Texas A&M University System Standard – Disaster Recovery Planning

Standard Statement

Maintaining a disaster recovery plan as part of a business continuity plan is of key importance in providing the ability to minimize the effects of a disaster. A disaster recovery plan that is kept up to date and tested on a regular basis allows a department to resume mission-critical functions in a timely and predictable manner.

Definitions

Information Resources (IR) - the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Mission Critical Information - information that is defined by the System Office or information resource owner to be essential to the continued performance of the mission of the System Office or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, and failure to comply with regulations or legal obligations, or closure of the department.

Owner of an Information Resource - an entity responsible for:

- A business function; and,
- Determining controls and access to information resources supporting that business function.

Official Standards

1. Applicability

This standard applies to all mission critical information resources.

The information resource owner or designee (e.g., custodian, user) is responsible for ensuring that the risk mitigation measures described in this standard are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this standard. All exclusions must be in

accordance with the standard *Exclusions from Required Risk Mitigation Measures*.

2. Standards

2.1 A documented disaster recovery plan shall be maintained for all mission critical information resources. The plan will contain: measures that address the impact and magnitude of loss or harm that will result from an interruption; identify recovery resources and a source for each; and contain step-by-step instructions for implementing the plan. The information resource owner or designee will approve the plan.

2.2 The plan shall be tested at least annually. Tests of the plan may include a range of testing methods from virtual (e.g., table-top) tests to actual events which may encompass testing individual elements that are mission-critical to recovery, such as networks and financial systems. The tests shall be documented and the results shall be used to update the plan if needed. The information resource owner or designee shall approve the results of the tests and any resulting actions. Additional guidance can be obtained from the standards under System Regulation 29.01.03.

2.3 Back-up/recovery media must be tested on a regular basis (at least annually) to ensure the validity of the recovery media and process.

Related Statutes, Policies, or Requirements

Supplements *System Regulation 29.01.03* and the standard for *Contingency Planning*

Related Standards see the standard for *Backup Recovery*

Contact Office

For interpretation or clarification, contact The Texas A&M University System Chief Information Officer and the System Chief Application Architect.

OFFICE OF RESPONSIBILITY: The Texas A&M University System Chief Information Officer