

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

29.01.06.P1.01 Information Resources – Administrator/Special Access

Approved: (May 26, 2009)

Next Scheduled Review: (May-2012)

1. PURPOSE

- 1.1 Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Prairie View A&M University has developed rules and procedures that administrator's special access to information resources. The purpose of this University Administrative Procedure (UAP) is to identify those relevant policies and procedures.

This UAP applies to all University information resources.

The purpose of the implementation of this UAP is also to provide a set of measures that will mitigate information security risks associated with acceptable use of University information resources. 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 will be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, 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 information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer.

- 1.2 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.

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 Information Security Officer (ISO): responsible for administering the information security functions within Prairie View A&M University and reports to the Information Resources Manager (IRM).
- 2.3 Descriptive data (e.g., logs): Information created by a computer system or information resource that is electronically captured and which relates to the operation of the system and/or movement of files, regardless of format, across or between a computer system or systems. Examples of captured information are dates, times, file size, and locations sent to and from.
- 2.4 User data: User-generated electronic forms of information that may be found in the content of a message, document, file, or other form of electronically stored or transmitted information.

3. PROCEDURES AND RESPONSIBILITIES

- 3.1 Prairie View A&M University departments shall maintain a list or lists of personnel who have administrator, or special access accounts for departmental information resources systems. The list(s) shall be reviewed at least annually by the appropriate department head, director, or their designee.

PRAIRIE VIEW A&M UNIVERSITY
Administrative Procedures Manual

- 3.2 All users of Administrator and Special Access accounts must have account management instructions, training and authorization.
- 3.3 Each individual that uses Administrator and Special Access accounts must do investigations only under the direction of the ISO.
- 3.4 Each individual that uses Administrator and Special Access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- 3.5 Each account used for Administrator and Special Access must meet the Prairie View A&M University Standard Administrator Procedure Password Authentication.
- 3.6 The password for a shared Administrator and Special Access account must change when an individual with the password leaves the department or Prairie View A&M University or upon a change in the vendor personnel assigned to the Prairie View A&M University contract.
- 3.7 In the case where a system has only one administrator there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
- 3.8 When Special Access accounts are needed for internal or external audit, software development, software installation, or other defined need, they:
 - 1. must be authorized,
 - 2. must be created with a specific expiration date, and
 - 3. must be removed when work is complete

Contact Office: Information Security Officer; 936/261-9351

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

29.06.01.P1.02 Information Resources – Backup Recovery

Approved: (May 26, 2009)

Next scheduled review: (May–2012)

1. PURPOSE

- 1.1 Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Prairie View A&M University has developed rules and procedures that address acceptable use of information resources. The purpose of this University Administrative Procedure (UAP) is to identify those relevant policies and procedures.

This UAP applies to all University 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 acceptable use of University information resources. 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 will be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this SAP based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer.

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.

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 Information Security Officer (ISO): responsible for administering the information security functions within Prairie View A&M University and reports to the Information Resources Manager (IRM).
- 2.3 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, and failure to comply with regulations or legal obligations, or closure of the University or department.

3. PROCEDURES AND RESPONSIBILITIES

- 3.1 The frequency and extent of backups shall be determined by the importance of the information, potential impact of data loss/corruption, and risk management decisions by the data owner (Department Heads and Information Security Administrators).
- 3.2 Mission critical information backup and recovery processes for each system, including those for offsite storage, shall be documented and reviewed periodically.

PRAIRIE VIEW A&M UNIVERSITY
Administrative Procedures Manual

- 3.3 Physical access controls implemented at offsite backup storage locations.
- 3.4 Processes must be in place to verify that the actual offsite storage of mission critical data is taking place.
- 3.5 Backups shall be periodically tested to ensure that they are recoverable.

Contact Office: Information Security Officer; 936/261-9351

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

29.01.06.P1.03 Information Resources – Email Usage

Approved: (May 26, 2009)

Next Scheduled Review: (May-2012)

1. PURPOSE

- 1.1. This UAP provides procedures regarding the use of email through University owned 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 email use. 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. In accordance with Texas Administrative Code 202 - Information Security Standards, 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 information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer (ISO).

