SAP 29.01.03.T0.16 Information Technology Services – Vendor Access

Approved: May 4, 2006
Revised: February 28, 2012
Revised May 21, 2014
Next Scheduled Review: May 21, 2019

Procedure Statement

Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors may have the capability to remotely view, copy, and modify data and audit logs. They might remotely correct software and operating systems 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 vendors will eliminate or reduce the risk of liability, embarrassment, and loss of revenue and/or loss of trust to the university.

Reason for Procedure

This Standard Administrative Procedure (SAP) applies to vendor-accessible Tarleton State University mission critical and confidential information.

The purpose of the implementation of this SAP is to provide a set of measures that will mitigate information security risks associated with vendor access. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this SAP based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated information security officer (ISO).

The procedures described in this SAP apply to all departments, administrators, and vendors who are responsible for vendor supplied information resources.

Procedures and Responsibilities

1. Personnel who provide vendors' access to university mission critical or confidential information resources shall obtain formal acknowledgement from the vendor of their responsibility to comply with all applicable university policies, rules, standards, practices and agreements, including but not limited to: safety policies, privacy policies, security policies, auditing policies, software licensing policies, acceptable use policies, and nondisclosure as required by the providing entity.

2. Tarleton employees who are procuring the services of vendors who are given access to mission critical and/or confidential information are expected to define the following with the vendor:

    2.1 The university information to which the vendor should have access;

    2.2 How university information is to be protected by the vendor;

    2.3 Acceptable methods for the return, destruction, or disposal of university information in the vendor's possession at the end of the contract;

    2.4 That use of Tarleton information and information resources are only for the purpose of the business agreement; any other university information acquired by the vendor in the course of the contract cannot be used for the vendors' own purposes or divulged to others; and,

    2.5 Vendors shall comply with terms of applicable non-disclosure agreements.

3. Tarleton shall provide an information resources point of contact for the vendor. The point of contact will work with the vendor to make certain the vendor complies with university policies.

4. The resource owner shall specify appropriate access authorization for each on-site vendor employee (i.e., university affiliate) according to the criticality of the information resource.

5. Vendor personnel shall report all security incidents directly to appropriate university personnel.

6. The responsibilities and details of any vendor management involvement in university security incident management shall be specified in the contract.

7. The vendor must follow all applicable university change control processes and procedures. Regular work hours and duties shall be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate university management.

8. Except for very limited exceptions, all vendors must use VPN to access or support Tarleton State University's network infrastructure.

Related Statutes, Policies, or Requirements

Supplements *SAP 29.01.03.T0.19 Security of Electronic Information Resources*

Definitions

1. **Confidential Information**: information that is excepted from disclosure requirements under the provisions of applicable state or federal law (e.g., the Texas Public Information Act).

2. **Information Resources (IR)**: the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.
3. **Information Security Officer (ISO):** responsible for administering the information security functions within Tarleton and reports to the information resources manager (IRM).

4. **Mission Critical Information**: information that is defined by the university or information resource owner to be essential to the continued performance of the mission of the university or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the university or department.

Contact Office

Information Technology Services
Executive Director and CIO of Information Technology Services
254.968.9395