29.01.99.K1.210 Third Party Access Standard Administrative Procedure

Effective: April 1, 2004
Revised June 7, 2013
Revised: February 13, 2019
Next Scheduled Review: February 13, 2024

Introduction

Third parties may play an important role in the support of hardware and software management, and operations. Third parties may remotely view, copy and modify data, correct software and operating systems problems, and monitor and fine tune system performance. Setting limits and controls on what can be seen, copied, modified, and controlled by third parties will reduce the risk of loss of revenue, liability, loss of trust, and embarrassment to Texas A&M University-Kingsville (TAMUK).

Purpose

The purpose of this procedure is to establish the rules for third party access to the University Information Resources, third party responsibilities, and protection of University information.

Audience

This procedure applies to individuals that are responsible for the installation, operations and maintenance of information resources and who permit third party access for maintenance, monitoring and troubleshooting purposes.

Third Party Access Procedure

1. Third parties must comply with all iTech procedures, standards and agreements.
2. Third party agreements and contracts must specify that:
   a. University information must not be disclosed.
   b. Confidential or sensitive data needs to be encrypted and stored in the United States.

   c. Third Party will promptly notify TAMUK of any unauthorized release of proprietary information.
3. Non-Disclosure Agreement must be completed for all third party personnel who require access to information resources which contain confidential or sensitive data.
4. The third party must only use TAMUK information and information resources for the purpose of the business agreement.
5. Any other TAMUK information acquired by the third party in the course of the contract cannot be used for the third party's own purposes or divulged to others.
6. Third party contracts will specify a TAMUK point of contact for the third party. The TAMUK point of contact must request accounts for each third party member needing access. The point of contact will work with the third party to make certain the third party is in compliance with iTech procedures.
7. The TAMUK point of contact will notify iTech of changes in third party personnel assignments.
8. Third party employees with access to TAMUK sensitive or confidential information must be approved by the information owner.
9. Third party personnel must report all information security incidents directly to the Information Security Officer (ISO).
10. Third party access must be uniquely identifiable and password management must comply with the TAMUK Password Procedure 29.01.99.K1.120.
11. Upon departure of a third party employee from the contract, the third party will ensure that all sensitive or confidential information is returned to TAMUK or destroyed.
12. Upon termination of contract or at the request of TAMUK, the third party will return or destroy all TAMUK information and provide written certification of that return or destruction.
13. Upon termination of contract or at the request of TAMUK, the third party must surrender all TAMUK Identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the third party must be documented by authorized TAMUK management.
14. Third parties are required to comply with all state and TAMUK auditing requirements, including the auditing of the third party's work.
15. All software used by the third party in providing service to TAMUK must be properly licensed.
16. Violations of this procedure must be reported to the ISO.

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. 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 Acceptable Use Procedure 29.01.99.K1.010
14. Texas Government Code, Section 441

Contact Office

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