Backup Policy

Introduction
Electronic backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, or system operations errors.

1. Purpose
   The purpose of the Texas A&M University-Kingsville Backup Policy is to establish the rules for the backup and storage of electronic information.

2. Audience
   The Texas A&M University-Kingsville Backup Policy applies to all individuals within the TAMUK enterprise that are responsible for the installation and support of Information Resources, individuals charged with Information Resources security and data owners.

3. Backup Policy
   3.1. The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.
   3.2. The Texas A&M University-Kingsville Information Resources backup and recovery process for each system must be documented and periodically reviewed.
   3.3. The vendor(s) providing offsite backup storage for Texas A&M University-Kingsville must be cleared to handle the highest level of information stored.
   3.4. Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally backup media must be protected in accordance with the highest sensitivity level of information stored.
   3.5. At the time of backup all backup jobs should be set to verify the data that has been backed up.
   3.6. Backups must be bi-annually tested to ensure that they are recoverable.
   3.7. Signature cards held by the offsite backup storage vendor(s) for access to Texas A&M University-Kingsville backup media must be reviewed annually or when an authorized individual leaves Texas A&M University-Kingsville.
   3.8. Procedures between Texas A&M University-Kingsville and the offsite backup storage vendor(s) must be reviewed at least annually.
   3.9. Backup tapes and other media such as optical disks and backup to disk data must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:
       3.9.1. System name
       3.9.2. Creation Date
       3.9.3. Sensitivity Classification [Based on applicable electronic record retention regulations].
       3.9.4. Name of data custodian
       3.9.5. Texas A&M University-Kingsville Contact Information
4. Users are required to report to the IRM any condition that might result in the loss of backup data integrity, confidentiality or availability for any reason.

5. Disciplinary Actions
   Violation of this policy 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 Texas A&M University-Kingsville Information Resources access privileges, civil, and criminal prosecution.