Procedure Statement

This Procedure establishes processes for effective information-technology (“IT”) disaster-recovery planning. This Procedure applies to all IT systems at Texas A&M University-Corpus Christi. The intended audience of this Procedure is all Owners and Custodians of University IT systems.

Reason for Procedure

IT disaster-recovery planning is a required component of widely-adopted information-security frameworks (e.g., NIST 800-53). 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.

Procedure

1. For each University IT system (“the system”), the Owner(s) of the system or their designee(s) shall:

   1.1. Determine a Recovery Time Objective (RTO) and a Recovery Point Objective (RPO) for the system. Those determinations should be made in consultation with: 1) the owners of business processes that depend directly on the system; 2) the Custodian(s) of the system; 3) the Owner(s) and Custodian(s) of information resources that depend directly on the system, and; 4) the Owner(s) and Custodian(s) of information resources upon which the system directly depends. In particular, the RTO and RPO values should support the RTO and RPO requirements of the business-process owners as documented in the business continuity plans of those business-process owners.

   1.2. Create a documented disaster recovery plan (“the DR plan”) for the system or associate the system with an existing plan. If a new DR plan is created for a given system, the presumption is that the Owner of the system is the Owner of the DR plan.
1.3. Ensure that the DR plan:

1.3.1. Contains the RTO and RPO determinations and identifies which measures the system Owner will implement to support those commitments. Examples of such measures include: alternate sources of key information resources and skills; locked rooms; fire suppression; uninterruptible power supplies; redundant hardware components (e.g. NICs, power supplies, RAID); onsite and offsite data backups; server clustering, and; backup sites.

1.3.2. Identifies dependencies, i.e., other resources that must be operational for the system to be operational, e.g., electricity, air conditioning, network connectivity, authentication services.

1.3.3. Identifies primary and backup personnel, vendors, contractors, etc. required to recover the system, and primary and alternate contact information for those parties.

1.3.4. Identifies a recovery team that will lead the recovery effort for that system, and a command structure for that team.

1.3.5. Identifies a primary method of recovery-team communication (e.g., University email) and a secondary method of recovery-team communication (e.g., third-party chat service) in case the primary is unavailable.

1.3.6. Contains step-by-step processes for 1) determining when disaster recovery plans should be activated (e.g., specific triggers), and 2) performing recovery processes (e.g., restoring a backup, switching to a backup site).

1.3.7. Contains or identifies key information required to recover the resource, e.g., passwords, contract numbers, and license keys.

1.4. At least annually, 1) review the plan, 2) update the plan if warranted, and 3) submit the plan to IRM for approval via the University’s risk-assessment process.

1.5. For those systems designated by the Chief Information Officer (CIO) as critical, test the plan at least annually.

1.5.1. Tests of the plan may include a range of testing methods from virtual (e.g., table-top exercises) to actual events (e.g., file restores).

1.5.2. Tests of the plan must be documented to be valid.

Training

The Information Technology Department will provide training and assistance to Owners and others upon request.
Monitoring

Documented DR plans will be stored in the University’s inventory of information resources and reviewed annually as part of the risk assessment process.

Related Policies

- Texas A&M University – Corpus Christi Procedures
  - 29.01.03.C2.05 Backup/Recovery
  - 29.01.03.C2.24 Vendor Access
  - 29.01.03.C2.18 Risk Assessment

Definitions

Please refer to University Procedure 29.01.03.C2.01 Definitions. The following definitions apply to this Procedure only.

Information Resource Manager or IRM is defined in §2054.071 of the Texas Government Code. At Texas A&M University – Corpus Christi the CIO is the IRM.

An IT system is a logical collection of information resources that provides a service. For example, an IP address management system might comprise several servers and the IPAM server software. Each system is an information resource in its own right.

The Recovery Time Objective (RTO) for a given information resource is a number that represents the maximum time the information resource can be unavailable, as determined by the business process owners who depend on that information resource. For example, an RTO of one week for a given information resource means that the business process owners have determined that that information resource cannot be unavailable for more than a week; otherwise the institution will suffer significant harm to its operations.

The Recovery Point Objective (RPO) for a given information resource is a number that represents that maximum amount of recent data can be lost as determined by the business process owners who depend on that data. For example, an RPO of 24 hours for a given information resource means that the business process owners have determined that no more than
the most recent 24 hours’ worth of data entered into that information resource may be lost; otherwise the institution will suffer significant harm to its operations.

________________________________________________________

Contact Office

________________________________________________________

For clarification and interpretation, contact the Information Resource Manager at (361) 825-2693.