a process that can be implemented in a system to protect information in transit;
2. Instilling security processes throughout the whole life-cycle of the system/information, at the correct place and moment, from initiation to end of life;
3. Defining appropriately these security processes by following a risk-based approach (itself a process);
4. Managing these security processes (Management System) and
5. Improving continuously these security processes to ensure they stay appropriate during the whole life-cycle (also known as Deming virtuous cycle, or PDCA for PLAN-DO-CHECK-ACT).

The *S²LC – IT Security in System Life-Cycle* document provides a global view on the security processes required to implement these principles to develop and operate appropriately protected Systems, from their inception to their decommissioning. It will be complemented by various topic-specific documents detailing how to implement these security processes, as for example the ITSRM² risk management methodology and the ITSRM² Security Plan guidelines which are the main pillars of the risk-based approach that should be followed.

3.1. Secure Systems Development

Software applications must be secured in order to protect them from accident or abuse. The necessary controls must be built into information systems, and the earlier that this is done, the better,

since adding them later on is more costly and likely to leave vulnerabilities if the applications have not been designed with security in mind.

The *standard on secure systems development [6]* provides instructions for the processes relating to the acquisition, development and maintenance of information systems. The objective is to ensure that appropriate security controls are identified and included in such systems, and that risks such as the introduction of unauthorised code are minimised. The standard also contains specific controls for outsourced software development.

Minimum security requirements are specificed for the following topics:

1. Correct processing in applications
2. Secure development envrionment
3. Security in development and support processes
4. Outsourced software development

This standard applies to all information systems that are acquired or developed by or on behalf of the European Commission. The measures mandated by this standard must be followed by all relevant personnel, including all Commission officials, contractors and third parties involved in this process.

3.2. Web Application Security

Building secure web applications, a holistic approach to application security is required and security must be applied at all three layers: application, host and network. The security *standard on web application security [7]* covers the design, development and deployment of a web application. It establishes principles that developers should respect over the different phases of the web application lifecycle. Certain requirements have been suggested as recommended, and compliance with them may be evaluated on a case-by-case basis, based on a risk assessment. Mandatory requirements, however, apply to any web application, regardless of its exposure, nature, functionalities or published information.

The purpose of this standard is to define the minimum set of security requirements which need to be satisfied in order to design, build and configure secure web applications, ensure resilience over attacks and limit the extent of damage should an attack occur. It sets the baseline of the security requirements for any new or existing web application within the European Commission in the following domains:

- Authentication
- Session management
- Access control
- Input validation and output sanitization
- Communications

- Data protection
- Secure handling of resources
- Error and exception handling
- Logging
- Mobile applications
- Host and Network Security
- Deployment

The defined requirements apply to all IT Systems in the Commission, either hosted on-premises or in the Cloud, providing the minimum set of requirements with which the applications shall comply. Mandatory requirements are subject to compliance verification. Some requirements in this standard are recommended, hence not subject to compliance verification, which means they shall be used as a guidance and they are based on market best practices. Exceptions to mandatory requirements must be handled according to the article 8.3.d.iv of the Implementing Rules of the Commission Decision 2017/46.

The reader is also encouraged to take into consideration the *"Web application secure development guidelines" [8]* where technical issues regarding application level security are identified and addressed by presenting the main types of vulnerabilities and suggesting related countermeasures. Furthermore, additional checklists (cheat sheets) of web application vulnerabilities can be found in the *Open Source Security Testing Methodology Manual (OSSTMM) [9]* and on the *Open Web Application Security Project (OWASP) [10].*

4. OUTSOURCING PRINCIPLES

The Commission Decision 2017/46 defines outsourcing as follows: a Commission 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.

The main criterion for the definition of outsourcing is the location of the computer hardware, since the legal jurisdiction in which the computer systems reside is a key factor in many of the related risks.

The System Owners of outsourced systems are responsible for the security of their systems and information, and for ensuring that the appropriate measures are implemented and adequately documented.

