

Procedure 29.01.03.T1.16 (Effective 5/4/2006)
(Supplements [Rule 29.01.03.T1](#))

Information Resources – Vendor Access

1. GENERAL

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.

2. APPLICABILITY

This Standard Administrative Procedure (SAP) applies to vendor-accessible 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 herein apply to all departments, administrators, and vendors who are responsible for vendor supplied information resources.

3. DEFINITIONS

3.1 **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.

3.2 **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.

3.3 **Information Security Officer (ISO):** responsible for administering the information security functions within Tarleton State University and reports to the Information Resources Manager (IRM).

3.3 **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.

4. PROCEDURES

4.1 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.

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

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

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

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

4.2.4 That use of Tarleton State University 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,

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

4.3 Tarleton State University 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 is in compliance with university policies.

4.4 Appropriate access authorization for each on-site vendor employee (i.e., university affiliate) shall be specified by the resource owner according to the criticality of the information resource.

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

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

4.7 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.

OFFICE OF RESPONSIBILITY: Department of Information Resources

CONTACT: Executive Director of Information Resources