- 1.2. The intended audience of this UAP is any University employee, student, guest, or visitor that may use any University information resource that has the capacity to send, receive or store email.

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. Confidential Information - Information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.
- 2.3. Sensitive Personal Information – An individual's first name or first initial and last name in combination with any one or more of the following items:
- Social Security Number;
 - Driver's license number or government-issued identification number (including UIN or Student ID)
 - Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account

3. PROCEDURES AND RESPONSIBILITIES

Prohibited Use:

- 3.1. The PVAMU email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any PVAMU employee should report the matter to their supervisor immediately.

Individuals must not send, forward or receive confidential or sensitive Prairie View A&M University information through non-Prairie View A&M University email accounts. Examples of non-Prairie View A&M University email accounts include, but are not limited to: Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).

PRAIRIE VIEW A&M UNIVERSITY
Administrative Procedures Manual

No sensitive and/or confidential Prairie View A&M University material should be transmitted via PVAMU email unless encrypted.

- 3.2. Personal Use. Using a reasonable amount of PVAMU resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a PVAMU email account is prohibited. Virus or other malware warnings and mass mailings from PVAMU shall be approved by PVAMU VP Business Affairs before sending. These restrictions also apply to the forwarding of mail received by a PVAMU employee.
- 3.3. Monitoring. PVAMU employees shall have no expectation of privacy in anything they store, send or receive on the University's email system. PVAMU may monitor messages without prior notice. PVAMU is not obliged to monitor email messages.
- 3.4. Enforcement. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment

Contact Office: Information Security Officer; 936/261-9351

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

29.01.06.P1.04 Information Resources – Intrusion Detection

Approved: (May 26, 2009)

Next Scheduled Review: (March-2012)

1. PURPOSE

- 1.1 Intrusion detection plays an important role in implementing and enforcing an organizational security policy. As information resources grow in complexity, effective security systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed systems, some type of assurance is needed that the systems and network are secure. Intrusion detection systems can provide part of that assurance. Intrusion detection provides two important functions in protecting information resources:
 - 1.1.1 Feedback is information that addresses the effectiveness of other components of a security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.
 - 1.1.2 A trigger is a mechanism that determines when to activate planned responses to an intrusion incident.
- 1.2 Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Prairie View A&M University has developed rules and procedures that address acceptable use of information resources. The purpose of this University Administrative Procedure (UAP) is to identify those relevant policies and procedures.

This UAP applies to all University information resources.
- 1.3 The purpose of the implementation of this UAP is to provide a set of measures that will mitigate information security risks associated with acceptable use of University information resources. 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 will be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, 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 information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer.
- 1.4 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.

2. DEFINITIONS

- 2.1 Confidential Information: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g. the Texas Public Information Act.
- 2.2 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.
- 2.3 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

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, and failure to comply with regulations or legal obligations, or closure of the University or department

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

3. PROCEDURES AND RESPONSIBILITIES

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 Alarm and alert functions as well as audit logging of any firewalls and other network perimeter access control systems shall be enabled.
- 3.1.3 Audit logs from the network perimeter access control systems shall be monitored/reviewed as risk management decisions warrant.
- 3.1.4 Audit logs for servers and hosts on the internal, protected network shall be reviewed monthly.
- 3.1.5 Host based intrusion tools will be tested on a routine schedule.
- 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 the University Administration for disposition
 - a. 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.
 - b. 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.
- 3.1.8 All confirmed instances of successful intrusions shall be reported monthly to the Department of Information Resources (DIR) via the Security Incident Reporting System (SIRS).

3.2 RESPONSE AND RECOVERY

- 3.2.1 Based on the assessment of risk, appropriate action should be taken to protect Prairie View A&M University information resources.