In order to maintain appropriate control of the security of the information, the outsourced CIS should follow 12 security rules:

1. Outsourced information must be identified and categorized.
2. Commission Use (CU) and sensitive non-classified (SNC) information must be hosted within the European Union, as well as personal data.
3. Relevant legal requirements and conditions must be included in the outsourcing contract.
4. Commission information must be isolated from other clients of the outsourcing provider.
5. Authentication mechanisms and credentials must be controlled by the Commission.
6. The availability of Commission information must be ensured.
7. The availability of a security-related logs must be ensured.
8. A security incident response procedure must be in place.
9. External network connections must be approved.
10. Persistent encryption mechanisms must be under the control of the Commission.
11. Access to Commission information by service provider staff must be minimised.
12. Outsourcing must be recorded in GovIS 2 (the internal EC CISs portfolio system).

5. IT SECURITY MANAGEMENT

The legal basis for IT Security Management as expressed in the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 states: "*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*" ([CD46/2017] Art.3 §4).

Also, the Commission decision 2017/46, under the Article 8, specifies that each Head of Commission department shall "*ensure that appropriate IT security risk assessments and IT security plans have been made and implemented*".

Therefore, in order to support one of the principles for IT security in the Commission as described also in the Article 3, "*IT security plans and IT security measures shall be proportionate to the security needs of the CIS"*, after performing a risk assessment using the *IT Security Risk Manamagent Methodology ITSRM² [21]*, the *ITSRM² Security Plan Template Guideline [22]* shall be used as a supporting tool to elaborate the related security plan.

5.1. Information Security Risk Management

Every Communication and Information System is exposed to IT security threats, giving rise to IT Security Risks. As any other organisation, the Publications Office must ensure the appropriate IT Security of its CIS.

Achieving this goal in practice relies on five main principles [25]:

1. Consider security as a process, not as a product, and consider security controls as processes to implement in an organized way;
2. Instilling security processes throughout the whole life-cycle of the system/information, at the correct place and moment, from initiation to end of life;
3. Defining appropriately these security processes by following a risk-based approach (itself a process);
4. Managing these security processes (Management System) and
5. Improving continuously these security processes to ensure they stay appropriate during the whole life-cycle (a.k.a. PLAN-DO-CHECK-ACT).

The *standard on Information Security Risk Management [26]* defines the risk management process for the CIS of the European Commission with the aim to provide a consistent framework in which the risks related to information systems are identified, considered and addressed. It defines the minimal steps an information security risk management process must implement:

1. Scope definition
2. Asset identification and classification

3. Risk identification
4. Risk assessment
5. Risk treatment
6. Risk acceptance
7. Risk monitoring
8. Risk communication

As already mentioned, the ITSRM^2 risk management methodology and the related ITSRM^2 Security Plan guidelines shall be used as the most appropriate supporting tools for applying this standard.

5.2. IT Asset Management

The IT security *standard on IT Asset Management [23]* is based on Commission Decision (EU, Euratom) 2017/46 on the security of communication and information systems in the European Commission and Commission Decision laying down implementing rules for Articles 3, 5, 7-15 of Decision 2017/46, C (2017) 8841, in particular its Article 12.

The objective of IT Asset Management is to ensure that all IT assets are uniquely identified, have an identified owner and have appropriate IT security responsibilities assigned to them. IT asset management is a key process supporting other IT security management processes, and shall consist of:

a) Identifying and inventorying: ensuring that all IT assets under the responsibility of Commission Departments are formally assigned to a System Owner and are registered and maintained accurately in the Commission IT asset inventory.

b) Managing the IT assets: defining and applying rules for managing and reviewing IT assets from their planning and purchase, registration, through their handling, until their disposal following a workflow-based approach.

c) Maintaining any other specific inventory of IT assets in full coherence with the Commission IT asset inventory.

The provisions in this IT Security Standard cover the aspects of IT Asset Management necessary to support other IT Security processes and apply to all IT systems in the Commission. The principles of IT Asset Management shall also apply to outsourced IT systems and shall be documented in bilateral agreements or contracts with the Commission.

