Texas A&M University System Contingency Planning Standard

Purpose

The purpose of this Standard is to ensure that the business functions and information resources of the Texas A&M member institutions ("member(s)") are protected against service interruptions, including large-scale disasters, by the development, implementation, and testing of contingency plans.

Scope

This Standard applies to all members and to all individuals employed at those members.

Roles and Responsibilities

The CEO of each member shall:

- Appoint one or more persons to a Contingency Planning Management Team ("CPMT") or designate an existing group as the CPMT. CPMT members should come both from information technology and from other member units e.g. HR, police, senior management.
- Ensure that the Chief Information Officer ("CIO") and the Information Security Officer ("ISO") and are members of the CPMT.

The CIO of each member shall:

- At least annually, review and approve the member's documented Continuity of Operations Plan ("CoOP").

The CPMT shall:

- Have overall responsibility for the member's Contingency Planning ("CP") efforts.
- Ensure member compliance with and implementation of various CP law and policy, including the "State Implementation" sections of the CP family of controls in the DIR Security Control Standards Catalog.
- Develop and document the member's CoOP, which contains the member's Disaster Recovery plan ("DR plan"). See "Additional Required CoOP Elements" below.
- Ensure distribution of CoOP hardcopies to all relevant personnel and the storage of at least one hardcopy offsite.
- Make an electronic copy of the plan available to all relevant personnel.
- At least annually, review the CoOP, revise if necessary, and redistribute.
- At least annually, present the CoOP to the CIO for his or her approval.

Additional Required CoOP Elements

In addition to the elements required by the DIR Security Control Standards Catalog, each member's CoOP shall contain the following elements:

1. At least annually, the DR Plan shall be tested with a tabletop exercise.
2. At least every 3 years, the DR Plan provisions for mission-critical, on-premise services shall be tested with a full interruption.

Appendix: What DIR Says About Contingency Planning and Disaster Recovery

The key sections of the DIR Security Control Standards Catalog are CP-1 and CP-2.

The "State Implementation" section of CP-1 says that "[s]tate organizations shall maintain written Continuity of Operations Plans that address information resources so that the effects of a disaster will be minimized..." So, there shall be one or more CoOPs, and their purpose is to minimize the effects of a disaster.

The "State Implementation" section of CP-2 talks about "the plan" and enumerates "elements of the plan," one of which elements is a Disaster Recovery Plan. Therefore, "the plan" appears to refer to the larger CoOP, of which the DR plan is a subplan. According to CP-2, the DR Plan shall:

a. Be written;
b. Include provisions for annual testing and be tested annually;
c. Be updated with the results of the annual test;
d. Contain measures which address the impact and magnitude of loss or harm that will result from an interruption;
e. Identify recovery resources and a source for each;
f. Contain step-by-step implementation instructions;

1. CP-1 Contingency Planning

State Implementation

State organizations shall maintain written Continuity of Operations Plans that address information resources so that the effects of a disaster will be minimized, and the state organization will be able either to maintain or quickly resume mission-critical functions.

Example

Written, documented CoOP documentation is in place.

2. CP-2 Contingency Plan

State Implementation

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

a. Business Impact Analysis to assess systematically 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 shall 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 effects on 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.

b. 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--Each state organization shall 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.