Contact Office: Information Security Officer; 936/261-9351

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

29.01.06.P1.05 Information Resources – Malicious Code

Approved: (May 26, 2009)

Next Scheduled Review: (May-2012)

1. PURPOSE

- 1.1 Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Prairie View A&M University has developed rules and procedures that address acceptable use of information resources. The purpose of this University Administrative Procedure (UAP) is to identify those relevant policies and procedures.

This UAP applies to all University 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 acceptable use of University information resources. 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 will be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, 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 information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer.

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.

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 Information Security Officer (ISO): responsible for administering the information security functions within Prairie View A&M University and reports to the Information Resources Manager (IRM).
- 2.2.1 Malicious code: Software that is designed to operate in a manner that is inconsistent with the intentions of the user and which typically results in annoyance or damage to the user's information systems. Examples of such software include:
- A. Viruses: Pieces of code that attach to host programs and propagate when infected program is executed.
 - B. Worms: Particular to networked computers to carry out preprogrammed attacks that jump across the network
 - C. Trojan Horses: Hide malicious code inside a host program that appears to do something useful.
 - D. Attack scripts: These may be written in common languages such as Java or ActiveX to exploit weaknesses in programs; usually intended to cross network platforms.

PRAIRIE VIEW A&M UNIVERSITY
Administrative Procedures Manual

- E. Spyware: Software planted on your system to capture and reveal information to someone outside your system. It can do such things as capture keystrokes while typing passwords, read and track e-mail, record the sites visited, pass along credit card numbers, and so on. It can be planted by Trojan horses or viruses, installed as part of freeware or shareware programs that are downloaded and executed, installed by an employer to track computer usage, or even planted by advertising agencies to assist in feeding targeted ads.

3. PROCEDURES AND RESPONSIBILITIES

3.1. PREVENTION AND DETECTION:

- 3.1.1 For each computer connected to the University network, security updates from the manufacturer of the appropriate operating system, and/or application software, must be kept current (e.g. patched and updated).
- 3.1.2 Where feasible, personal firewall software or hardware shall be installed to aid in the prevention of malicious code attacks/infections.
- 3.1.3 Email attachments and shared files of unknown integrity shall be scanned for malicious code before they are opened or accessed.
- 3.1.4 Diskettes and mass storage devices will be scanned for malicious code before accessing any data on the media.
- 3.1.5 Software to safeguard against malicious code shall be installed and functioning on susceptible information resources that have access to the University network.
- 3.1.6 Software safeguarding information resources against malicious code shall not be disabled or bypassed.
- 3.1.7 The settings for software that protect information resources against malicious code should not be altered in a manner that will reduce the effectiveness of the software.
- 3.1.8 The automatic update frequency of software that safeguards against malicious code shall not be altered to reduce the frequency of updates.

3.2. RESPONSE AND RECOVERY:

- 3.2.1 All reasonable efforts shall be made to contain the effects of any system that is infected with a virus or other malicious code. This may include disconnecting systems from the network or disabling email.
- 3.2.2 If malicious code is discovered, or believed to exist, an attempt should be made to remove or quarantine the malicious code using current anti-virus or other control software.
- 3.2.3 If malicious code cannot be automatically quarantined or removed by anti-virus software, the system shall be disconnected from the network to prevent further possible propagation of the malicious code or other harmful impact. The presence of the malicious code shall be reported to IT personnel so that they may take appropriate actions in removing the malicious code and protecting other systems.
- 3.2.4 Personnel responding to the incident should have the necessary system access privileges and authority to affect the necessary measures to contain/remove the infection.
- 3.2.5 If possible, identify the source of the infection and the type of infection to prevent recurrence
- 3.2.6 Utilize anti-viral, anti-spyware, etc. software to execute a complete system scan including the boot sector and all physical drives, to eradicate all malicious code that may be identified.

