

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

**29.01.03.P0.18 Information Resources – Incident Management**

Approved (May 26, 2009)

Next Scheduled Review (May-2012)

**1. PURPOSE**

- 1.1 This procedure describes the requirements for dealing with computer security incidents. 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 This University Administrative Procedure (UAP) applies to all PVAMU information resources. 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 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 their designee.

The intended audience is system administrators, Directors, and Department Heads.

**2 DEFINITIONS**

- 2.1 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.
- 2.2 SIRS – Security Incident Reporting - an electronic system for reporting (after the fact, after-action) incidents in compliance with Texas Department of Information Resources (DIR) regulations.

**3 PROCEDURES AND RESPONSIBILITIES**

- 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 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 The system administrators shall report the security incidents that may involve criminal activity under Texas Penal Code Chapters 33 (Computer Crimes) or 33A (Telecommunications Crimes) to the Director or Department Head and the Information Security Officer see TAC 202.76 (c) for reporting requirements (as of 05/06/05).

- 3.5 If fraud or theft is suspected as part of security incident detection, the person detecting the incident shall follow System Policy 21.04, Control of Fraud and Fraudulent Actions.
- 3.6 If there is a substantial likelihood that security incidents could be propagated to other systems beyond departmental control, system administrators shall report such incidents to: IT HelpDesk, (936) 261-2525, if action is urgently needed or via email to [rvmooore@pvamu.edu](mailto:rvmooore@pvamu.edu) and [lamorgan@pvamu.edu](mailto:lamorgan@pvamu.edu) as soon as an incident is identified.
- 3.7 System administrators shall file an after-action incident report to the Information Security Officer.
- 3.8 The Information Security officer will be the responsible party to report the incident in the monthly DIR SIRS report.

**Contact Office:** Information Security Officer; 936-261-2126