29.01.03.H0.24 Third Party Access

Approved: April 2014
Revised: January 5, 2024
Next Scheduled Review: January 2029

Procedure Summary

Third party entities play an important role in the support of hardware and software management, and operations for customers. They can remotely view, copy, and modify data and audit logs; they correct software and operating system problems, monitor and fine tune system performance, monitor hardware performance and errors, modify environmental systems, and reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by a third party will eliminate or reduce the risk of loss of revenue, liability, loss of trust and potential embarrassment to Texas A&M University-Texarkana (TAMUT).

This procedure applies to third party accessible University mission critical and confidential information. The purpose of this procedure is to provide a set of measures that will mitigate information security risks associated with third party access. This includes but is not limited to A/C, UPS, PDU, fire suppression, etc., and the third-party responsibilities and protection of TAMUT's information. This procedure also applies to all individuals who are responsible for the installation of new TAMUT Information Resources assets and who allow third party access for maintenance, monitoring and troubleshooting purposes of existing IR.

Definitions

Data Center: The facility used to house servers and network systems.

Information Resources (IR): Any computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, tablets, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), smartphones, telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it includes the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Security Officer (ISO): Person responsible to the executive management for administering the information security function within the University. The ISO is TAMUT'sinternal and external point of contact for all information security matters. **Third**

Party: An external entity that supplies goods or services including but not limited to vendors and other Universities members of the Texas A&M System.

Vendor: Someone who exchanges goods or services for money.

Procedures and Responsibilities

To ensure the security of our central data center, all third-party physical access must be approved and authorized by the Chief Information Officer (CIO) or Information Technology Advisory Council (ITAC). Logs will be maintained for all third-party access, and prior to accessing the TAMUT network, third-party vendors must sign a Guest Access Form and be escorted by the Office of Information Technology (OIT).

Access to the data center is restricted to key access only, and access control cards will not be issued to third-party vendors. It is important to note that third-party access is temporary and escorted to ensure the safety and security of our data center.

1. THIRD PARTY ACCESS

1.1 Third parties must comply with all applicable rules, policies and TAMUT standards and agreements, including, but not limited to:

1.1.1 Safety

1.1.2 Privacy

1.1.3 Security

1.1.4 Auditing

1.1.5 Software Licensing

1.1.6 Acceptable Use

1.2 Third party agreements and contracts must specify:

1.2.1 The TAMUT information a third party should have access to.

1.2.2 How TAMUT information is to be protected by the third party.

1.2.3 Acceptable methods for the return, destruction, or disposal of TAMUT information in the third party's possession at the end of the contract.

1.2.4 The third party must only use TAMUT information and Information Resources for the purpose of the business agreement.

1.2.5 Any other TAMUT 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.

1.3 TAMUT will provide an Information Technology IT point of contact for the third party. The point of contact will work with the third party to make certainthat they are in compliance with these rules.

1.4 Each third-party employee with access to TAMUT sensitive information must be cleared to handle that information.

1.5 Third party personnel must report all security incidents directly to TAMUT's ISO at itsecurity@TAMUT.edu.

1.6 If third party management is involved in TAMUT security incident management, the responsibilities and details must be specified in the contract.

1.7 The third party must follow all applicable TAMUT change control processes and procedures.

1.8 Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by the corresponding department head.

1.9 All third-party maintenance equipment on the TAMUT network that connects to the outside world via the network, telephone line, or leased line, and all TAMUT Information Resources third party accounts, will remain disabled except when in use for authorized maintenance.

1.10 Third party access must be uniquely identifiable, and password management must comply with University Procedure 29.01.03.H0.11 *Identification and Authentication* andUniversity Procedure 29.01.03.H0.03 *Administrative/Special Access*. Third party's major work activities must be entered into a log and made available to TAMUT management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.

1.11 Upon termination of a contract or at the request of TAMUT, the third party will return or destroy all TAMUT information and provide written certification of that return or destruction within 24 hours.

1.12 Upon termination of a contract or at the request of TAMUT, the third party must surrender all equipment and supplies immediately. Equipment and/or supplies to be retained by the third party must be documented by the Associate VP for Information Technology/CIO.

1.13 Third parties are required to comply with all State and TAMUT auditing requirements, including the auditing of the third party's work.

2. DISCIPLINARY ACTIONS

Violation of this Procedure may result in disciplinary action which may include termination

for employees, termination of business relationships for contractors or consultants, dismissal forinterns and volunteers, or suspension or expulsion for students. Additionally, individuals aresubject to loss of TAMUT Information Resources access privileges and civil and criminal prosecution.

Related Statutes, Policies, or Requirements

Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C, Rule § 202.75, Information Resources Security Safeguards

University Procedure 29.01.03.H0.11 *Identification and Authentication*

University Procedure 29.01.03.H0.03 *Administrative/Special Access*.

Contact Office

Office of Information Technology

903-223-3084