PRAIRIE VIEW A&M UNIVERSITY
Administrative Procedures Manual

- 3.2.7 Any removable media (including diskettes, mass storage cards, etc.) recently used on an infected machine shall be scanned prior to opening and/or executing any files contained therein.
- 3.2.8. IT personnel should thoroughly document the incident noting the source of the malicious code (if possible), resources impacted, and damage or disruption to information resources

Contact Office: Information Security Officer; 936/261-9351

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

29.01.06.P1.06 Information Resources – Network Configuration

Approved: (May 26, 2009)

Next Scheduled Review: (May-2012)

1. PURPOSE

- 1.1 The information resources network infrastructure is provided by Prairie View A&M University for all University departments. It is important that the infrastructure, which includes media, active electronic equipment (i.e., routers, switches, cables, etc.) and supporting software, be able to meet current performance requirements, while retaining the flexibility to allow emerging developments in high-speed networking technology and enhanced user services.

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Prairie View A&M University has developed rules and procedures that address acceptable use of information resources. The purpose of this University Administrative Procedure (UAP) is to identify those relevant policies and procedures.

This UAP applies to all University 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 acceptable use of University information resources. 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 will be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, 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 information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer.

- 1.2 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.

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 Information Security Officer (ISO): responsible for administering the information security functions within Prairie View A&M University and reports to the Information Resources Manager (IRM).

3. PROCEDURES AND RESPONSIBILITIES

- 3.1 All network connected equipment must be configured to a specification approved by Prairie View A&M University Information Technology Services.
- 3.2 All hardware connected to the Prairie View A&M University network is subject to its Information Technology Services management and monitoring standards.

PRAIRIE VIEW A&M UNIVERSITY
Administrative Procedures Manual

- 3.3 Changes to the configurations of active network management devices must not be made without the approval of Information Technology Services.
- 3.4 The University network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by the Information Technology Services.
- 3.5 All connections of the network infrastructure to external third party networks is the responsibility of Prairie View A&M University Information Technology Services. This includes connections to external telephone networks.
- 3.6 The use of departmental firewalls is not permitted without the written authorization from Information Technology Services.
- 3.7 Users must not extend or re-transmit network services in any way. Devices such as routers, switches, hubs, or wireless access points cannot be installed on the Prairie View A&M University network without approval from Information Technology Services.
- 3.8 Users must not install network hardware or software that provides network services without Prairie View A&M University Information Technology Services approval.
- 3.9 Users are not permitted to alter network hardware in any way.

Contact Office: Information Security Officer; 936/261-9351

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

29.01.06.P1.07 Information Resources – Network/Wireless Access

Approved: (May 26, 2009)

Next Scheduled Review: (May-2012)

1. PURPOSE

- 1.1 The information resources network infrastructure is provided by Prairie View A&M University for all University departments. It is important that the infrastructure, which includes media, active electronic equipment (i.e., routers, switches, cables, etc.) and supporting software, be able to meet current performance requirements, while retaining the flexibility to allow emerging developments in high-speed networking technology and enhanced user services.

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Prairie View A&M University has developed rules and procedures that address acceptable use of information resources. The purpose of this University Administrative Procedure (UAP) is to identify those relevant policies and procedures.

This UAP applies to all University information resources.

- 1.2 The purpose of the implementation of this SAP is to provide a set of measures that will mitigate information security risks associated with acceptable use of University information resources. 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 will be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this SAP based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer.
- 1.3 The intended audience for this SAP includes, but is not limited to, all information resources management personnel, owners, system administrators, and users of University information resources.

2. DEFINITIONS

- 2.1 Anonymous write capability - the ability of people to save (on Prairie View A&M University computers) information they create without their identity being known (to system administrators).
- 2.2 Anonymously originating network traffic - causing a (Prairie View A&M University) computer system to send traffic via the network where the custodian/owner is not known.
- 2.3 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.

3. PROCEDURES AND RESPONSIBILITIES

- 3.1 Network management/control devices shall not be connected to network infrastructure without prior consultation with the Information Technology Services department.

