EUROPEAN
COMMISSION

Brussels, 26.10.2018
C(2018) 7285 final

IT Security Standard

IT Asset Management

Contents

1. INTRODUCTION 2
   1.1. Legal Base 2
   1.2. Subject matter and scope 2
   1.3. Definitions 2
2. PROCESS, ORGANISATION AND RESPONSIBILITIES 2
   2.1. IT Asset Management 2
   2.2. Commission IT asset inventory 3
   2.3. Roles and Responsibilities 4
3. MISCELLANEOUS AND FINAL PROVISIONS 4
   3.1. Transparency 4
   3.2. Technical Standards 5
   3.3. Entry into force 5

1. INTRODUCTION

1.1. Legal Base

This IT security standard 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 repeals the IT Security Standard on Asset Management related to Commission Decision C(2006) 3602.

1.2. Subject matter and scope

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

2. The provisions in this IT Security Standard apply to all IT systems in the Commission. The relevant responsibilities and IT security measures for IT systems handling EU classified information shall be in line with Decision (EU, Euratom) 2015/444.

3. The provisions in this IT Security Standard cover the aspects of IT Asset Management necessary to support other IT Security processes and limited to IT assets.

4. 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.

1.3. Definitions

For the purposes of this IT Security Standard, in addition to the definitions in Article 2 of Commission Decision (EU, Euratom) 2017/46 and in Article 2 of Commission Decision (EU, Euratom) 2017/8841 the following definitions also apply:

1) 'IT Asset Attribute' means a (detailed) characteristic of IT asset.
2) 'Commission IT asset inventory' means the inventory of all IT assets within the Commission.
3) 'IT asset inventory' means a comprehensive identification of all IT assets in an organisation.
4) 'IT Asset Management' means the systematic process to guide the planning, acquisition, operation and maintenance, renewal and disposal of assets.
5) 'Priority Level' means a label for IT systems and their IT assets used in IT security processes, in particular IT Vulnerability and Remediation Management.

2. PROCESS, ORGANISATION AND RESPONSIBILITIES

2.1. IT Asset Management

1. 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.

2.2. Commission IT asset inventory

1. Only information on IT assets shall be collected as required to support IT security management processes, in particular IT vulnerability and remediation management.

2. IT assets shall be assigned one of the following priority labels; very high, high, major, medium or low; and labelling shall be based on the asset valuation defined by the System Owner as part of the IT Risk Management methodology.

3. The Commission IT asset inventory shall enable the registration, collection and consolidation of information for all IT assets under the responsibility of Commission Departments and shall assist System Owners in performing their responsibilities for IT asset management.

4. Before an IT system shall be accepted in production, an inventory of all its IT assets shall be registered in the Commission IT asset inventory.

5. Automated inventory management tools and interfaces shall be used whenever possible to keep the Commission IT asset inventory up to date.

6. The Commission IT asset inventory shall be reviewed manually for IT Assets not captured in the existing inventories.

7. The Commission IT asset inventory shall record as a minimum:

    a) A unique identification of the IT asset;

    b) a brief description of the IT asset;

    c) IT system name the IT asset is part of;

    d) the owner of the IT asset (and optionally responsible SSO);

    e) the value for the Commission in the form of priority level of the IT system where the IT asset is part of:

        i. 1 (Low)
        ii. 2 (Medium)
        iii. 3 (Major)
        iv. 4 (High)
        v. 5 (Very high)

    f) Its logical and physical location;

    g) hardware and software attributes, where relevant for the type of IT asset;

        i. Operating system and version number
        ii. Software packages and version numbers
        iii. Network services
        iv. Internet Protocol (IP) address (if it is static)
        v. A fully qualified domain name (FQDN)
        vi. Hardware configuration
        vii. Central processing unit
        viii. Memory
        ix. Ethernet addresses (i.e., network cards)
        x. Wireless capability
        xi. Secure identity (e.g. device certificates)

8. The Commission IT asset inventory shall provide the flexibility to register additional information about IT assets, in particular details of a Local Information System Officer and/or System Manager and/or System Security Officer to contact during IT security incident handling.

