UTEP Standard 6: Backup and Disaster Recovery

6.1 Backup Plan Requirement. All UTEP Data, including Data associated with research, must be backed up in accordance with Risk management decisions implemented by the Data Owner. Each Institution's Backup plan must incorporate Procedures for:

(a) recovering Data and applications in case of events such as natural disasters, system disk drive failures, espionage, Data entry errors, human error, or system operations errors;

(b) assigning operational responsibility for backing up of all Servers;

(c) scheduling Data Backups and establishing requirements for off-site storage;

(d) securing on-site/off-site storage and Media in transit; and

(e) testing Backup and recovery Procedures.

6.2 Disaster Recovery Plan (DRP). Owners of Mission Critical Information Resources and of Information Resources containing Confidential Data must adopt a disaster recovery plan commensurate with the Risk and value of the Information Resource and Data. The disaster recovery plan must incorporate Procedures for:

(a) recovering Data and applications in the case of events that deny access to Information Resources for an extended period (e.g., natural disasters, terrorism, etc.);

(b) assigning operational responsibility for recovery tasks and communicating step-by-step implementation instructions;

(c) testing the disaster recovery plan and Procedures every two years at minimum (e.g., tabletop or scenario testing, leveraging major schedule upgrades, activating actual service outages in a controlled scenario, etc.); and

(d) making the disaster recovery plan available to the UTEP CISO and other stakeholders.

6.3 Revision History

First Draft: May 12, 2017 (complete rewrite based on new UTS165)
Approved: May 12, 2017
Gerard D. Cochrane Jr., Chief Information Security Officer