EUROPEAN
COMMISSION

Brussels, 4.11.2019
C(2019) 8018 final

IT security standard

Removable media

CONTENTS

1. INTRODUCTION

In accordance with Commission Decision (EU, Euratom) 2017/461 and Commission Decision laying down the 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, C(2017)8841, and in particular Article 12, the standard on management of removable media relating to Commission Decision C(2006) 3602 should be repealed.

Removable media such as USB flash drives are commonly used to store or transfer data between different systems. In recent years, the capacity of such devices has increased making it possible to store large amounts of information on them.

Removable media may be standalone information storage devices that can be plugged directly into a PC, or they may be used as internal memory on mobile devices such as mobile phones or tablets. In the latter case, the mobile device is usually connected to a PC and the removable medium is accessed in the same way as a standalone medium would be.

The use of removable media must take into consideration some major threats such as:

- The introduction of malware onto Commission workstations, particularly if these media are also used on non-Commission workstations (e.g. users' home PCs) or if their origin is untrusted.
- Loss of confidentiality of Commission data if the medium is lost or stolen.
- Retrieval of recycled or discarded media. When media is used to store non-public information, the information shall be removed, deleted or destroyed in the correct way. If this is not the case, the information could be stolen or old versions of information may be used by accident.
- Destruction of equipment or media, when malicious USB devices are connected to them.
- Violation of software licencing agreement and intellectual property rights (IPR).

The rules applicable under this standard intend to mitigate these threats.

2. PURPOSE

This standard provides instructions for the secure handling of removable media. The instructions are intended to ensure that the information stored on such media and the Commission environment is protected against any threats posed by their use.

3. SCOPE

This standard applies to all removable media used in the Commission. The measures mandated by this standard must be followed by all relevant personnel, including all Commission officials, contractors and third parties who use removable media to store Commission information and/or connect to Commission workstations and networks.

This standard does not apply directly to mobile devices such as mobile phones and tablets, although it does apply to removable media that may be used in these devices.

4. EXCEPTIONS

This security 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 the Commission decision 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, C(2017)8841.

5. DEFINITIONS

For the purposes of this standard, in addition to the definitions provided in Article 2 of Decision (EU, Euratom) 2017/46 and the definitions in Article 2 of its implementing rules 2017/8841 the following definitions also apply:

TERM	DEFINITION
CART kiosk	Is a free-standing system developed and run by the DG HR Security Directorate. It allows users to safely check their USB sticks for malicious content, and is capable of identifying more than a normal anti-virus scan. The CART Kiosk can also check your CD, DVD and SD card. Use the following link to locate your nearest CART kiosk: https://myintracomm.ec.europa.eu/corp/security/FR/CyberDefence/CART/Pages/CART-kiosk.aspx.
removable media	Refers to storage media which is designed to be removed from the computer. Examples include: • optical or magnetic discs (DVDs, CDs, Blu-ray, floppy disks), • USB flash drives, • external hard disk drives, • memory cards (CompactFlash card, secure digital card, memory stick), • tapes (e.g. back-up tapes), • any other connected removable device which appears as storage.
sanitisation of media	Refers to techniques and methods such as disposal, clearing, purging, destruction, overwriting and degaussing. More details on each method are given as part of the standard on sanitisation of media.

6. SECURE HANDLING OF REMOVABLE MEDIA

Removable media containing information must be protected against unauthorised access, misuse or corruption.

6.1. General rules

(M=mandatory, R=recommended)

S/N	Requirement	Implementation
1.	Removable media **should** be used as little as possible and only in situations where it is not technically possible (feasible) to use other means of exchanging information or transporting information.	R
2.	Information **shall** only be held on removable media for as long as it is required.	M

S/N	Requirement	Implementation
3.	Users **shall** use different removable media for storing Commission and private information.	M
4.	Commission information marked as sensitive non-classified information **shall** only be copied to encrypted removable media.	M
5.	Removable media **shall not** be the sole or primary repository of Commission documents; consequently, there is no specific requirement to back them up.	M
6.	AutoRun, AutoPlay (and similar functions) **shall** be disabled on all workstations and servers to prevent unauthorised applications or malware from running automatically from removable media.	M
7.	If an application attempts to run automatically from removable media, the user **shall** cancel it and take steps to ensure that it does not run again.	M
8.	Any removable non-encrypted media provided by the Commission **shall** be reformatted when delivered.[1]	M
9.	Removable media **shall** only be taken off Commission premises when necessary, and care must be taken to avoid their loss, theft, damage, abuse or misuse.	M
10.	Users **shall** not connect media from unknown or suspicious sources to Commission computers (e.g. media that are found unattended or received from unknown people) before they have been analysed by Commission's authorised tools (e.g. a CART kiosk).	M
11.	Users **shall** format or analyse media used on external or personal computers/devices (including mobile phones and tablets) before using them to Commission computers; they must do so using Commission authorised tools (e.g. a CART kiosk, Commission approved software).	M
12.	Removable media **shall** be sanitised before disposal as described in the standard on sanitisation of media.	M

6.2. Reporting incidents relating to removable media

(M=mandatory, R=recommended)

S/N	Requirement	Implementation
13.	All users of removable media **shall** report lost or stolen removable media containing information classified as 'sensitive non-classified information' to the EC Helpdesk or to the corresponding security incident contact point. They must include a damage assessment specifying the information held and the potential consequences of its loss or disclosure.	M

[1] For more details refer to the standard on sanitisation of media.

S/N	Requirement	Implementation
14.	Any suspicious file or malware detected on removable media **shall** also be reported to the EC Helpdesk.	M

7. ROLES AND RESPONSIBILITIES

(M=mandatory, R=recommended)

S/N	Requirement	Implementation
15.	LISO **shall** provide support for applying appropriate security measures to removable media and advise end users on training requirements.	M
16.	DIGIT **shall** use removable media in conformance with the rules of this standard.	M

8. ENTRY INTO FORCE

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