5.3. IT Vulnerability and Remediation Management

The IT security *standard on IT Vulnerability and Remediation Management [24]* is based on Commission Decision (EU, Euratom) 2017/46 on the security of communication and information

systems in the European Commission and Commission Decision laying down implementing rules for Articles 3, 5, 7-15 of Decision 2017/46, C (2017) 8841, in particular its Article 12.

IT vulnerability and remediation management is a security practice designed to identify and remediate vulnerabilities in a timely way. The objectives are to prevent proactively the exploitation of IT vulnerabilities that exist within IT systems and to validate the proper execution of the regular patching process.

The IT vulnerability and remediation management process is divided into two phases, namely identification and response, where at each step, appropriate communication is released to relevant stakeholders:

a) Identification phase: monitor security sources for vulnerability announcements, remediation measures, and emerging IT security threats; perform IT vulnerability assessments; and analyse possible remediation.

b) Response phase: prioritizing, testing, implementing and monitoring of IT vulnerability remediation measures; exception handling.

System Managers, System Suppliers and IT Service Providers, with delegated responsibilities from the System Owner, shall ensure that patches are applied in accordance with the relevant change control procedures and shall perform, where feasible, authenticity, integrity and anti-virus testing for the downloaded patches.

The provisions in this IT Security Standard apply to all IT systems in the Commission. The principles of IT Vulnerability and Remediation Management shall also apply to outsourced IT systems and shall be documented in bilateral agreements or contracts with the Commission.

5.4. Incident Management

Whether accidentally or deliberately, events that could have a negative impact on information security occur frequently. From virus infections to equipment failures, human errors or hacking attempts, many different events can potentially breach the confidentiality, integrity or availability of EC information.

The IT *security standard on incident management [11]* provides instructions for the essential elements that must be in place for the reporting of and response to events that may impact information confidentiality, integrity or availability. This is a broad definition since most ICT-related incidents have the potential to impact one of these three aspects of information security. Consequently, the standard also provides rules for determining the security relevance of such events so that they may be reported and escalated when appropriate, according to the risks involved.

Specific instructions are provided for the following domains:

- Reporting security events and weaknesses
- Management of security incidents and improvements

- Collection of evidence

This standard applies to all information systems, software, databases, networks and other Commission assets involved in handling or protecting EC information, including but not limited to the following: servers, workstations, portable PCs, other portable computing devices (PDAs etc.), storage devices and network equipment. The measures mandated by this standard must be followed by all relevant personnel, including all Commission officials, contractors and third parties that handle EC information or computing assets.

6. SECURE OPERATIONS

The Commission's information needs are served by a wide variety of computerised information systems. Many of these systems are very sensitive and/or instrumental in supporting critical administrative functions of the Commission, and so they must be carefully managed to ensure that they operate correctly and securely.

6.1. Operational Management

Computer operations must be well managed and documented to minimise the risk of errors or security incidents. The *standard on operational management [12]* contains some of the basic rules for the operation of Commission computer systems; additional rules are documented in other related standards as presented in this document.

This standard provides instructions to ensure the correct and secure operation of information processing facilities. In particular, this document focuses on the everyday procedures for operating and applying changes to IT systems, and the segregation of responsibilities and facilities to minimise security risks.

More specifically the following domains are addressed:

- Documented operating procedures
- Change management
- Segregation of duties
- Third-party service delivery management
- System planning and acceptane

The defined security requirements apply to all IT systems that are operated by or on behalf of the European Commission, and to all facilities housing these systems. The measures mandated by this standard must be followed by all relevant personnel, including all Commission officials, contractors and third parties who are responsible for operating Commission IT systems.

6.2. Back-ups

The *standard on back-ups [13]* provides the appropriate controls to follow to back up all types of electronically stored data on IT systems, including servers and network equipment.

The goal of this standard is not to force all data to be backed up but to ensure that system/data owners identify the data that require backing up and implement backup procedures accordingly. The frequency and type of backups should be based on an analysis of the availability and integrity requirements of the data (e.g. during the analysis phase of the business continuity planning process). Based on this analysis, the system owner should decide which of the backup plans offered in the

service catalogue of the IT service provider is suitable for their IT systems. To maintain the integrity and availability of data and data processing facilities, backups of data and software shall be made in accordance with established procedures. They shall be regularly tested, including the timely restoration of data.

