PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.14 Information Resources – Vendor Access
Approved May 26, 2009
Revised November 4, 2014
Revised August 14, 2017
Revised January 19, 2023
Next Scheduled Review: January 1, 2028

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to establish the process for vendor access, responsibilities, and protection of Prairie View A&M University (PVAMU) information resources. In addition, the performance of these procedures is necessary to ensure compliance with the Texas Administrative Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education.

Definitions

Confidential Information - information that is confidential pursuant to state or federal law. Such information may also be subject to state or federal breach notification requirements. See the Texas A&M University System Data Classification Standard for additional information.

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.

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

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.

Official Procedures and Responsibilities

1. GENERAL

1.1 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.

1.2 In accordance with Texas Administrative Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this UAP 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).

2. APPLICABILITY

2.1 This UAP applies to vendor-accessible PVAMU mission critical and confidential information. The intended audience for this UAP includes, but is not limited to, all departments, administrators, and vendors who are responsible for vendor supplied information resources.

3. PROCEDURES

3.1 Personnel who provide vendors access to PVAMU mission critical or confidential information resources must notify the ISO and must obtain formal acknowledgement from the vendor of their responsibility to comply with all applicable university policies, rules, procedures, 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.

3.2 Prairie View A&M university 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:

3.2.1 The PVAMU information to which the vendor should have access;

3.2.2 How PVAMU information is to be protected by the vendor;

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

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

3.2.5 Terms of applicable non-disclosure agreements.

3.3 Prairie View 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 PVAMU policies.

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

3.5 Vendor personnel shall report all security incidents directly to the appropriate PVAMU personnel, including the ISO.

3.6 Information Technology contracts and agreements must address security, backup, and privacy requirements. The contracts and agreements should include right-to-audit, and other provisions, to provide appropriate assurances that applications and information will be adequately protected. Vendors and third parties must adhere to all state and federal laws, and System policies and regulations pertaining to the protection of information resources and privacy of sensitive information. The ISO must review new or renewing contracts that contain technology.

3.7 The university's point of contact must follow all applicable PVAMU change control processes and procedures for any changes done by the vendor.

3.8 In accordance with Texas Government Code 2054.519 State Certified Cybersecurity Training Programs, all vendors and contractors with access to university systems must complete Texas Department of Information Resources approved cybersecurity training programs (Statewide Cybersecurity Awareness Training).

Related Statutes, Policies, Regulations and Rules

Tex. Admin. Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education

System Policy 29.01 Information Resources

System Regulation 29.01.03 Information Security

The Texas A&M University System Information Security Standards

Security Control Standards Catalog

Statewide Cybersecurity Awareness Training

Contact Office

Center for Information Technology Excellence 936-261-9350
