Texas A&M University System Standard – Vendor Access

Standard Statement

The purpose of the implementation of this standard is to provide a set of measures that will mitigate information security risks associated with vendor access.

Reason for standard

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 System Office.

Definitions

Confidential - Information that must be protected from unauthorized disclosure or public release based on state or federal law, (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements). Please refer to System Regulation 29.01.03 and the related Data Classification standard for more information.

Examples of "Confidential" data may include but are not limited to the following:

- Personally Identifiable Information, such as: a name in combination with Social Security Number (SSN) and/or financial account numbers
- Student Education Records
- Intellectual Property, such as: certain intellectual property as set forth in section 51.914 of the Texas Education Code
- Medical Records

Information Resources - 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 System Office or Information Resource owner, or designee, to be essential to the continued performance of the mission of the

System Office 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 System Office or department.

Information Resource Owner - an entity responsible for:

- A business function; and,
- Determining controls and access to information resources supporting that business function.

Applicability

This standard applies to vendor-accessible Mission Critical and Confidential Information.

The purpose of the implementation of this 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 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 designee.

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this standard are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this standard. All exclusions must be in accordance with standard *Exclusions from Required Risk Mitigation Measures*.

The steps described herein apply to all departments, administrators, and vendors who are responsible for vendor supplied Information Resources.

Standards

1. Information Resource owners, or designees, who provide vendors with access to 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. This formal

acknowledgement requirement shall be incorporated into any applicable vendor contract and such contract must include all terms under Sections 3.1 through 3.5 below.

2. Access to Mission Critical and/or Confidential Information shall not be given to anyone without the Information Resource owner's, or designee's, explicit authorization. Documentation of the access authorization shall be maintained by the Information Resource owner, or designee.

3. To assure compliance with section 1 above, Information Resource owners, or designees, entering into a contract for services with a vendor must supply a written memo to the Office of General Counseling at the time the contract is submitted for review indicating that the vendor will have access to Mission Critical or Confidential Information. Vendors who are given access to Mission Critical and/or Confidential Information shall have contracts that specify:

   3.1 The System Office information to which the vendor should have access;

   3.2 How Mission Critical and/or Confidential Information is to be protected by the vendor;

   3.3 Acceptable methods for the return, destruction, or disposal of Mission Critical and/or Confidential Information in the vendor's possession at the end of the contract;

   3.4 That use of Mission Critical and/or Confidential Information and Information Resources are only for the purpose of the business agreement; any other System Office information acquired by the vendor in the course of the contract cannot be used for the vendors' own purposes or divulged to others; and,

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

4. Information Resource owners, or designees, shall provide an Information Resources point of contact to the vendor. The point of contact will work with the vendor to make certain the vendor is in compliance with System Office policies. The identity of the Information Resources point of contact shall also be identified in the contract (described in 3) with the vendor.

5. Each vendor must provide the point of contact (established in 4) with a list of all employees assigned to University contracts. The list shall be updated and provided to the point of contact within 24 hours of staff changes. The list shall also be provided in the contract

(described in 3) with any updates provided to the Office of General Counseling by the Information Resources point of contact.

6. Appropriate access authorization for each on-site vendor employee (i.e., System Office affiliate) shall be specified by the Information Resource owner, or designee, according to the criticality of the Information Resource. Where applicable, departmentally-issued identification may be required as cited in University Rule 33.99.12.M1, Employee Identification Cards.

7. Vendor personnel shall report all security incidents directly to System Office personnel specified by the Information Resource owner, or designee.

8. If vendor management is involved in System Office security incident management, the responsibilities and details must 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 the Information Resource owner, or designee, and if necessary to modify the scope of work in the vendors' agreement with the System Office, the Information Resource owner, or designee, will coordinate review of the formal modification/amendment through the Office of General Counseling.

Related Statutes, Policies, or Requirements

Regulation 29.01.03 and related standards

Contact Office

For standard clarification or interpretation, contact Texas A&M University System Chief Information Officer.

OFFICE OF RESPONSIBILITY: Texas A&M University System Chief Information Officer