This document sets out the minimum requirements that apply to all applications and IT systems hosted on European Commission premises. Some are mandatory and subject to compliance verification. Some are in the form of recommendations (i.e. guidance) based on industry best practices, and not subject to compliance verification. These may become mandatory in future versions of this standard, in the light of customer feedback, further best practices identified and compliance analysis.

The archiving of data falls outside the scope of this standard. Workstations and mobile devices are also outside its scope.

6.3. Logging and Monitoring

Preventive controls can go a long way in assuring the security of information and systems, but they cannot guarantee absolute security. Systems must also be supervised to check whether information security breaches have taken place so that corrective measures can be taken. This supervision is performed through logging and monitoring.

Information systems used by the Commission must record at least the basic information security-related events in logs so that they can be monitored in (near) real-time and/or reviewed after an incident has occurred. In many commercial sectors there are legal and regulatory requirements to perform information security logging and to retain the logs for specific periods.

The *standard on logging and monitoring [14]* provides mandatory instructions for the procedures to be used for logging and monitoring on all types of computer systems that are capable of generating information security-related log events, including servers, network equipment, workstations and mobile devices. Its aim is to ensure that a sound minimum of logging and monitoring is performed consistently across the Commission, without incurring unreasonable costs or administrative burdens.

This standard applies to all computer systems, including but not limited to the following: servers, workstations, portable PCs, other portable computing devices (PDAs etc.), storage devices and network equipment. The measures mandated by this standard must be followed by all relevant personnel, including all Commission personnel and contractors.

6.4. Physical and Environmental Security

In order to protect the confidentiality, integrity and availability of computer systems and the information held therein, controls must be applied to assure their physical protection. These controls are intended to prevent physical damage and unauthorised physical access, whether accidental or deliberate.

Accidental damage may be caused by any number of factors, ranging from environmental conditions (such as bad weather, earthquakes etc) to simple accidents such as a person tripping over a cable and accidentally disconnecting it. Deliberate threats are normally either aimed at theft, causing physical damage (sabotage), or gaining logical access to computer systems for other purposes (such as espionage), which is greatly facilitated when physical access is possible. The controls described in this standard are intended to cover all aspects of physical security.

The *standard on physical and environmental security [15]* provides detailed instructions for the physical and environmental protection of all types of computer systems, including servers, network equipment, cabling and end user devices. It applies to all premises that are occupied by the European Commission and/or that contain EC information systems. It also applies to physical computing assets that are used for EC systems, including systems that are owned, housed or operated by third parties on behalf of the Commission.

The scope includes but is not limited to the following: servers, workstations, portable PCs, other portable computing devices (PDAs etc), storage devices, network equipment and cabling. The measures mandated by this standard must be followed by all relevant personnel, including all Commission officials, contractors and third parties having access to these assets.

6.5. Compliance

The provisions of this IT security standard cover the IT security compliance of Commission IT systems and related processes with the European Commission IT security policies and standards and the specific IT security provisions or requirements included in relevant legislation and contracts [16].

Specifically, the provisions of this IT security standard cover the following three types of IT security compliance verification:

a. review of IT security,

b. IT security compliance review,

c. IT security technical compliance review.

Provisions on IT security audits and IT security inspections fall outside the scope of this standard.

IT security compliance metrics provide insight into the effective implementation of IT security measures and correct execution of IT security processes, including IT risk management, IT asset management and IT vulnerability and remediation management.

A ‘three lines of defence’ operational model provides for three layers of IT security assurance activities involving different groups of actors:

a. The first line of defence encompasses IT security risk management. The actors involved are system owners, system managers and heads of department, who are responsible and accountable for operational management.

b. The second line of defence encompasses of IT security compliance reviews. The actors involved are the Directorate-General for Informatics (DIGIT) and the Human Resources Directorate of Security (HRDS), who monitor and facilitate the implementation of effective IT security compliance management practices and assist in reporting compliance-related information across all levels of the organisation.

c. The third line of defence encompasses internal IT security audits. The actors involved are entities with official capacity to carry such audits; they provide independent assurance.