2.3. Roles and Responsibilities

1. The main IT Asset Management responsibilities are:

a) Heads of Commission Departments are accountable for IT asset management in their Department for the IT assets owned by their department.

b) Head of Commission Departments are accountable for asset return when a person employed by the Commission, either as Commission staff, contractor or third-party user, is terminating his/her relationship with the Commission, his/her immediate manager/responsible shall provide for all Commission's IT assets in his/her custody before (s)he leaves the Commission.

c) The System Owner or System Managers, with delegated responsibilities :

i. Are responsible for IT asset management of their IT systems, in particular performing the IT asset identification, inventorying and making the information available to the Commission IT asset inventory as well as managing the lifecycle of their IT assets.

ii. Are responsible for the retirement or disposal of their IT assets, in compliance with Commission IT security sanitization and/or removable media standards.

iii. Shall keep the Commission IT asset inventory up to date for their IT assets.

iv. Shall document acceptable use of the IT assets and disseminate the information to the end-users;

v. Shall make a formal reporting statement to DG DIGIT in Q3 of every calendar year to confirm that their IT asset inventories have been reviewed and their IT assets are accurately registered in the Commission IT asset inventory.

vi. Shall take corrective actions in updating the Commission IT asset inventory.

d) DG DIGIT shall:

i. Perform, where feasible, random verifications of the accuracy of the Commission IT asset inventory and shall analyse inaccuracies;

ii. Escalate recurring non-compliance with the IT Asset Management Security Standard to the ISSB.

iii. Set up and maintain the Commission IT asset inventory infrastructure that will facilitate the collection and consolidation from other IT asset inventories, and will enable System Owners to perform their responsibilities in IT asset management in support of IT security management processes.

iv. Perform automated IT asset inventory discovery for all IT asset connected to the Commission’s public and private network(s) managed by DG DIGIT. Active and passive tools may be used to achieve this goal, always considering all requirements to not affect the regular operations of the IT systems.

e) End-Users shall return Commission IT assets in their custody before they leave the Commission

3. MISCELLANEOUS AND FINAL PROVISIONS

3.1. Transparency

This IT Security Standard shall be brought to the attention of Commission staff and to all individuals to whom it applies.

3.2. Technical Standards

1. The provisions of this IT Security Standard shall, where necessary, be further detailed in technical standards and/or guidelines to be adopted in line with Commission Decision (EU, Euratom) 2017/46 and its implementing rules C(2017) 8841. These technical standards and guidelines shall be based on industry best practices and are selected to suit the Commission's IT environment.

2. The Standard on Asset Management and related guidelines adopted under Decision C (2006) 3602 of 16 August 2006 are repealed

3.3. Entry into force

This standard shall enter into force on the day following the date of adoption of this standard.

Appendix 1: Roles & Responsibilities (RASCI)

Role: / Activity:	Head of Commission Department	System Owner	System Manager	System Security Officer	System Supplier or IT Service Provider	DIGIT	User	ISSB
Inventory of IT assets	A	R	R(D)[1]	S	S	C/S[2]		I
Ownership of IT assets	A	R/I	R(D)[1]	I		I		
Acceptable use of IT assets	A	R	R(D)[1]	S	I	I	I	
Return of IT assets	A	R	R(D)[1]		S	S[2]	R[3]/I	
Labelling of IT assets	A	R	R(D)[1]	S	S	S[2]/C		
Handling of IT assets	A	R	R(D)[1]	S	S	S[2]		
Reviewing of IT assets	A	R	R(D)[1]	S	S	S[2]		

'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.

[1] Delegated Responsibility from the System Owner
[2] As part of the DIGIT Commission IT asset management activities supporting the System Owner
[3] Responsibility from the User in case an IT asset is in custody of the User.