Backup Procedure

Introduction
Electronic backups are a business requirement at Texas A&M University-Kingsville (TAMUK) to enable the recovery of systems in the event of disasters, system disk drive failures or system operations errors.

Purpose
The purpose of this procedure is to establish the rules for the backup and storage of electronic systems.

Audience
This procedure applies to individuals within TAMUK who are responsible for the installation and support of information resources, system administrators, individuals charged with information resource security, and data owners.

Backup Procedure
1. The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by an annual risk assessment.
2. The backup and recovery procedure for each system must be documented and periodically reviewed.
3. Critical system backups must be stored offsite:
   a. The vendor(s) providing offsite backup storage must be approved by the Information Security Officer (ISO).
   b. Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems.
   c. Signature cards held by the offsite backup storage vendor(s) for access to backup media must be reviewed annually or when an authorized individual leaves the university.
   d. Procedures between the offsite backup storage vendor(s) and the university must be reviewed periodically.
4. At the time of backup, all backup jobs should be set to verify the data that has been backed up.
5. Backups must be tested annually to ensure that they are recoverable.
6. Backup media must be clearly labeled to identify the information resource to which it belongs.
7. The use of personally owned external storage devices is not permitted.
8. Users are required to report to the ISO any condition that might result in the loss of backup data confidentiality, integrity or availability for any reason.

Disciplinary Actions
Violation of this procedure may result in disciplinary action up to and including termination for employees and temporaries; a termination of employment relations 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 TAMUK Information Resources access privileges, civil, and criminal prosecution.
References

1. Copyright Act of 1976
2. Computer Fraud and Abuse Act of 1986
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
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