PRAIRIE VIEW A&M UNIVERSITY
Administrative Procedures Manual

- 3.2 Management of network addresses and name space is managed by Information Technology Services. Users are permitted to use only those network addresses issued to them by Network Services Group of Information Technology Services.
- 3.3 End-users are not to connect to or install any equipment to the network infrastructure without prior approval from Information Technology Services. Additionally, end-users shall not alter or disable University network infrastructure devices or equipment.
- 3.4 Network scans and network vulnerability scans of devices attached to the Prairie View A&M University network as well as the appropriate remediation are occasionally necessary to ensure the integrity of Prairie View A&M University computing systems. Network scans and network vulnerability scans may only be conducted by University employees designated by the organizational unit head responsible for the information resource.
- 3.5 Individuals controlling right-to-use for systems attached to the network infrastructure will ensure only authorized persons are granted access.
- 3.6 Allowing anonymous write capability to University systems or anonymously originating network traffic requires Information Resources permission.
- 3.7 Users shall not alter University-owned network hardware in any way.
- 3.8 [Airspace Guidelines](#) for Using the 2.4 and 5.0 GHz Radio Frequency.
- 3.9 Link to: [AirspacePolicy3.doc](#) for complete guidelines.

Contact Office: Information Security Officer; 936/261-9351

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

29.01.06.P1.08 Information Resources – Password Authentication

Approved: (May 26, 2009)

Next Scheduled Review: (May-2012)

1. PURPOSE

1.1 Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Prairie View A&M University has developed rules and procedures that address acceptable use of information resources. The purpose of this University Administrative Procedure (UAP) is to identify those relevant policies and procedures.

This UAP applies to all University information resources.

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 acceptable use of University information resources. 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 will be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, 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 information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer.

1.3 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.

2. DEFINITIONS

2.1 Confidential Information: information that is accepted from disclosure requirements under the provisions of applicable state or federal law, e.g. the Texas Public Information Act.

2.2 Account information: resource users are typically assigned logon credentials, which include, at the minimum, a unique user name and password.

2.3 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.

2.4 Information Security Officer (ISO): responsible for administering the information security functions within Prairie View A&M University and reports to the Information Resources Manager (IRM).

2.5 Logon ID: a user name that is required as the first step to logging into a secure system. Generally, a logon ID must be associated with a password to be of any use.

2.6 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, and failure to comply with regulations or legal obligations, or closure of the University or department.

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

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

3. PROCEDURES

- 3.1 All passwords shall be constructed and implemented according to the following criteria:
- 3.1.1 Servers that are mission critical and/or maintain confidential information shall have passwords that conform to this SAP.
 - 3.1.2 Passwords must be treated as confidential information. Passwords shall only be revealed to Prairie View A&M University Information Technology Services Personnel (e.g., Help desk) if contact has been initiated by end user/system owner; and, such information is absolutely necessary to conduct routine maintenance on information resources.
 - 3.1.3 Passwords shall be routinely changed (no longer than 90 day intervals for systems processing/storing mission critical and/or confidential data).
 - 3.1.4 Where feasible, owners of systems that maintain mission critical and/or confidential information shall establish a reasonable period of time for passwords to be maintained in history to prevent their reuse.
 - 3.1.5 Passwords shall not be anything that can be easily associated with the account owner such as: user name, social security number, UIN, nickname, relative's name, birth date, telephone number, etc.
 - 3.1.6 Passwords shall not be dictionary words or acronyms regardless of language of origin.
 - 3.1.7 Stored passwords shall be encrypted.
 - 3.1.8 There shall be no more than five tries before a user is locked out of an account. Delay, or progressive delay, helps to prevent automated "trial- and-error" attacks on passwords.
 - 3.1.9 If the security of a password is in doubt, the password shall be changed immediately. If the password has been compromised, the event shall also be reported to the appropriate system administrator(s).
 - 3.1.10 Users should not circumvent password entry with auto logon, application remembering, embedded scripts, or hard-coded passwords in client software for systems that process/store mission critical and/or confidential data. Users should always enter "no" when asked to have a password "remembered".
 - 3.1.11 Exceptions may be made for specific applications (like automated backup) with the approval of the information resource owner. In order for an exception to be approved, there must be a procedure in place for the user to change passwords.
 - 3.1.12 Computing devices shall not be left unattended in unsecured areas without enabling a password-protected screensaver or logging off device.
 - 3.1.13 Forgotten passwords shall be replaced, not reissued.
 - 3.1.14 Procedures for setting and changing information resource passwords include the following:
 - a. The user must verify his/her identity before the password is changed;
 - b. The password must be changed to a "strong" password – (see section 6 below of Password Guidelines); and,
 - c. The user must change password at first log on – where applicable.
 - d. Where possible, passwords that are user selected shall be checked by a password audit system that adheres to the established criteria of the system or service.
 - e. Automated password generation programs must use non- predictable methods of generation.
 - 3.1.15 Systems that auto-generate passwords for initial account establishment must force a password change upon entry into the system.
 - 3.1.16 Password management and automated password generation must have the capability to maintain auditable transaction logs containing information such as:
 - a. Time and date of password change, expiration, administrative reset;
 - b. Type of action performed; and,

