PURPOSE

Develop policies and procedures for risk assessment.

PROCESS

Risk Assessment Policy and Procedures (RA-01)

The College Information Technology Department:

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

Risk Assessment Policy

Security Categorization (RA-02)

The College Information Technology Department:

A. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
B. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
C. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

Risk Assessment (RA-02)

The College Information Technology Department:

A. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
B. Documents risk assessment results in risk assessment report;
C. Reviews risk assessment results annually;
D. Disseminates risk assessment results to Chief Information Security Officer (CISO), The Division Director of Information Technology, and owners as appropriate; and
E. Updates the risk assessment annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Vulnerability Scanning (RA-05)

The College Information Technology Department:

A. Scans for vulnerabilities in the information system and hosted applications periodically to confirm information systems are running the latest versions and when new vulnerabilities potentially affecting the system/applications are identified and reported;
B. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and
    3. Measuring vulnerability impact;
C. Analyzes vulnerability scan reports and results from security control assessments;
D. Remediates legitimate vulnerabilities in coordination with information system owners and custodians in accordance with an organizational assessment of risk; and
E. Shares information obtained from the vulnerability scanning process and security control assessments with information system owners and custodians to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
    1. Affected system(s) may be isolated from the network.

*If the Chief Information Security Officer (CISO) and the Division Director of Information Technology are the same individual, the coordination as indicated in the policy requires coordination with immediate supervisor.

- 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.