Disaster Recovery (DR) Planning Standard Administrative Procedure

Introduction

Disaster recovery planning is a business requirement at Texas A&M University-Kingsville (TAMUK) to enable the recovery of systems in the event of disasters.

Purpose

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.

Audience

This procedure applies to all mission critical information resources and the individuals responsible for these critical systems.

DR Planning Procedure

1. Procedures

   1.1 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 from an interruption; identify recovery resources and a source for each; and contain step-by-step instructions for implementing the plan.

   1.2 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. The tests shall be documented and the results shall be used to update the plan if needed.

   1.3 Back-up/recovery media must be tested on a regular basis to ensure the validity of the recovery media and process.

Disciplinary Actions

Violation of this policy may result in disciplinary action up to and including termination for employees and temporaries; termination of contracts in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Texas A&M University-Kingsville Information Resources access privileges, civil, and criminal prosecution.

References

1. Copyright Act of 1976
2. Computer Fraud and Abuse Act of 1986
3. Computer Security Act of 1987
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
6. Foreign Corrupt Practices Act of 1977
7. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
8. IRM Act, 2054.075(b)
9. The State of Texas Information Act
10. The State of Texas Penal Code, Chapters 33 and 33A
11. Texas Administrative Code, Chapter 202
12. Texas A&M University-Kingsville Procedure 29.01.03.K1.010
13. Texas A&M University-Kingsville Procedure 29.01.04.K1.010
14. Texas Government Code, Section 441