Procedure Statement

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.

Reason for Procedure

This procedure applies to any university owned or operated information resource being accessed or managed by any vendor. This procedure supplements Texas A&M System Regulation 29.01.03 Electronic Information Services Access and Security.

The purpose of this procedure 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 or division heads will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are 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 in this PROCEDURE based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and reviewed by the University Information Security Officer (ISO) and the University Information Resource Manager (IRM).

The procedure applies to all departments, administrators, and vendors who 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, operations, monitoring and troubleshooting purposes.

These procedures apply to remote vendor access to systems, applications, or storage media containing university sensitive information over any type of medium.
procedures also apply to direct vendor access to systems, applications, or storage media containing university sensitive information whether located on information resources owned and operated by the university or the vendor.

---

**Responsibilities**

1. The information resource owners must be informed of and may deny any vendor access to information resources containing sensitive information before vendor access is granted. Requests may require a risk assessment dependent upon the system and nature of the request. Any necessary risk assessments are to be performed by the ISO or designee.

2. 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, procedures and agreements, including but not limited to: safety, privacy, security, auditing, software licensing, acceptable use, and nondisclosure as required by the providing entity.

3. University employees who are procuring the services of vendors who are given access to mission critical and/or confidential information resources are expected to define the following with the vendor:
   
   3.1. The university information to which the vendor should have access;
   
   3.2. How university information is to be protected by the vendor;
   
   3.3. Acceptable methods for the return, destruction, or disposal of university information in the vendor's possession at the end of the contract;
   
   3.4. That use of 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;
   
   3.5. Vendors shall comply with terms of applicable non-disclosure agreements.
   
   3.6. Ownership of any upgrades, modifications, patches, downloads, websites, website information, operating systems, source code and data.

4. The 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 and procedures.

5. Each vendor shall provide the information resources point of contact and notify the University of all employees assigned to university contracts. This information may be provided through an initial list of assigned employees and/or electronic communications to the University of any and all access changes. Vendors are to
provide the University point of contact this information within 24 hours of staff changes.

6. Appropriate access authorization for each on-site vendor’s employee shall be specified by the resource owner according to the criticality of the information resource. Where applicable, the university-issued identification or access privileges may be required and all requirements associated with issue and return of the identification must be followed.

7. Vendor personnel shall report all security incidents directly to appropriate university personnel that will, in return, follow the applicable University procedures regarding Incident Response.

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

9. 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.

10. Upon termination of contract or at the request of the university, the vendor shall return or destroy all university information and provide written certification of that return or destruction within 24 hours. Destruction of university information shall follow the guidelines set forth by the Texas Administrative Code Rule 202.78 Removal of Data from Data Processing Equipment.

11. Upon termination of contract or at the request of the university, the vendor must immediately surrender all university identification badges, access cards, keys, software, equipment, supplies and all university owned information as defined in section 3.6. Equipment and/or supplies to be retained by the vendor must be documented by the providing entity.

12. CONSEQUENCES FOR VIOLATIONS

12.1 All university employees as well as contractors, consultants, and vendors required to adhere to this university procedure may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and university rules.

12.2 Individuals found in violation of this university procedure are subject to loss of access privileges to university information resources. In addition, contracts associated with contractors, consultants, or vendors are subject to review and possible termination. Any device, system, or software found in violation of this procedure may be confiscated and temporarily stored by the IRM or a representative.
Definitions

Confidential Information - Information that is excluded from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.

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.

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.

Information Security Officer (ISO) - Responsible to the executive management for administering the information security functions within the agency. The University ISO is the university’s internal and external point of contact for all information security matters.

Information Resource Owner – an entity responsible for:
- A business function; and,
- Determining controls and access to information resources supporting that business function.

Vendor – Someone who exchanges goods and services for money.

Information Resources Manager (IRM) - Responsible to the State of Texas for management of the agency/university’s information resources.

Related Rules

- System Policy 29.01 Information Resources
- System Regulation 29.01.03 Security of Electronic Information
- Texas Administrative Code (TAC) 202 as amended or supplemented

Contact Office

Information Technology Services – (210) 784-4357 (HELP)