PRAIRIE VIEW A&M UNIVERSITY
Administrative Procedures Manual

- c. Source system (e.g., IP and/or MAC address) that originated the change request.

Contact Office: Information Security Officer; 936/261-9351

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

29.01.06.P1.09 Information Resources – Physical Access

Approved: (May 26,2009)

Next Scheduled Review: (May-2012)

1. BACKGROUND

1.1 Technical support staff, system administrators, and others may have information resource physical facility access requirements as part of their function. The granting, controlling, and monitoring of the physical access to information resource facilities is extremely important to an overall security program. The purpose of the Prairie View A&M University physical access procedure is to establish the process for the granting, control, monitoring, and removal of physical access to information resource facilities.

This procedure applies to facilities that house multi-user systems (i.e., “data centers”) that process or store mission critical and/or confidential information.

1.2 The purpose of the implementation of this SAP is to provide a set of measures that will mitigate information security risks associated with physical access. 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. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this SAP based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer.

Responsibility for ensuring secure physical access to information resources may be part of the job function for departmental staff which may include, but not be limited to, information technology staff, system administrators, supervisors, managers, and others.

2. DEFINITIONS

2.1 Confidential Information: Information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g. the Texas Public Information Act.

2.2 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.

2.3 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.

3. PROCEDURES AND RESPONSIBILITIES

3.1 All physical security systems shall comply with applicable regulations such as, but not limited to, building codes and fire prevention codes.

3.2 Physical access procedures to all information resources facilities shall be documented and managed.

3.3 All information resource facilities shall be physically protected in proportion to the criticality or importance of their function at Prairie View A&M University.

3.4 Access to information resources facilities shall be granted only to departmental personnel, vendors, or other authorized personnel whose job responsibilities require access to that facility.

3.5 There shall be an approval and documentation process for granting and revocation/return of security codes, access cards, and/or key access to information resources facilities.

PRAIRIE VIEW A&M UNIVERSITY
Administrative Procedures Manual

- 3.6 Individuals who are granted access rights to an information resource facility must sign appropriate access agreements. Facilities users should also receive information regarding appropriate physical security practices and emergency procedures.
- 3.7 Security access codes, access cards and/or keys to information resource facilities shall not be shared or loaned to others.
- 3.8 Appropriate departmental personnel responsible for the physical security of information resources shall review access rights for the facility on a periodic basis and revoke access for individuals that no longer require such access.
- 3.9 Access cards or keys must not be reallocated to another individual, bypassing the return process.
- 3.10 Access cards and/or keys must not have identifying information other than a return mail address.
- 3.11 Visitors must be escorted in restricted access areas of information resource facilities.
- 3.12 Physical access records shall be maintained as appropriate for the criticality of the information resources being protected. Such records shall be reviewed as needed by organizational unit heads or their designees.