In complement to the above-mentioned model, external IT security audit capabilities are the only ones authorised to perform external IT security audits.

7. APPLICATION LEVEL SECURITY

In addition to the security requirements that are specified in this chapter, the contractor is also encouraged to reference and take into consideration DIGIT's documents on ***"Web application secure development guidelines" [3]*** and ***"Web Application Security Standard" (****see section 3.2****)***. In these documents, technical issues regarding application level security are identified and addressed by presenting the main types of vulnerabilities and suggesting related countermeasures.

7.1. Access Control and Authentication

The security *standard on access control and authentication [17]* is mandatory and an integral part of the Commission's information security policy. Exceptions must be handled in accordance with Article 8.3.d.iv of Commission Decision (EU, Euratom) 2017/8841.

It establishes:

- minimal requirements for access control and authentication on IT systems;
- requirements for setting and issuing authenticators;
- requirements applying to user access management processes; and
- roles and responsibilities in the management of access control.

This standard sets out minimum requirements applying to all applications and IT systems hosted on Commission premises. Some are mandatory and subject to compliance verification. Some are in the form of recommendations (i.e. guidance) based on market best practices, and not subject to compliance verification. These may become mandatory in future versions of this standard, in the light of customer feedback, further best practice and compliance analysis.

7.2. Passwords

This *technical standard* sets out requirements for the management of *passwords [18].* The aim is to strike a balance between user experience and the security of the Commission's information. Every setting contributes to that balance: failure to comply with one of the requirements would destabilise it and significantly increase the level of risk to which an account is exposed.

This standard provides for two parallel modi operandi that can be selected by the system owner:

- traditional password use and handling, allowing for systems to continue their existing password implementation and setup without any impact; and
- user-centric password use and handling, bringing forward a new approach in line with new best practices, standards and technology evolutions.

It specifies a set of rules designed to enhance the security of the Commission's information systems by enhancing the user-friendly approach to authentication.

The defined minimum requirements apply to all applications and IT systems hosted on Commission premises. Some are mandatory and subject to compliance verification. Some are in the form of recommendations (i.e. guidance) based on market best practices, and not subject to compliance verification. These may become mandatory in future versions of this standard, in the light of customer feedback, further best practice and compliance analysis.

This standard is mandatory and an integral part of the Commission's information security policy. Exceptions must be handled in accordance with Article 8.3.d.iv of Commission Decision (EU, Euratom) 2017/8841 (Implementing Rules for Commission Decision (EU, Euratom) 2017/46).

7.3. Transport Layer Security

This *technical standard* sets out the technical parameters relating to the use of the *transport layer security (TLS) security protocols [19] t*hat are authorised for implementation on Commission systems and infrastructures, including (but not only) web servers, proxies, reverse proxies and specialised cryptographic hardware.

The fact that the technical parameters or algorithms specified here are authorised for use does not necessarily imply that all of them are exhaustively supported by DIGIT infrastructure and services. Particular vendor and technical solution implementations and evolution at DIGIT mean that it is quite possible that only a specific subset is supported. System owners requiring integration of their information systems with DIGIT components while using the TLS protocols are strongly advised to consult the DIGIT service catalogue for the particular parameters and algorithms supported at DIGIT before making design and/or product acquisition decisions.

In the scope of this standard, the data to be protected by TLS protocols are restricted to unclassified data and do not include EU classified information (EUCI) data. Consequently, this document applies to data of 'publicly available', 'Commission use' and 'sensitive non-classified' confidentiality levels (see section 2).

The security standard does not cover cryptographic key management issues. TLS implementations are expected to comply with the key management section of the standard on cryptography and public key infrastructure.The recommendations apply only to the protection of data in motion in TLS-based secure channels; they may be unsuitable for other purposes, including (but not only) long-term data confidentiality or integrity protection and digital signatures.

This technical standard is mandatory and an integral part of the Commission's information security policy. Exceptions must be handled in accordance with Article 8.3.d.iv of Commission Decision (EU, Euratom) 2017/8841 (Implementing Rules for Commission Decision (EU, Euratom) 2017/462).

