Media Protection (MP)

Purpose:

The following standards are established to support the policy statement 10.11 that "CSCU will: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse."

Scope:

1. Institutional Units of the Connecticut State College and University System including the Connecticut Board of Regents System Office.

2. All Connecticut State College and University institutional units' information systems.

Standard:

1. Media Access [NIST 800-53r4 MP2]

1.1 For all information systems, the Data Owner and Information System Owner ensure that access to digital media is restricted to authorized users.

2. Media Marking [NIST 800-53r4 MP3]

2.1 For all moderate and high risk information systems, the Data Owner and Information System Owner ensure that:

a.) Information system digital media is marked indicating the distribution limitations, handling caveats, and applicable data classification markings (if any) of the information.

3. Media Storage [NIST 800-53r4 MP4]

3.1 For all moderate and high risk information systems, the Data Owner and Information System Owner ensure that:

a.) All digital media is physically controlled and stored within environmentally appropriate, and access restricted environments.

b.) Data stored on secondary storage devices (devices that retain copies of data stored on primary data storage devices) must be encrypted.

c.) Information system media is protected until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

4. Media Transport [NIST 800-53r4 MP5]

4.1 For all moderate and high risk information systems, the Data Owner and Information System Owner ensure that:

a.) Digital media is protected and controlled during transport outside of controlled areas using defined security measures that are CSCU approved;

b.) Accountability is maintained for information system media during transport outside of controlled areas;

c.) Activities associated with the transport of information system media are documented; and

d.) The activities associated with the transport of information system media is restricted to authorized personnel.

e.) The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. [NIST 800-53r4 MP-5(4)]

5. Media Sanitization [NIST 800-53r4 MP6]

5.1 For all information systems, the Data Owner and Information System Owner ensure that:

a.) Digital media is sanitized prior to disposal, release out of organizational control, or release for reuse using approved CSCU sanitization techniques and procedures in accordance with applicable federal and state standards and policies; and

b.) Sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information are employed.

5.2 For high risk information systems, the Data Owner and Information System Owner ensure that media sanitization and disposal actions are reviewed, approved, tracked, documented, and verified. [NIST 800-53r4 MP6 (1)]

5.3 For high risk information systems, the Data Owner and Information System Owner ensure that testing to sanitization equipment and procedures to verify that the intended sanitization is being achieved occurs annually. [NIST 800-53r4 MP6 (2)]

5.4 For moderate and high risk information systems, the Data Owner and Information System Owner ensure that nondestructive sanitization techniques are applied to portable storage devices prior to connecting such devices to the information system under the following circumstances:

a.) Such devices are first purchased from the manufacturer or vendor prior to initial use; or

b.) The organization loses a positive chain of custody for the device.

6. Media Use [NIST 800-53r4 MP7]

6.1 For all information systems, ISPO will approve removable media device types and requirements for use with information systems.

6.2 For all information systems, the Data Owner and Information System Owner ensure that:

a.) Non-CSCU approved removable media device use on information systems is prohibited.

6.3 For all moderate and high risk information systems, the Data Owner and Information System Owner prohibits the use of portable storage devices when such devices have no identifiable owner. [NIST 800-53r4 MP-7(1)]

Roles & Responsibilities

Refer to the Roles and Responsibilities located on the website.

Definitions

Security Marking The term security marking refers to the application/use of human-readable security attributes.

Digital Media A form of electronic media where data are stored in digital (as opposed to analog) form.

Non-digital Media Non-digital media includes, for example, paper and microfilm.

Controlled Areas	Controlled areas are areas or spaces for which CSCU provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems.
Information System Media	Information system media includes both digital and non-digital media.
Removable Media	Portable data storage medium that can be added to or removed from a computing device or network. Note: Examples include, but are not limited to: optical discs (CD, DVD, Blu-ray); external / removable hard drives; external / removable Solid State Disk (SSD) drives; magnetic / optical tapes; flash memory devices (USB, eSATA, Flash Drive, Thumb Drive); flash memory cards (Secure Digital, CompactFlash, Memory Stick, MMC, xD); and other external / removable disks (floppy, Zip, Jaz, Bernoulli, UMD).
Portable Storage Devices	A Portable device that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data).
Sanitization	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.

References

ITS-04 CSCU Information Security Policy

NIST 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

NIST 800-171 Rev. 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, December 2016.