TEXAS A&M **INTERNATIONAL** UNIVERSITY

Standard Administrative Procedure (SAP)

29.01.99.L1.22 Third Party Access

First Approved: March 28, 2013
Revised: June 22, 2017
Next Scheduled Review: June 22, 2022

Procedure Statement and Reason for Procedure

Third party entities assume a large role in the complexity of information resource management. Setting limits and controls on monitoring, copying, and modifications by a third party will reduce the risk of liability, loss of trust, loss of revenue, and prevent reputational harm to Texas A&M International University (TAMIU).

This SAP applies to third party access and responsibilities when accessing TAMIU's Information Resources. The purpose of this SAP 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 TAMIU's information.

This SAP will also apply to individuals who install new assets for TAMIU's Information Resources and to those who allow third party access for the maintenance, monitoring, and troubleshooting of existing Information Resources. This SAP supplements *TAMIU Rule 29.01.99.L1, Use of Information Resources and Facilities* and *TAMIU Rule 24.99.01.L1, Security of Electronic Information Resources*.

Procedures and Responsibilities

---

1. Third Party Access

   Third party physical or logical access to TAMIU's Information Resources will require the appropriate approval and authorization by the Associate Vice President of IT/CIO or Information Security Officer (ISO).

1.1 Third parties must comply with all applicable TAMIU rules, policies, 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 What TAMIU information the third party may access.
1.2.2 How TAMIU information will be protected by the third party according to classification and risk.
1.2.3 Acceptable methods for the return, destruction, or disposal of TAMIU information in the third party's possession upon termination of the agreement or contract.
1.2.4 That the third party must only use TAMIU information and Information Resources in accordance with the business agreement or contract.
1.2.5 That any other TAMIU information acquired by the third party throughout the course of the contract cannot be used for the third party's own purposes or disclosed to others without written consent.
1.2.6 That the third party agrees to comply with the State of Texas Security Control Standards Catalog, SA-9.
1.2.7 That the third party must provide information for appropriate security analysis.

1.3 TAMIU will provide for the third party an Office of Information Technology (OIT) representative to assist with regulatory requirements.

1.4 Based on risk, each third-party employee with access to TAMIU confidential or sensitive information must have completed applicable training and background checks.

1.5 Third party personnel must report all security incidents directly to TAMIU's Information Security Officer (ISO) at itsecurity@tamiu.edu.

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

1.7 The third party must follow or have in place processes and procedures similar to applicable TAMIU change control processes and procedures.

1.8 Regular work hours and duties will be defined in the contract, statement of work, or written agreement. Work outside of defined parameters must be approved in writing by the corresponding department head or appropriate VP.

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

1.10 Third party access must be uniquely identifiable and password management must comply with *TAMIU SAP's 29.01.99.L1.13, Password Management* and *29.01.99.L1.03, Administrative/Special Access* unless an exemption is documented. Third parties' major work activities must be made available to TAMIU management upon request.

1.11 Upon termination of a contract or at the request of TAMIU, the third party will return or destroy all TAMIU information and provide written certification of that return or destruction within 96 hours or by terms outlined in the third party contract.

1.12 Upon termination of a contract or at the request of TAMIU, the third party must surrender all equipment, keys, access cards, and supplies immediately.

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

Related Statutes, Policies, Regulations, or Rules

Texas Administrative Code 202, Subchapter C – Information Security Standards for Institutions of Higher Education
TAMIU Rule 24.99.01.L1, Security of Electronic Information Resources
TAMIU Rule 29.01.99.L1, Use of Information Resources and Facilities

Appendix

References:
Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications

Contact Office

Office of Information Technology, 956-326-2310