7.4. Crypotography and PKI

Cryptography is the practice and study of transforming information to make it inaccessible or illegible to unauthorised parties. Within an ICT environment, this is performed through encryption and

subsequent decryption of information, using a variety of methods. Encryption is used for a number of different purposes, including protecting the confidentiality of information and guaranteeing the integrity and authenticity of data.

The objective of the *standard on cryptography and PKI [20]* is to ensure that encryption is used when appropriate, and that appropriate controls are put in place to ensure that the encryption is effective and does not create new risks.

This standard applies to all current or proposed EC systems that use cryptography, including but not limited to the following: servers, workstations, portable PCs, other portable computing devices (PDAs, smartphones etc.), storage devices, network equipment and media storage (floppy disks, USB devices etc.). The measures mandated by this standard must be followed by all relevant personnel, including all Commission officials, contractors and third parties in possession of such information.

This standard is applicable to all systems that use cryptography , handling both EUCI and non-EUCI, although systems handling EUCI must comply with additional rules . Chapter 8 of this document must be followed in all cases when deciding whether cryptography should be used. If cryptography is used, then the rest of the standard must be followed. The standard is also applicable to systems and information operated by third parties on behalf of the Commission.

8. OTHER OBLIGATIONS

8.1. Adherence to the EC IT Security framework

- All contractor's staff working at/for the Publications Office are required to comply with the EC IT Security framework and its implementing rules, guidelines, notices and standards.

8.2. Protection of Personal Data

- The legislation that governs the processing of personal data in the European Institutions and bodies is Regulation (EU) 2018/1725[6]. The Regulation applies, as a main rule, to all processing (wholly or partly by automated means) of personal data by all EU Institutions or bodies, including the processing by a contractor on behalf of an EU Institution or body.
- The Data Controller needs to keep in mind the obligation to ensure data protection by design and by default which means that before designing the processing operation and during its lifespan the Controller must 'think privacy'. Appropriate technical and organisational measures must be taken to ensure that data protection is essential to the processing operation and that personal data is processed only to the extent necessary for each specific purpose of the processing. Privacy by design means to implement data protection principles both at the time of the determination of the means for processing and at the time of the processing itself. Privacy by default means to apply the strictest privacy settings automatically.
- Processing of personal data may involve use of an external contractor ('processor') to help with the processing on behalf of the controller. This does not shift the controller's responsibility to the contractor. The data protection rules impose clear and mandatory requirements on the minimum guarantees such contractor shall be able to provide and, on the minimum topics to be addressed in the agreement between the controller and the processor. The Contractor shall be able to provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
- Whenever personal data are being processed, the following principles and conditions should be satisfied:
  - Transparency: Process data in a transparent manner in relation to the data subject.
  - Purpose limitation: Process only personal data for specified, explicit and legitimate purposes.

[6] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

- Data minimization: Data must be adequate, relevant and limited to what is necessary for the purposes for which they are processed.
- Accuracy: Data must be accurate and kept up to date.
- Storage limitation: Keep for no longer than necessary.
- Integrity and confidentiality: Processed in a secure manner, which means the controller puts in place technical and organisational measures to prevent any unauthorised act.
- Accountability: the controller is responsible for compliance and shall be able to demonstrate it.
- Lawfulness and fairness: The controller needs a legal ground for the processing. Lawful processing means that the processing is necessary:
    (a) for the performance of a task carried out in the public interest;
    (b) for compliance with a legal obligation to which the Controller is subject;
    (c) for the performance of a contract to which the data subject is party or to take steps at the request of the data subject before entering into a contract;
    (d) to protect the vital interests of the data subjects.

8.3. Non-Disclosure Agreement

- The contractor should sign a non-disclosure agreement declaring that she/he will treat as confidential and will not disclose to a third party or use for her/his own benefit or that of a third party any information disclosed to her/him in writing or orally or to which she/he has access in direct or indirect relation to the fulfilment of obligations under the contract, without the prior written approval of the Publications Office.

