PURPOSE

Develop policies and procedures for security program.

PROCESS

Information Security Program Plan (PM-01)

The College:

A. Develops and disseminates an organization-wide information security program plan that:
    1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
    2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
    3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and
    4. Is approved by the Chief Information Security Officer (CISO) with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;
B. Reviews the organization-wide information security program annually;
C. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and
D. Protects the information security program plan from unauthorized disclosure and modification.

Senior Information Security (PM-02)

The College appoints a Chief Information Security Officer (CISO) with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Information Security Resources (PM-03)

The College:

A. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;
B. Employs a business case Exhibit 300/Exhibit 53 to record the resources required; and
C. Ensures that information security resources are available for expenditure as planned.

Plan of Action and Milestones (PM-04)

The College:

A. Implements a process ensuring plans of action and milestones for the security program and associated organizational information systems:

1. Are developed and maintained;
2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
3. Are reported in accordance with OMB FISMA reporting requirements.

B. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Information Security Inventory (PM-05)

The Information Technology Department develops and maintains an inventory of its information systems. The physical inventory must be maintained in the technology help desk system.

Information Security Measures of Performance (PM-06)

The Information Technology Department develops, monitors, and reports on the results of information security measures of performance. Monthly security reports must be submitted to the Information Systems Network and Infrastructure Team per their requirements. Annual security program vulnerability assessment is presented and acknowledged by the Division Director of Information Technology.

Enterprise Architecture (PM-07)

The Information Technology Department develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

The Division Director of Information Technology must develop an enterprise architecture in consideration of information security and risks to College data and operations.

Threat Awareness Program (PM-16)

The Information Technology Department implements a threat awareness program that includes a cross-organization information-sharing capability.

The Chief Information Security Officer (CISO) must develop a threat awareness program sharing cybersecurity information amongst information system owners, yearly cybersecurity awareness training for employees, and training as part of new employee orientation.

- 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.