PURPOSE

Develop policies and procedures for information system maintenance.

PROCESS

Media Protection Policy and Procedures (MP-01)

The College:

A. Develops, documents, and disseminates to information system owners:
    1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
B. Reviews and updates the current:
    1. Media protection policy biennially; and
    2. Media protection procedures annually.

Media Protection Policy

All electronic media containing sensitive or personally identifiable information must be protected and secured to limit access to authorized personnel and systems only. Electronic media in employee portable devices must be encrypted using current cryptographic technology (IA-07). Portable media containing sensitive or personally identifiable information must be encrypted using current cryptographic technology (IA-07). Electronic media while not physically in its information system must be physically stored in a locked room or container.

All electronic media must be destroyed using means of physical destruction or using crypto or secure erase techniques per NIST guidelines. Documentation of electronic media including serial numbers of hard drives disposed must be maintained for three years by information system owners.

Information system owners are responsible for implementing the media protection policy.

Media Access (MP-02)

The College restricts access to removable media containing sensitive or personally identifiable information to information system owners and authorized users.

Media Sanitization (MP-06)

The College:

A. Sanitizes portable and removable media prior to disposal, release out of organizational control, or release for reuse using physical destruction, crypto or secure erase techniques in accordance with applicable federal and organizational standards and policies; and

B. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Information Technology has primary responsibility for sanitizing and disposing of media in coordination with the Purchasing department.

Media Use (MP-07)

The College prohibits the use of portable media containing sensitive or personally identifiable information that is not encrypted.

- Temple College is responsible for IT regulatory compliance as specified by the Department of Education, the Texas Higher Education Coordinating Board, and the State of Texas Administrative Code (TAC202) for Information Technology. The IT policies include the specific guidance, requirements, and procedures in line with the regulatory and audit requirements.