PURPOSE

Develop policies and procedures for information system incident response.

PROCESS

Incident Response Policy and Planning (IR-01)

The College:

A. Develops, documents, and disseminates to information resource owners or custodians and third parties:
    1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
B. Reviews and updates the current:
    1. Incident response policy biennially; and
    2. Incident response procedures annually.

Incident Response Training (IR-02)

The College provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within 60 days of assuming an incident response role or responsibility; b. when required by information system changes; and c. annually thereafter.

Incident Handling (IR-04)

The College:

A. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
B. Coordinates incident handling activities with contingency planning activities; and
C. Incorporates lessons learned from ongoing incident handling activities into incident response procedures,training, and testing/exercises, and implements the resulting changes accordingly.

Incident Monitoring (IR-05)

The College tracks and documents information system security incidents using a combination of logging and alerts from information security systems. Both automated and human-based detection is utilized. Incident remediation is tracked using the help desk ticketing system.

Incident Reporting (IR-06)

The College:

A. Requires personnel to report suspected security incidents to the Help Desk immediately; and
B. Reports security incident information to the Chief Information Security Officer (CISO).

The Chief Information Security Officer (CISO) must follow information security incident reporting requirements designated by the Department of Information Resources State of Texas.

Incident Response Assistance (IR-07)

The College provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

The Chief Information Security Officer (CISO) and Temple College Information Technology Department form the core resource to assist users.

Incident Response Plan (IR-08)

The College:

A. Develops an incident response plan that:
    1. Provides the organization with a roadmap for implementing its incident response capability;
    2. Describes the structure and organization of the incident response capability;
    3. Provides a high-level approach for how the incident response capability fits into the overall organization;
    4. Meets the unique requirements of the organization, which relate to mission, size, structure, andfunctions;
    5. Defines reportable incidents;
    6. Provides metrics for measuring the incident response capability within the organization;
    7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
    8. Is reviewed and approved by the Division Director of Information Technology and the Chief Information Security Officer (CISO);
B. Distributes copies of the incident response plan to information resource owners;
C. Reviews the incident response plan annually;
D. Updates the incident response plan to address system/organizational changes or problems encounteredduring plan implementation, execution, or testing;
E. Communicates incident response plan changes to information system owners and
F. Protects the incident response plan from unauthorized disclosure and modification.

*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.