PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.18 Information Resources - Incident Management

Approved May 26, 2009
Revised November 4, 2014
December 5, 2019
Next Scheduled Review: December 2024

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to describe the requirements for dealing with computer security incidents. 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

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.

Security Incident Reporting (SIRS) - an electronic system for reporting (after the fact, after-action) incidents in compliance with Texas Department of Information Resources (DIR) regulations.

Security Incident - A security incident is a computer, network, or paper based activity which results (or may result) in misuse, damage, denial of service, compromise of integrity, or loss of confidentiality of a network, computer, application, or data; and threats, misrepresentations of identity, or harassment of or by individuals using these resources.

Official Procedures and Responsibilities

1. GENERAL

1.1 Security incidents include, but are not restricted to: malicious code detection; unauthorized use of computer accounts and computer systems; theft of computer equipment or theft of information; accidental or malicious disruption or denial of service as outlined in security monitoring procedures, intrusion detection procedures, internet/intranet procedures, and acceptable use procedures.

1.2 The purpose of the implementation of this UAP is to provide a set of measures that will mitigate information security risks associated with incident management. 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 ISO.

2. APPLICABILITY

2.1 This UAP applies to all Prairie View A&M University (PVAMU) information resources. The intended audience for this UAP includes, but is not limited to, all system administrators, directors, and department heads.

3. PROCEDURES

3.1 PVAMU system administrators have information security roles and responsibilities which can take priority over normal duties.

3.2 System administrators are responsible for notifying the ISO, their directors or department heads and initiating the appropriate action including restoration.

3.3 Departmental system administrators are responsible for determining the physical and electronic evidence to be gathered as part of the incident investigation such as initiating, completing, and documenting the incident investigation.

3.4 If fraud or theft is suspected as part of security incident detection, the person detecting the incident shall follow the procedures outlined in System Policy 10.02 Fraud, Waste and Abuse.

3.5 All security incidents must be reported to the ISO using the Security Incident Reporting Form.

3.6 System administrators shall file an after-action incident report to the ISO.

3.7 The ISO will be the responsible party to report the incident in the monthly DIR SIRS report.

3.8 The ISO will maintain an incident response plan in accordance with the Texas A&M University System Incident Management Standard.

Related Statutes, Policies, Regulations and Rules

System Policy 29.01 Information Resources

System Regulation 29.01.03 Information Security

Texas Administrative Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education

Contact Office

Office of Information Resources Management	936-261-9350