EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY
Directorate DS - Security
Informatics Security

Brussels, 04/07/2011
HR.DS5/GV/ac ARES (2011) 719444
SEC20.10.05/04 - Standards

European Commission

Information System Security Policy

C(2006) 3602

STANDARD ON MANAGEMENT OF REMOVABLE MEDIA

ADOPTED BY MRS. IRENE SOUKA,

DIRECTOR-GENERAL OF DG HUMAN RESOURCES AND SECURITY, ON 04/07/2011

Version 0.4_06/05/2011

TABLE OF CONTENTS

1. ADOPTION PROCEDURE

This Security Standard is adopted in accordance with Article 10(3) of Commission Decision C(2006) 3602 concerning the security of information systems used by the European Commission, adopted on 16 August 2006.

It is drawn up under the responsibility of the Security Directorate pursuant to Article 9(1)(b) and takes into account the items listed in Article 10(2) of Commission Decision C(2006)3602, in particular internationally recognised norms and standards applicable in the field of information systems security.

Under Article 10(3) of Commission Decision C(2006) 3602, the implementing rules may be supplemented by measures of a technical, physical, procedural or organisational nature proposed by the Director of the Security Directorate and adopted by the Director-General of the Directorate-General for Human Resources and Security in consultation with departments that have a legitimate interest. These supplementary measures are called 'security standards' where their application is mandatory, or 'security guidelines' where their application is optional or where they provide guidance on security standards implementation.

2. INTRODUCTION

Removable media such as USB flash drives are commonly used to store or transfer information between different systems. Increases in the capacity of such devices in recent years mean that it is possible to store a large amount of data on a very small device that is very hard to detect. These media are frequently used for legitimate purposes within the EC.

Removable media may be standalone data storage devices that can be plugged directly into a PC, or they may be used as internal memory by mobile devices such as mobile phones, PDAs or digital cameras. In the latter case, the mobile device can also usually be connected to a PC and the removable medium accessed in the same way as a standalone medium.

The use of removable media presents a number of threats, including:

- The introduction of malware onto EC workstations, particularly if media are also used on non-EC workstations (e.g. users' home PCs)
- Loss of confidentiality of EC information if the medium is lost or stolen

The rules in this standard are intended to mitigate these threats.

3. OBJECTIVES

This standard provides instructions for the management of removable computer media, such as USB storage devices or optical discs. The instructions are intended to ensure that the information stored on such media and the Commission environment are protected against any threats posed by their use.

4. SCOPE

This standard applies to all removable computer media used within the European 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 EC information and/or connected to EC workstations and networks.

This standard does not apply to information held on paper, microfiche or other media that are not designed to be used with computers. It also does not apply directly to mobile devices such as mobile phones, PDAs or digital cameras[1], although it does apply to removable media that may be used in these devices.

5. THREATS COVERED

Security controls defined in this information security standard will help to reduce the impact of the following threats (their description is in the *Standard on Information Security Risk Management*).

T05 – Destruction of equipment or media

T20 – Theft of media or documents

T22 – Retrieval of recycled or discarded media

T23 – Disclosure

T33 – Unauthorised use of equipment

T36 – Corruption of data

6. TERMINOLOGY

Removable media refers to storage media which is designed to be removed from the computer without powering the computer off.

Some types of removable media are designed to be read by different types of readers and drives. Examples include:

- Optical discs (DVDs, CDs)
- USB flash drives
- External hard disk drives
- Memory cards (CompactFlash card, Secure Digital card, Memory Stick)
- Floppy disks / Zip disks
- Tapes (e.g. back-up tapes)

[1] These devices are covered in the *Standard on Mobile Computing and Teleworking*.

7. MANAGEMENT OF REMOVABLE MEDIA

Policy objective 5.7.1 – Management of Removable Media – Removable media containing information must be protected against unauthorised access, misuse or corruption, and its readability guaranteed during the whole lifetime of the information.

7.1. General Rules

AutoRun and AutoPlay (or similar functions) must be disabled on all workstations and servers to prevent unauthorised applications or malware from running automatically from removable media. In the event that an application attempts to run automatically from removable media, the user must cancel it and take steps to ensure that it does not run again.

Information that is classified as LIMITED BASIC or higher may not be stored on non-EC removable media (including personal devices of EC staff).

Any removable media provided by the Commission must be blank or reformatted when delivered (i.e. free from any portable applications such as SanDisk U3 or Startkey), with the exception of the management software for encrypted USB flash drives.

When there is a rule mandating encryption for data transmission, that data must also be encrypted when stored on removable media. This is the case, for example, for some types of information defined in Security Notice 1, which must be encrypted using SECEM for transmission. In such cases, where information is stored or transmitted on removable media, the data must be encrypted using approved encryption software[2].

Users must handle removable media with care in order to minimise the risks posed by their use. Removable media must only be taken off Commission premises when necessary, and care must be taken to avoid their loss or theft. Before connecting EC removable media to a non-EC PC, the user must make sure that anti-virus software is installed, active and up to date on the PC.

The use of non-EC removable media is discouraged, since removable media are a common channel for malware infections. Users must not connect media from unknown or suspicious sources to EC computers (e.g. media that are found unattended or received from unknown people). If non-EC removable media are used for EC data, then the same rules must be applied as for EC media.

Information must only be held on removable media for as long as it is required. Care must be taken to avoid holding large quantities of information on a single medium which may then, through the aggregation of

[2] See *Security Notice 1* (particularly section 3.2(3) and Annex 1) and the *Standard on Cryptography and Public Key Infrastructure*.

data, mean that the totality of the data should be classified higher than the individual parts. As a general principle, removable media should be used as little as possible.

Removable media must be sanitised before disposal or reuse as described in the *Standard on Sanitisation of Media*.

Removable media must not be the sole or primary repository of EC documents; consequently, there is no specific requirement to back them up.

Encrypted removable media devices shall have a maximum lifetime of five years from the date of procurement, since advances in computing technology are likely to significantly weaken the effectiveness of the encryption.

7.2. Reporting Incidents relating to Removable Media

All lost or stolen removable media containing information classified as LIMITED HIGH or higher must be reported through the normal security incident handling procedures, including a damage assessment specifying the information held and the potential consequences of its loss or disclosure.

Any suspicious file or detected malware on Removable Media must also be reported as a security incident.

See the *Standard on Information Systems Security Incident Management* for more information.

7.3. User Awareness

Users must be made aware of this policy through appropriate training and reminders to staff.

8. ROLES AND RESPONSIBILITIES

LISO: responsible for advising on appropriate security measures to be applied to removable media; also for advising on training requirements for end users.

DIGIT: responsible for selecting suitable removable media for users in conformance with the rules of this standard.

Users: responsible for handling removable media in a secure way; removing information from media when no longer required; and reporting the loss or theft of removable media.

9. REFERENCES

Note that standards marked (*) are in draft at the time of writing of this standard.

- Commission Decision C(2006) 3602 of 16/8/2006

- Implementing rules for Commission Decision C(2006) 3602 of 16.8.2006.

- Standard on Risk Management (*)

- Standard on Asset Management

- Standard on Cryptography and Public Key Infrastructure

- Standard on Sanitisation of Media (*)

- Standard on Information Systems Security Incident Management (*)

- Security Notice 1: The use and application of security designators and markings, 18/11/2010

10. RELATED DOCUMENTS

- International standard ISO/IEC 27001 – Second edition 2005-06-15

- ENISA – Secure USB Flash Drives, June 2008