PURPOSE

Establish procedures and policies to establish a security assessment procedure.

PROCESS

Security Assessment and Authorization Policy and Procedures (CA-01)

The Division Director of Information Technology and the Chief Information Security Officer (CISO) in coordination with information system owners:

A. Develops, documents, and disseminates to information system owners:

1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and

B. Reviews and updates the current:

1. Security assessment and authorization policy as necessary; and
2. Security assessment and authorization procedures as necessary.

Security Assessment Policy Security Assessments (CA-02)

A review of the College's information security program for compliance with these standards will be performed at least biannually, based on business risk management decisions, by individual(s) independent of the information security program and designated by the Division Director of Information Technology or his or her designated representative(s).

The Division Director of Information Technology and Chief Information Security Officer (CISO) must develop a security assessment plan. The security assessment will review the security controls and operation determining the extent to which the controls are implemented correctly and operate as intended. The assessment must be performed by individual(s) independent of the Chief Information Security Officer (CISO). The results of the security assessment must be reported to the President, the Temple College Board of Trustees, and Executive Cabinet.

System Interconnections (CA-03)

The Division Director of Information Technology authorizes all connections from internal/organization information system to other information systems outside of organization through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.

Information Technology must authorize all dedicated sustained connections from an information resource to external information resources through the use of interconnection security agreements. Document each interconnection interface, security requirements and information communicated. Agreements must be reviewed by Chief Information Security Officer (CISO) and updated as necessary. These connections will be included in the annual risk assessments.

Plan of Action and Milestones (CA-05)

The Division Director of Information Technology develops and updates, a plan of action and milestones for the information systems that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

The Division Director of Information Technology in coordination with Chief Information Security Officer (CISO) must develop a plan of action including milestones to remediate deficiencies noted during security assessments and reduce or eliminate known vulnerabilities in the system in particular applying security patches and software updates.

Security Authorization (CA-06)

The Division Director of Information Technology authorizes the information system for processing before operations or when there is a significant change to the system.

An Information Technology resource owner is assigned to each information system. The Division Director of Information Technology must authorize the information resource for processing before commencing operations and ensures the security authorization is updated.

Continuous Monitoring (CA-07)

The Information Technology department monitors the security controls in the information system on an ongoing basis.

The Chief Information Security Officer (CISO) in coordination with the Division Director of Information Technology must develop a continuous monitoring strategy and implement continuous monitoring including metrics to be monitored along with monitoring methodology and response actions to the correlation of related security monitoring events.

Penetration Testing (CA-08)

The Information Technology department conducts penetration testing at least biannually on external facing information systems.

The Chief Information Security Officer (CISO) coordinates with the Division Director of Information Technology in the conduct of penetration testing to confirm vulnerabilities are corrected and access controls are in-place. The results of penetration testing are part of the security assessment.

Internal System Connections (CA-09)

The Information Technology department has a procedure for authorizing internal information resource connections.

The Division Director of Information Technology must authorize all dedicated sustained connections from an information resource to internal information resources. Document each interconnection interface, security requirements and information communicated. Connections must be reviewed by Chief Information Security Officer (CISO) and updated annually. These connections will be included in the annual risk assessments.

*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.