Contact Office: Information Security Officer; 936/261-9351

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

29.01.06.P1.11 Information Resources – Security Awareness Training

Approved: (May 26, 2009)

Next Scheduled Review: (March-2012)

1. PURPOSE

- 1.1 Understanding the importance of information security and individual responsibilities and accountability pertaining to information security are paramount to achieving organization security goals. This can be accomplished with a combination of general information security awareness training and targeted, product-specific training. The security awareness and training information needs to be ongoing and updated as needed. The purpose of the security training procedure is to describe the requirements to ensure each user of university information resources receives adequate training on information security issues.
This University Administrative Procedure (UAP) applies to all users of Prairie View A&M University information resources.
- 1.1 The intended audience is all users of information resources.

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.

3. PROCEDURES AND RESPONSIBILITIES

- 3.1 All Prairie View A&M University personnel who use information resources are required to comply with the procedures outlined in this UAP. A method to accomplish the requirements listed below is provided through the use of the Information Security Awareness (ISA) training module. This web based training module is accessed via Single Sign-On (SSO). The module is one of the offerings listed in the Training section.
- 3.2 All new employees shall complete security awareness training prior to, or at least within 30 days of, being granted access to any Prairie View A&M University information resources. This shall be part of the new employee's orientation training session.
- 3.3 All users must acknowledge they have read, understand, and will comply with university requirements regarding computer security policies and procedures.
- 3.4 All users shall acknowledge completion of university security awareness training on an annual basis. Failure to complete this training may result in the user not being able to access information resources necessary to complete their assigned job duties. The Information Security Officer will work with the Office of Human Resources to identify those individuals who have not completed the required training within 30 days of becoming delinquent in meeting the annual requirement.
- 3.5 Departments may require additional incidental training and require acknowledgement as determined by the department.
- 3.6 Departmental information technology personnel shall establish and maintain a process to communicate new security program information, security bulletin information, and security items of interest to departmental personnel.

CONTACT OFFICE: Information Security Officer; 936/261-9351

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

29.01.06.P1.12 Information Resources – Security Monitoring

Approved: (May 26, 2009)

Next Scheduled Review: (May-2012)

1. PURPOSE

- 1.1 Security Monitoring is a method used to confirm that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as the review of: user account logs, application logs, data backup and recovery logs, automated intrusion detection system logs, etc.

The purpose of security monitoring is to ensure that information resource security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities.

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Prairie View A&M University has developed rules and procedures that address acceptable use of information resources. The purpose of this University Administrative Procedure (UAP) is to identify those relevant policies and procedures.

This UAP applies to all University information resources.

- 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 acceptable use of University information resources. 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 will be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, 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 information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer.
- 1.3 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.

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 Information Security Officer (ISO): responsible for administering the information security functions within Prairie View A&M University and reports to the Information Resources Manager (IRM).
- 2.3 Confidential Information: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.
- 2.4 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

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

financial loss, institutional embarrassment, and failure to comply with regulations or legal obligations, or closure of the University or department.

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

3. PROCEDURES AND RESPONSIBILITIES

- 3.1 Security monitoring of information resources shall be implemented based on risk management decisions by the resource information owner(s).
- 3.2 Mission critical or confidential information resource systems shall, at a minimum, enable operating system logging features. Automated tools shall be used where deemed beneficial by the resource owner based on risk management decisions.
- 3.3 Non-mission critical and non-confidential information resource systems may enable operating system logging features and other security monitoring features.
- 3.4 Network security monitoring will be conducted by Information Technology Services. Any other monitoring shall be coordinated with Information Technology Services, at 936-261-9300.
- 3.5 Logs and other data generated by security monitoring shall be reviewed periodically.
- 3.6 Where feasible, a security baseline shall be developed for determining controls and access to information resources by conducting an annual security risk assessment using the ISAACS tool.
- 3.7 Any significant security issues discovered and all signs of unauthorized activity shall be reported using the procedures detailed in the Incident Management procedure.

