PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.23 Information Resources – Application Security
Approved September 26, 2013
Revised December 7, 2018
Next Scheduled Review: December 2023

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to ensure computer applications written to support Prairie View A&M University (PVAMU) are developed using secure coding practices and follow an accepted application programming standard. Secure application coding practices are intended to reduce or eliminate the vulnerabilities and exploits with limited impact to the business. 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

Computer Applications – a subclass of computer software that employs the capabilities of a computer directly and thoroughly to a task that the user wishes to perform. This should be contrasted with system software, which is involved in integrating a computer's various capabilities, but typically does not directly apply them in the performance of tasks that benefit the user. In this context, the term application refers to both the application software and its implementation.

Secure Coding Practices – program source codes that are written to withstand attacks. The amount of effort that goes into writing a secure program is substantially greater than writing code without such concern. Normally, programmers deal with a solution to a data processing or transmission task without worrying about every line of code being a potential attack vector.

Data Source – a logical location where data is stored for a computer application. Typically refers to a database, but can also be a collection of files within a directory. Its purpose is to store and exchange information with the front-end of a computer application.

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.

Information Resource Owner – an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

Official Procedures and Responsibilities

1. GENERAL

1.1 There may be additional measures that department heads or deans will implement 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 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 all PVAMU information resources that store or process mission critical and/or confidential information. The intended audience for this UAP includes, but is not limited to, all university faculty, staff, student employees, contractors, and vendors developing or administering applications designed to handle or manage University data.

3. PROCEDURES AND RESPONSIBILITIES

3.1 Computer applications should follow a standardized application lifecycle. At a minimum, this should include requirement gathering, development, testing, and production maintenance phases. Updates, patches, and feature changes should follow the same phases and processes as if the application were being developed from concept.

3.2 Each individual user (whether a developer, administrator, or user) should have a unique set of credentials for accessing a computer application. Each process or application role should also have a unique credential that is not coincident with a user.

3.3 Only authenticated users should have access to a computer application. Each user should only be allowed to access the information they require. The application's data owner should approve establishing and changing access for a user or group.

3.4 Developers should follow best practices for creating secure applications with the intention being to minimize the impact of attacks to a computer application. A code validation process should be followed to discover and remediate any code errors before an application is approved for production.

3.5 The production data source should not be used to develop or test an application. Development and testing databases will be redacted if copied from production data sources. Production data sources will be stored in an encrypted format. Data in transit to and from the application will also be encrypted. A separate data source will be created for each application.

3.6 Web-based computer applications shall be hosted on secure, robust servers with multi-layered security. Application and web services error messages should be anonymized or altered to prevent exposure of coding errors, directory structure, or other information about the application or server.

3.7 Logs for the server, application, and web services should be collected and maintained as per the Record's Retention Schedule.

4. NON-COMPLIANCE AND EXCEPTIONS

4.1 If it is suspected that this UAP is not being followed, report the incident to the Information Security Officer (ISO).

4.2 Any exceptions to this UAP must be approved in writing and shall be maintained by the ISO as per the Record's Retention Schedule.

Related Statutes, Policies, Regulations and Rules

System Policy 29.01 Information Resources

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

---

Contact Office

Office of Information Resources Management	936-261-9350