8.4. Third party access to Communication and Information Systems

- Third parties may not access the internal processing systems unless a formal contractual agreement is signed.
- Remote access to the Publications Office information systems:
    - by third party users (e.g. printers) or Services Providers (e.g. remote system managers) must be done by Virtual Private Network (VPN). Any exception should be checked and is subject to prior authorization from the System Owner.
    - Should the Service Provider need remote access to any communication and information system of Commission or data sets processed therein, they will be requested to comply with security rules referred to in Article 6(5) of the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017. This entails prior authorisation which shall be granted on the basis of a formal request for network access service "Remote Access for Companies" and approval process which takes in average 4-6 weeks. The outcome of the approval,

i.e. the security convention, shall be valid for a specified duration linked to the contract and shall be obtained before the connection is activated. The formal request is initiated by the concerned DG or service of the Commission and based on the risk assessment with the focus on nature and sensitivity of the tasks to be performed remotely and the security needs of each accessed communication and information system.

- During the authorisation process the Service Provider is asked to describe relevant organisational, physical, logical and network security measures in order to provide reasonable assurance that the risks are adequately and systematically covered at a level equivalent to the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017, its implementing rules and corresponding security standards. The authorisation process may lead to the refusal or impose additional security requirements as a prerequisite for approval, in order to protect the Commission's communication and information system and networks from the risks of unauthorised access or other security breaches.

8.5. Inspection & monitoring right

- The Publications Office reserves the right to request a security inspection of the contractor for compliance to the EC IT Security framework. Such inspection should be announced in advance with a reasonable notice.
- The Publications Office has the right to monitor and examine any information stored on its information processing systems or communicated over its network or equipment.
- The Publications Office will access this information without the contractor's consent or advance notice only:
  - for capacity planning purpose,
  - for back-up and archiving purpose,
  - if there is sufficient cause or evidence indicating abuse, non respect of the IT Security framework or the suspicion of a fraud or crime. In such case, the explicit authorization of the Publications Office Local Security Officer (LSO) will be required before conducting any investigation.

8.6. Obligation of reporting

- The contractor has the obligation to report all security incidents, software malfunctions, security weaknesses or threats to systems or services that their staff notice or is made aware of to the Publications Office help desk or the Publications Office Local Informatics System Officer (LISO).
- All users are instructed that they must not, unless formally authorized by the Publications Office Local Informatics System Officer, attempt to prove a suspected weakness because this will be interpreted as a potential misuse of the system, could also cause damage to the

information system or service and result in legal liability for the individual performing the testing.

8.7. Business Continuity Management

The Publications Office has developed a comprehensive Business Continuity Management framework:

- The target system must be integrated into the Publications Office BCM framework.
- A copy of the accepted production server content must be safe stored in a location distinct from the production site.

8.8. Change Management

The production systems are subject to strict change control management.

- All patches and service packs must be tested and validated before implemented into production.
- Automated updates must not be used as some updates may cause applications to fail.
- The decision to install changes in production is taken by the System Owner. Installation is typically performed after business hours; otherwise the service interruption procedure must be used in agreement with the infrastructure production manager.

8.9. Other miscellaneous obligations

- see the articles of the contract: processing of personnal data, confidentiality, intellectual property rights, legal software copies.

9. REFERENCES

[1] Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.
Available at:
https://op.europa.eu/en/publication-detail/-/publication/f9fd8acf-d7c9-11e6-ad7c-01aa75ed71a1/language-en

[2] Commission Decision C(2017) 8841 final of 13.12.2017 laying down implementing rules for Articles 3, 5, 7, 8, 9, 10, 11, 12, 14, 15 of Decision 2017/46 on the security of communication and information systems in the Commission.
Available at:
https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-8841-F1-EN-MAIN-PART-1.PDF

[3] DIGIT IT Security Standards and Guidelines.
Available at:
https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Pages/IT-security-standards-and-guidelines.aspx

[4] Security Notice Marking and handling of sensitive non-classified information.
Available at:
https://myintracomm.ec.europa.eu/corp/security/EN/newDS3/PolicyLegislation/Documents/C%282019%29%201904%20-%201_EN_ACT_part1_v4.pdf

