# The Division of Information Technology
# University Information Security Standards

**Information Security Standard – Third Party Access (Legacy TAC 202)**
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

## 1. General

Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors might 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 information security standard applies to vendor-accessible university mission critical and confidential information.

The purpose of this information security standard 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 department heads or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures is to be determined by the department heads and their identified information security administrators. 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 is based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

The West Texas A&M University Vendor Access Policy applies to all individuals that are responsible for the installation of new Information Resources assets, and the operations and maintenance of existing Information Resources and who do or may allow vendor access for maintenance, monitoring and troubleshooting purposes.

## 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: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, 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, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is 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.

3.3 Information Resources Manager (IRM): Responsible to the State of Texas for management of the agency/university's information resources. The designation of an agency/university information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the agency. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

3.4 Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the agency. The ISO is the university's internal and external point of contact for all information security matters.

3.5 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.

3.4 Vendor: Someone who exchanges goods and services for money.

## 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 West Texas A&M 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: (1) The university information to which the vendor should have access; (2) How university information is to be protected by the vendor; (3) Acceptable methods for the return, destruction, or disposal of university information in the vendor's possession at the end of the contract; (4) That use of West Texas A&M 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, (5) Vendors shall comply with terms of applicable non-disclosure agreements.

4.3 West Texas A&M 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:** Information Technology

**CONTACT:** Chief Information Officer