PURPOSE

Develop, maintain and test continuity of operations plans for information systems.

PROCESS

Contingency Planning (CP-01)

The College must maintain written Master Emergency Plan that address information resources so the effects of a disaster will be minimized, and the College will be able either to maintain or quickly resume mission-critical functions.

The Division Director of Information Technology in coordination with the Chief Information Security Officer (CISO) must develop and maintain a contingency/disaster recovery plan addressing critical information systems. The plan must include controls addressing purpose, scope, roles, responsibilities, management commitment and coordination among information owners and College departments.

Contingency Plan (CP-02)

The plan must be distributed to key personnel and a copy stored offsite. Elements of the plan for information resources must include:

A. Business Impact Analysis to systematically assess the potential impacts of a loss of business functionality due to an interruption of computing and/or infrastructure support services resulting from various events or incidents. The analysis must identify the following elements:

1. Mission-Critical Information Resources (specific system resources required to perform critical functions) to include:

    A. Internal and external points of contact for personnel that provide or receive data or support interconnected systems.

    B. Supporting infrastructure such as electric power, telecommunications connections, and environmental controls.

2. Disruption impacts and allowable outage times to include:

    A. Effects of an outage over time to assess the maximum allowable time that a resource may be denied before it prevents or inhibits the performance of an essential function.

    B. Effects of an outage across related resources and dependent systems to assess cascading effectson associated systems or processes.

3. Recovery priorities that consider geographic areas, accessibility, security, environment, and cost and may include a combination of:

    a. Preventive controls and processes such as backup power, excess capacity, environmental sensors and alarms.

b. Recovery techniques and technologies such as backup methodologies, alternate sites, software and hardware equipment replacement, implementation roles and responsibilities.

c. Risk Assessment to weigh the cost of implementing preventative measures against the risk of loss from not taking action.

c. Implementation, testing, and maintenance management program addressing the initial and ongoing testing and maintenance activities of the plan.

d. Disaster Recovery Plan—The College must maintain a written disaster recovery plan for major or catastrophic events that deny access to information resources for an extended period. Information learned from tests conducted since the plan was last updated will be used in updating the disaster recovery plan. The disaster recovery plan will:

1. Contain measures which address the impact and magnitude of loss or harm that will result from an interruption;

2. Identify recovery resources and a source for each;

3. Contain step-by-step implementation instructions;

4. Include provisions for annual testing.

Contingency Training (CP-03)

The College trains personnel in their contingency roles and responsibilities with respect to the information system and provides periodic refresher training.

The information system managers must ensure training is available to personnel in support of their roles in maintaining and implementing the contingency plan. Training must occur when personnel assume a role or responsibility related to the contingency plan or when required by significant information resource configuration changes.

Contingency Plan Testing (CP-04)

The College's written disaster recovery plan will include provisions for annual testing.

The information system managers will include annual testing of the disaster recovery plan. The testing should include elements of restoring from backup data and applications and testing the interconnectedness of the recovered systems to ensure functionality.

Alternate Storage Site (CP-06)

Mission-critical information must be backed up on a scheduled basis and stored off site in a secure,environmentally safe, locked facility accessible only to authorized College representatives.

The location and methods of storing mission critical data must be part of the contingency plan and meet the requirements of geographically disperse, securely stored, accessible during a disruption and recoverability.

Information System Backup (CP-09)

The College conducts backups of system-level information (including system state information) and critical user-level information contained in the information system and protects backup information at the storagelocation.

The Information Technology Department must develop, implement and verify backups of information systems and their data are conducted on a regular basis supporting data recovery needs and the contingency plan. The backup plan must be regularly reviewed by information system owners to ensure it meets business objectives.

Information System Recovery (CP-10)

The College employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.

The Information Technology Department must include in operations of information systems backup and restore states providing the ability to recover or reconstitute system data in cases of disruption or failure.
These operations could be included as part of the information system backup or separately established restore points during critical updates or configuration changes.

*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.