[5] S²LC – IT Security in System Life-Cycle Global approach to Security Processes.
Available at:
https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/GD_secure_system_lifecycle.pdf

[6] European Commission Information System Security Policy C(2006) 3602, Standard On Secure Systems Development.
Available at:
https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/ST_secure_development.doc

[7] C(2018) 7283 final, Web Application Security Standard.
Available at:
https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/IT%20Security%20Standard%20-%20Web%20Application%20Security%20Standard.pdf

[8] Web application secure development guidelines.
Available at:
https://webgate.ec.europa.eu/fpfis/wikis/display/SecurityAssurance/EC+DIGIT+SECURITY+ASSURANCE+Documents?preview=/200428571/200428590/Web%20Applications%20Secure%20Development%20Guidelines.pdf

[9] Open Source Security Testing Methodology Manual, OSSTMM.
Available at:
http://www.isecom.org/research/osstmm.html

[10] Open Web Application Security Project, OWASP:
Available at:
https://www.owasp.org/index.php/Main_Page.

[11] European Commission Information System Security Policy C(2006) 3602, Standard On Information Systems Security Incident Management.
Available at:
https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/ST_incident_mgt.doc

[12] European Commission Information System Security Policy C(2006) 3602, Standard On Operational Management.
Available at:
https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/ST_operational_mgt.doc

[13] C(2019) 8016 final, IT security standard Backup.
Available at:
https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/ST_backup.doc

[14] European Commission Information System Security Policy C(2006) 3602, Standard On Logging And Monitoring.
Available at:
https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/ST_logging_monitoring.doc

[15] European Commission Information System Security Policy C(2006) 3602, Standard On Physical and Environmental Security.
Available at:
https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/ST_physical_security.doc

[16] C(2019) 8017 final, IT security standard IT security compliance management.
Available at:
https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/ST_compliance.pdf

[17] C(2019) 2344 final, IT security standard Access control and authentication.
Available at:
https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/ST_access_control_authentication.pdf

[18] C(2019) 2345 final, IT technical standard Password.
Available at:
https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/ST_password_technical_standard.pdf

[19] C(2019) 2346 final IT technical standard Transport Layer Security (TLS).
Available at:

https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/ST_transport_layer_security_technical_standard.pdf

[20] European Commission Information System Security Policy C(2006) 3602 Standard On Cryptography And Public Key Infrastructure.
Available at:
https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/ST_crypto.doc

[21] IT Security Risk Management Methodology ITSRM^2.
Available at:
https://webgate.ec.europa.eu/fpfis/wikis/pages/viewpage.action?pageId=222010104

[22] Security Plan Template Guideline.
Available at: https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/ITSRM2%20-%20Security%20Plan%20Template%20Guidelines.docx

[23] C(2018) 7285 final, IT Security Standard IT Asset Management.
Available at:
https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/IT%20Security%20Standard%20-%20IT%20Asset%20Management.pdf

[24] C(2018) 7284 final, IT Security Standard, IT Vulnerability and Remediation Management.
Available at:
https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/IT%20Security%20Standard%20-%20IT%20Vulnerability%20and%20Remediation%20Management.pdf

[25] IT Security Risk Management Methodolody (ITSRM^2) Wiki.
Avaialble at:
https://webgate.ec.europa.eu/fpfis/wikis/display/ITSRM2/IT+Security+Risk+Management

[26] European Commission Information System Security Policy C(2006) 3602, Standard On Information Security Risk Management.
Available at:
https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/ST_risk_management.doc

[27] OP IT Security Guideline "Security-by-Design".
Available at:
http://units.publications.europa.eu/u51/Public/OP.01%20Working%20Instructions%20and%20Guidelines/S%C3%A9curit%C3%A9-LISO%20-%20WI%20-%20Guidelines/OP%20IT%20Security/OP%20ITSEC%20Guidelines/OP%20Guideline%20-%20Security%20by%20Design%20approach%20v1-2.pdf?Web=1

[28] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.
Available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN

End of document