13.3. Media Usage

Objective

13.3.1. Media is used with systems in a controlled and accountable manner.

Context

Scope

13.3.2. This section covers information on using media with systems. Further information on using media to transfer data between systems can be found in Section 20.1 - Data Transfers.

PSR references

13.3.3. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV3, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements Physical security (PHYSEC) | Protective Security Requirements

Rationale & Controls

Using media with systems

13.3.4.R.01. **Rationale**

To prevent classified data spills agencies will need to prevent classified media from being connected to, or used with, systems of a lesser classification than the protective marking of the media.

13.3.4.R.02. **Rationale**

Where media is used for backup purposes, the media will be certified for use at the highest level of classification to be backed-up. Refer also to Section 6.4 – Business Continuity and Disaster Recovery.

13.3.4.C.01. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must Not** [CID:4075]

Agencies MUST NOT use media containing classified information with a system that has a classification lower than the classification of the media.

Storage of media

13.3.5.R.01. **Rationale**

The security requirements for storage and physical transfer of classified information and IT equipment are specified in the PSR Policy Framework - Physical Security.

13.3.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4078]

Agencies MUST ensure that storage facilities for media containing classified information meets the minimum physical security storage requirements as specified in the PSR Policy Framework - Physical Security.

Connecting media to systems

13.3.6.R.01. **Rationale**

Some operating systems provide functionality to automatically execute or read certain types of programs that reside on optical media and flash memory media when connected. While this functionality was designed with a legitimate purpose in mind, such as automatically loading a graphical user interface for the system user to browse the contents of the media, or to install software residing on the media, it can also be used for malicious purposes.

13.3.6.R.02. **Rationale**

An attacker can create a file on optical media or a connectable device that the operating system will attempt to automatically execute. When the operating system executes the file, it can have the same effect as when a system user explicitly executes malicious code. The operating system executes the file without asking the system user for permission.

13.3.6.R.03. **Rationale**

Some operating systems will cache information on media to improve performance. As such, inserting media of a higher classification into a system of a lower classification could cause data to be read and saved from the device without user intervention.

13.3.6.R.04. **Rationale**

Using device access control software will prevent unauthorised media from being attached to a system. Using an allow listing approach gives security personnel greater control over what can, and what cannot, be connected to the system.

13.3.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4086]

Agencies MUST disable any automatic execution features within operating systems for connectable devices and media.

13.3.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4089]

Agencies MUST prevent unauthorised media from connecting to a system via the use of:

- device access control software;
- seals;
- physical means; or
- other methods approved by the Accreditation Authority.

13.3.6.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4091]

When writable media is connected to a writable communications port or device, agencies SHOULD implement controls to prevent the unintended writing of data to the media.

IEEE 1394 (FIREWIRE) interface connections

13.3.7.R.01. **Rationale**

Known vulnerabilities have been demonstrated where attackers can connect a FireWire capable device to a locked workstation and modify information in RAM to gain access to encryption keys. Furthermore, as FireWire provides direct access to the system memory, an attacker can read or write directly to memory.

13.3.7.R.02. **Rationale**

The best defence against this vulnerability is to disable access to FireWire ports using either software controls or physically disabling the FireWire ports so that devices cannot be connected. Alternatively select equipment without FireWire capability.

13.3.7.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:4096]

Agencies MUST disable IEEE 1394 interfaces.

13.3.7.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4097]

Agencies SHOULD disable IEEE 1394 interfaces.

Transferring media

13.3.8.R.01. **Rationale**

As media is often transferred through areas not certified to process the level of classified information on the media, additional protection mechanisms need to be implemented.

13.3.8.R.02. **Rationale**

Applying encryption to media may reduce the requirements for storage and physical transfer as outlined in the PSR. The reduction of any requirements is based on the original classification of information residing on the media and the level of assurance in the cryptographic product being used to encrypt the media.

13.3.8.R.03. **Rationale**

Further information on reducing storage and physical transfer requirements can be found in Section 17.1 - Cryptographic Fundamentals.

13.3.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4102]

Agencies MUST ensure that processes for transferring media containing classified information meets the minimum physical transfer requirements as specified in the PSR.

13.3.8.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4103]

Agencies SHOULD encrypt data stored on media with at least an Approved Cryptographic Algorithm (See Section 17.2 – Approved Cryptographic Algorithms) if it is to be transferred to another area or location.

Using media for data transfers

13.3.9.R.01. **Rationale**

Agencies transferring data between systems of different security domains or classifications are strongly encouraged to use media such as write-once CDs and DVDs. This will limit opportunity for information from the higher classified systems to be accidently transferred to lower classified systems. This procedure will also make each transfer a single, auditable event.

13.3.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4111]

Data transfers between systems of different classification SHOULD be logged in an auditable log or register.

13.3.9.C.02. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:4114]

Agencies transferring data manually between two systems of different security domains or classifications SHOULD NOT use rewriteable media.

Media in secure areas

13.3.10.R.01. **Rationale**

Certain types of media including USB, FireWire and eSATA capable devices MUST be disabled or explicitly approved as an exception by the Accreditation Authority for a TOP SECRET environment (the GCSB). This provides an additional level of system user awareness and security.

13.3.10.R.02. **Rationale**

This practice should be used in addition to device access control software on workstations in case system users are unaware of, or choose to ignore, security requirements for media.

13.3.10.C.01. **Control System Classifications(s): Top Secret; Compliance: Must Not** [CID:4121]

Agencies MUST NOT permit any media that uses external interface connections within a TOP SECRET area without prior written approval from the Accreditation Authority.