29.01.99.K1.040 Backup Standard Administrative Procedure

Effective: April 1, 2004
Revised: March 6, 2013
Revised: March 13, 2019
Next Scheduled Review: March 13, 2024

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 system administrators, individuals charged with information resource security, data owners, and individuals who are responsible for information resources.

Backup Procedure

1. The backup and recovery procedure must be documented and periodically reviewed.
2. Critical system backups must be stored offsite:
   a. The offsite backup storage location 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. Backup procedures must be reviewed periodically.
   c. Signature cards held by the offsite backup storage vendor(s) for access to backup media must be reviewed when an authorized individual leaves iTech.
3. At the time of backup, all backup jobs should be set to verify the data that has been backed up.

4. Backups must be tested annually to ensure that they are recoverable.
5. Backup media must be clearly labeled to identify the information resource to which it belongs.
6. The use of personally owned external storage devices is not permitted.
7. 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.
8. The frequency and extent of backups must be in accordance with the importance of the information. Replication may be used in place of backup or to augment backup.

Disciplinary Actions

Violation of this procedure may result in disciplinary action up to and including termination for employees and temporaries; a termination of contract relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of students. Additionally, individuals are subject to loss of TAMUK Information Resources access privileges, civil, and criminal prosecution.

References

1. DIR Practices for Protecting Information Resources Assets
2. The State of Texas Information Act
3. Texas Administrative Code, Chapter 202
4. Texas A&M University-Kingsville Acceptable Use Procedure 29.01.99.K1.010
5. System Regulation 29.01.03 Electronic Information Services Access and Security

Contact Office

For More Information, Contact: iTech
MSC 185, 700 University Blvd., Kingsville, TX 78363-8202
Contact Phone: 361-593-2404