PURPOSE

Develop policies and procedures for information systems and information integrity.

PROCESS

Information Systems and Information Integrity Policy and Procedures (SI-01)

The College:

A. Develops, documents, and disseminates to information system owners and custodians:
    1. An information system and information integrity 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 information integrity policy and associated information system and information integrity controls; and
B. Reviews and updates the current:
    1. Information System and information integrity policy biennially; and
    2. Information System and information integrity procedures annually.

Information System and Information Integrity Policy Flaw Remediation (SI-02)

The College:

A. Identifies, reports, and corrects information system flaws;
B. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
C. Installs security-relevant software and firmware updates by the established standards for each type of system of the release of the updates; and
    a. Software and update standards are developed in cooperation with the information system owners, information custodians and Chief Information Security Officer (CISO) based on risk mitigation analysis. (CM-01)
D. Incorporates flaw remediation into the organizational configuration management process. (CM-03)

Malicious Code Protection (SI-03)

The College:

A. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
B. Updates malicious code protection mechanisms whenever new releases are available in accordance with College configuration management policy and procedures;
C. Configures malicious code protection mechanisms to:
    1. Perform periodic scans of the information system weekly at minimum and real-time scans of files from external sources at endpoint; network entry/exit points as the files are downloaded, opened, or executed in accordance with College security policy; and
    2. Block malicious code; quarantine malicious code; send alert to administrator; in response to malicious code detection; and

D. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system per incident response plan (IR-08).

Information System Monitoring (SI-04)

The College:

A. Monitors the information system to detect:
    1. Attacks and indicators of potential attacks in accordance with the information security plan; and
    2. Unauthorized local, network, and remote connections;
B. Identifies unauthorized use of the information system through information security plan;
C. Deploys monitoring devices:
    1. strategically within the information system to collect organization-determined essential information; and
    2. at ad hoc locations within the system to track specific types of transactions of interest to the organization;
D. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
E. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations the Nation based on law enforcement information, intelligence information, or other credible sources of information;
F. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
G. Provides information security assessment data to information system owners and custodians annually or as needed.

Security Alerts, Advisories and Directives (SI-05)

The College:

A. The Chief Information Security Officer (CISO) and designees receive information system security alerts, advisories, and directives from internal and external sources as defined in the information security plan on an ongoing basis;
B. Generates internal security alerts, advisories, and directives as deemed necessary;
C. Disseminates security alerts, advisories, and directives to information system owners, custodians and users; and
D. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Information Output Handling and Retention (SI-12)

The College handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

- 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.