PURPOSE

Develop policies and procedures for information system and services.

PROCESS

Information System and Services Policy and Procedures (SA-01)

The College:

A. Develops, documents, and disseminates budget managers:
    1. An information system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Procedures to facilitate the implementation of the information system and services acquisition policy and associated information system and services acquisition controls; and
B. Reviews and updates the current:
    1. Information system and services acquisitions policy biennially; and
    2. Information system and services acquisitions procedures annually.

Information System and Services Policy Allocation of Resources (SA-02)

The College:

A. Determines information security requirements for the information system or information system service in mission/business process planning;
B. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
C. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

System Development Life Cycle (SA-03)

The College:

A. Determines information security requirements for the information system or information system service in mission/business process planning;
B. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
C. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Acquisition Process (SA-04)

The College includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders,

directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

A. Security functional requirements;
B. Security strength requirements;
C. Security assurance requirements;
D. Security-related documentation requirements;
E. Requirements for protecting security-related documentation;
F. Description of the information system development environment and environment in which the system is intended to operate; and
G. Acceptance criteria.

Before acquisition, information technology or processing systems receiving, containing or processing personallyidentifiable information, protected health information or institutional data whether operating on premise or in the cloud must be reviewed and approved by the Chief Information Security Officer (CISO).

Information System Documentation (SA-05)

The College:

A. Obtains administrator documentation for the information system, system component, or information system service that describes:
    1. Secure configuration, installation, and operation of the system, component, or service;
    2. Effective use and maintenance of security functions/mechanisms; and
    3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
B. Obtains user documentation for the information system, system component, or information system service that describes:
    1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
    2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
    3. User responsibilities in maintaining the security of the system, component, or service;
C. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and is retained by the information system owner in response;
D. Protects documentation as required, in accordance with the risk management strategy; and
E. Distributes documentation to information system custodians and applicable documentation to users.

External Information System (SA-09)

The College:

A. Requires providers of external information system services comply with college information security requirements and comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
B. Information system owners are responsible for oversight, defining user roles and responsibilities; and
C. Information system owners are responsible to monitor security control compliance by external service providers on an ongoing basis.

Developer Configuration Management (SA-10)

The College requires the developer of the information system, system component, or information system service to:

A. Perform configuration management during system, component, or service design, development, implementation and operation;
B. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];
C. Implement only college-approved changes to the system, component, or service;
D. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
E. Track security flaws and flaw resolution within the system, component, or service and report findings to information system owner and Chief Information Security Officer (CISO).

- 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.