UTSA Institutional Compliance Office of Information Security

OIS 11 – Standard for Disaster Recovery

I. STANDARD STATEMENT

The goal of this standard is to provide for the restoration and recovery of critical systems and applications in the event of an emergency or declared disaster. As a companion to the university's business continuity and emergency preparedness program, the focus of these standards is on mitigation of risk in the area of computing and technology throughout the campus.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

The Office of Information Security

informationsecurity@utsa.edu

V. PROCEDURES

A. Campus units must ensure that critical data are backed up periodically and copies maintained in an off-site location. Campus units must develop and maintain written recovery procedures for natural and man-made disasters. These plans must be available to staff at all times.

B. The disaster recovery plan must involve the ongoing process of data classification to identify critical data, planning, developing and implementing disaster recovery management procedures to ensure efficient and effective resumption of critical functions in the event of an unscheduled interruption.

C. Data Owners must identify the Recovery Time Objective (the length of time by which the system must be returned to an acceptable level of service) and the Recovery Point Objective (the point in time to which processing has to be returned).

D. Disaster recovery plans will be tested annually or when new systems are installed. Model templates will be provided to aid in planning and documentation.

Title: OIS 11 – Standard for Disaster Recovery
Effective Date: January 1, 2014
Last Revised: August 5, 2020