13.2. Media Handling

Objective

13.2.1. Media is properly classified, labelled and registered in order to clearly indicate the required handling instructions and degree of protection to be applied.

Context

Scope

13.2.2. This section covers information relating to classifying, labelling and registering media. Information relating to classifying and labelling IT equipment can be found in Section 12.3 - Product Classifying and Labelling.

Exceptions for labelling and registering media

13.2.3. Labels are not needed for internally mounted fixed media if the IT equipment containing the media is labelled. Likewise fixed media does not need to be registered if the IT equipment containing the media is registered.

References

13.2.4. Additional information relating to media handling is contained in:

Reference	Title	Publisher	Source
ISO/IEC 27001:2013	**10.7, Media Handling**	ISO	https://www.iso.org/standard/54534.html

PSR references

13.2.5. 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

Reclassification and declassification procedures

13.2.6.R.01. **Rationale**

When reclassifying or declassifying media the process is based on an assessment of risk, including:

- the classification of the media and associated handling instructions;
- the effectiveness of any sanitisation or destruction procedure used;
- the planned redeployment; and

- the intended destination of the media.

13.2.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3896]

Agencies MUST document procedures for the reclassification and declassification of media.

Classifying media storing information

13.2.7.R.01. **Rationale**

Media that is not classified or not correctly classified may be stored, identified and handled inappropriately.

13.2.7.R.02. **Rationale**

Incorrect or no classification may result in access by a person or persons without the appropriate security clearance.

13.2.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3904]

Agencies MUST classify media to the highest classification of data stored on the media.

Classifying media connected to systems of higher classifications

13.2.8.R.01. **Rationale**

Unless connected through a data diode or similar infrastructure, there is no guarantee that classified information was not copied to the media while it was connected to a system of higher classification than the classification level of the media itself.

13.2.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3910]

Agencies MUST classify any media connected to a system of a higher classification at the higher system classification until confirmed not to be the case.

Classifying media below that of the system

13.2.9.R.01. **Rationale**

When sufficient assurance exists that information cannot be written to media that is used with a system, then the media can be treated in accordance with the handling instructions of the classification of the information it stores rather than the classification of the system it is connected to or used with.

13.2.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3915]

Agencies intending to classify media below the classification of the system to which it is connected to MUST ensure that:

- the media is read-only;
- the media is inserted into a read-only device; or
- the system has a mechanism through which read-only access can be assured such as approved data diodes, write-blockers or similar infrastructure.

Reclassifying media to a lower classification

13.2.10.R.01. **Rationale**

Agencies must follow the reclassification process as illustrated in Section 13.6 – Media Disposal.

13.2.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3922]

Agencies wishing to reclassify media to a lower classification MUST ensure that:

- a formal decision is made to reclassify, or redeploy the media; and
- the reclassification of all information on the media has been approved by the originator, or the media has been appropriately sanitised or destroyed.

Reclassifying media to a higher classification

13.2.11.R.01. **Rationale**

The media will always need to be protected in accordance with the classification of the information it stores. As such, if the classification of the information on the media changes, then so will the classification of the media.

13.2.11.C.01.

Control System Classifications(s): All Classifications; Compliance: Must [CID:3979]

Agencies MUST reclassify media if:

- information copied onto the media is of a higher classification; or
- information contained on the media is subjected to a classification upgrade.

Labelling media

13.2.12.R.01. **Rationale**

Labelling helps all personnel to identify the classification of media and ensure that they afford the media the correct protection measures.

13.2.12.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:3982]

Agencies MUST label media with a marking that indicates the maximum classification and any endorsements applicable to the information stored.

13.2.12.C.02. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must** [CID:3983]

Agencies MUST ensure that the classification of all media is easily visually identifiable.

13.2.12.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3984]

When using non-textual (colour, symbol) protective markings for operational security reasons, agencies MUST document the labelling scheme and train personnel appropriately.

13.2.12.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3985]

Agencies SHOULD label media with a marking that indicates the maximum classification and any endorsements applicable to the information stored.

Labelling sanitised media

13.2.13.R.01. **Rationale**

It is not possible to effectively sanitise and subsequently reclassify SECRET or TOP SECRET non-volatile media to a classification lower than SECRET. Media of other classifications may be reclassified (See Section 13.6 – Media Disposal).

13.2.13.C.01. **Control System Classifications(s): Secret, Top Secret; Compliance: Must** [CID:3988]

Agencies MUST label non-volatile media that has been sanitised and reclassified for redeployment with a notice similar to:

Warning: media has been sanitised and reclassified from [classification] to [classification]. Further lowering of classification only via destruction.

Registering media

13.2.14.R.01. **Rationale**

If agencies fail to register media with an appropriate identifier they will not be able to effectively keep track of their classified media and there will be a greater likelihood of unauthorised disclosure of classified information.

13.2.14.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:3991]

Agencies MUST register all media with a unique identifier in an appropriate register.

13.2.14.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3992]

Agencies SHOULD register all media with a unique identifier in an appropriate register.