

**29.01.99.K1.040**

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, Title 5, Part 1, Chapter 101, Section 101.001, Subsection (c)(2)