**PRAIRIE VIEW A&M UNIVERSITY**
**UNIVERSITY ADMINISTRATIVE PROCEDURE**

# 29.01.03.P0.04 Information Resources – Intrusion Detection

Approved May 26, 2009
Revised March 5, 2014
Revised August 14, 2017
Reviewed December 22, 2022
Next Scheduled Review: December 1, 2027

## UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to provide a set of measures that will mitigate information security risks associated with intrusion detection. 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.

**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)** – 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 Intrusion detection plays an important role in implementing and enforcing an organizational security policy that is capable of preserving the integrity, availability, and confidentiality of data and information resources within the Prairie View A&M University (PVAMU) network. As information systems grow in complexity, effective security systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed and decentralized systems and network topology, some type of assurance is required so that the systems and network are secure. Intrusion detection capabilities can provide part of that assurance through detection of and altering to anomalous system and network activity so that incident management procedures can be initiated in an efficient and effective manner.

1.2 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 university information resources that store, process, or transmit mission critical and/or confidential information. The intended audience for this UAP includes, but is not limited to, all information resources management personnel, owners, system administrators, and users of university information resources.

## 3. PROCEDURES

3.1 Prevention and Detection

3.1.1 Operating system, user accounting, and application software audit logging processes shall be enabled on all host and server systems where resources permit.

3.1.2 The Security Operations Center, as described in System Regulation 29.01.03 Information Security, performs monitoring and alerting of security events and incidents.

3.1.3 Alarm and alert functions as well as audit logging of any firewalls and other network perimeter access control systems shall be enabled.

3.1.4 System administrators shall monitor/review audit logs from the network perimeter access control systems as risk management decisions warrant.

3.1.5 Audit logs for servers and hosts on the internal, protected network shall be reviewed periodically by the system administrator.

3.1.6 Reports shall be reviewed for indications of intrusive activity.

3.1.7 All suspected and/or confirmed instances of successful intrusions shall be immediately reported according to UAP 29.01.03.P0.18 Information Resources – Incident Management.

3.1.7.1 Information resource users are encouraged to report any anomalies in system performance and/or signs of unusual behavior or activity to their departmental system administrator or the Information Resources Help Desk.

3.1.8 System administrators shall keep abreast of industry best practices regarding current intrusion events and methods to detect intrusions. Intrusion detection methods shall be utilized as needed.

3.1.9 All confirmed instances of successful intrusions shall be reported monthly to the Department of Information Resources (DIR) via the Security Incident Reporting System (SIRS) by the ISO.

3.2 Response and Recovery

3.2.1 Based on the assessment of risk, appropriate action should be taken to protect PVAMU information resources.

## 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

## Contact Office

Center for Information Technology Excellence 936-261-9350