8.4. IT Equipment

Objective

8.4.1. IT equipment is secured outside of normal working hours, is non-operational or when work areas are unoccupied.

Context

Scope

8.4.2. This section covers information relating to the physical security of IT equipment containing media. This includes but is not limited to workstations, printers, photocopiers, scanners and multi-function devices (MFDs).

8.4.3. Additional information relating to IT equipment and media can be found in the following chapters and sections of this manual:

- Section 11.2 - Fax Machines, Multifunction Devices and Network Printers;
- Chapter 12 - Product Security; and
- Chapter 13 – Decommissioning and Disposal.

Handling IT equipment containing media

8.4.4. During non-operational hours agencies need to store media containing classified information that resides within IT equipment in accordance with the requirements of the PSR. Agencies can comply with this requirement by undertaking one of the following processes:

- ensuring IT equipment always reside in an appropriate class of secure room;
- storing IT equipment during non-operational hours in an appropriate class of security container or lockable commercial cabinet;
- using IT equipment with removable non-volatile media which is stored during non-operational hours in an appropriate class of security container or lockable commercial cabinet as well as securing its volatile media;
- using IT equipment without non-volatile media as well as securing its volatile media;
- using an encryption product to reduce the physical storage requirements of the non-volatile media as well as securing its volatile media; or
- configuring IT equipment to prevent the storage of classified information on the non-volatile media when in use and enforcing scrubbing of temporary data at logoff or shutdown as well as securing its volatile media.

8.4.5. The intent of using cryptography or preventing the storage of classified information on non-volatile media is to enable agencies to treat the media within IT equipment in accordance with the storage requirements of a lower classification, as specified in the PSR, during non-operational hours. Temporary data should be deleted at log off or shut down and volatile media secured.

8.4.6. As the process of using cryptography and preventing the storage of classified information on non-volatile media does not constitute the sanitisation and reclassification of the media, the media retains its classification for the purposes of reuse, reclassification, declassification, sanitisation, destruction and disposal requirements as specified in this manual.

IT equipment using hybrid hard drives or solid state drives

8.4.7. The process of preventing the storage of classified information on non-volatile media, and enforcing deletion of temporary data at logoff or shutdown, is NOT approved as a method of lowering the storage requirements, when hybrid hard drives or solid state drives are used.

Rationale & Controls

Accounting for IT equipment

8.4.8.R.01. **Rationale**

Ensuring that IT equipment containing media is accounted for by using asset registers, equipment registers, operational & configuration records and regular audits will assist in preventing loss or theft, or in the cases of loss or theft, alerting appropriate authorities to its loss or theft.

8.4.8.R.02. **Rationale**

Asset registers may not provide a complete record as financial limits may result in smaller value items not being recorded. In such cases other registers and operational information can be utilised to assist in building a more complete record.

8.4.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1400]

Agencies MUST account for all IT equipment containing media.

Processing requirements

8.4.9.R.01. **Rationale**

As the media within IT equipment takes on the classification of the information it is processing, the area that it is used within needs to be certified to a level that is appropriate for the classification of that information.

8.4.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1407]

Agencies MUST certify the physical security of facilities containing IT equipment to the highest classification of information being processed, stored or communicated by the equipment within the facilities.

Storage requirements

8.4.10.R.01. **Rationale**

The PSR states that either Class C, B or A secure rooms or Class C, B or A security containers or lockable commercial cabinets can be used to meet physical security requirements for the storage of IT equipment containing media. The class of secure room or security container will depend on the physical security certification of the surrounding area and the classification of the information.

8.4.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1403]

Agencies MUST ensure that when secure areas are non-operational or when work areas are unoccupied IT equipment with media is secured in accordance with the minimum physical security requirements for storing classified information as specified in the PSR Policy Framework - Physical security and supporting documents.

Securing non-volatile media for storage

8.4.11.R.01. **Rationale**

The use of techniques to prevent the storage of classified information on non-volatile media and processes to delete temporary data at logoff or shutdown may sound secure but there is no guarantee that they will always work effectively or will not be bypassed in unexpected circumstances such as a loss of power. As such, agencies need to consider these risks when implementing such a solution.

8.4.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1409]

Agencies choosing to prevent the storage of classified information on non-volatile media and enforcing scrubbing of temporary data at logoff or shutdown SHOULD:

- assess the security risks associated with such a decision; and
- specify the processes and conditions for their application within the system's SSP.

Securing volatile media for storage

8.4.12.R.01. **Rationale**

If agencies need to conduct a security risk assessment as part of the procedure for storing IT equipment containing media during non-operation hours, they should consider security risks such as:

- an attacker gaining access to the IT equipment immediately after power is removed and accessing the contents of volatile media to recover encryption keys or parts thereof. This is sometimes described as a data remanence attack;
- extreme environmental conditions causing data to remain in volatile media for extended periods after the removal of power; and
- the physical security of the locations in which the IT equipment will reside.

8.4.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1412]

Agencies securing volatile media for IT equipment during non-operational hours SHOULD:

- disconnect power from the equipment the media resides within;
- assess the security risks if not sanitising the media; and
- specify any additional processes and controls that will be applied within the system's SSP.

Encrypting media within IT equipment

8.4.13.R.01.

Rationale

Current industry good practice is to encrypt all media within IT equipment. Newer operating systems provide this functionality and older operating systems can be supported with the use of open source or proprietary applications.

8.4.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1415]

Agencies SHOULD encrypt media within IT equipment with an Approved Cryptographic Algorithm. See Section 17.2 - Approved Cryptographic Algorithms.