Contact Office: Information Security Officer; 936/261-9351

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

29.01.06.P1.13 Information Resources – Server Hardening

Approved: (May 26, 2009)

Next Scheduled Review: (May-2012)

1. PURPOSE

- 1.1 Servers are relied upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Prairie View A&M University has developed rules and procedures that address acceptable use of information resources. The purpose of this University Administrative Procedure (UAP) is to identify those relevant policies and procedures.

- 1.1 This UAP applies to all University 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 acceptable use of University information resources. 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 will be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, 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 information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer.

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.

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 Information Security Officer (ISO): responsible for administering the information security functions within Prairie View A&M University and reports to the Information Resources Manager (IRM).
- 2.3 Confidential Information: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act. .
- 2.4 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, and failure to comply with regulations or legal obligations, or closure of the University or department.
- 2.5 Owner of an Information Resource: an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

PRAIRIE VIEW A&M UNIVERSITY
Administrative Procedures Manual

3. PROCEDURES AND RESPONSIBILITIES

- 3.1 Systems administrators will test security patches prior to implementation.
- 3.2 System administrators shall ensure that vendor supplied patches are routinely acquired, systematically tested, and installed promptly.
- 3.3 System administrators shall remove unnecessary software, system services, and drivers.
- 3.4 System administrators shall enable security features included in vendor supplied systems including, but not limited to, firewalls, virus scanning and malicious code protections, and other file protections (see Malicious Code procedure). Audit logging shall also be enabled. User privileges shall be set utilizing the least privileges concept of providing the minimum amount of access required to perform job functions. The use of passwords shall be enabled in accordance with the University Password Policy.
- 3.5 System administrators shall disable or change the password of default accounts.
- 3.6 Servers shall be tested for known vulnerabilities when new vulnerabilities are announced, and shall seek and implement best practices for securing their particular system platform(s).

Contact Office Information Security Officer; 936/261-9351

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

29.01.06.P1.14 Information Resources – Vendor Access

Approved: (May 26, 2009)

Next Scheduled Review: (May-2012)

1. PURPOSE

- 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. This University Administrative Procedure (UAP) applies to vendor-accessible university mission critical and confidential information.
- 1.3. The purpose of the implementation of this UAP is to provide a set of measures that will mitigate information security risks associated with vendor access. 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. In accordance with Texas Administrative Code 202 - Information Security Standards, *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 information security risk management decisions and business functions.* Such risk management decisions must be documented and reported to the designated Information Security Officer (ISO).
The procedures described herein apply to all departments, administrators, and vendors who are responsible for vendor supplied information resources.

2. DEFINITIONS

- 2.1. Confidential Information: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.
- 2.2. 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.
- 2.3. Information Security Officer (ISO): responsible for administering the information security functions within Prairie View A&M University and reports to the Information Resources Manager (IRM).
- 2.4. 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.

3. PROCEDURES AND RESPONSIBILITIES

- 3.1. Personnel who provide vendors access to university mission critical or confidential information resources shall obtain formal acknowledgement from the vendor of their responsibility to comply with all applicable

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

University policies, rules, standards, 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 are expected to define the following with the vendor:
 - 3.3. The university information to which the vendor should have access;
 - 3.3.1. How university information is to be protected by the vendor;
 - 3.3.2. Acceptable methods for the return, destruction, or disposal of university information in the vendor's possession at the end of the contract;
 - 3.3.3. That use of Prairie View A&M University information and information resources are only for the purpose of the business agreement; any other university information acquired by the vendor in the course of the contract cannot be used for the vendors' own purposes or divulged to others; and,
 - 3.3.4. Vendors shall comply with terms of applicable non-disclosure agreements.
 - 3.4. 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 university policies.
 - 3.5. Appropriate access authorization for each on-site vendor employee (i.e., university affiliate) shall be specified by the resource owner according to the criticality of the information resource.
 - 3.6. Vendor personnel shall report all security incidents directly to appropriate university personnel.
 - 3.7. The responsibilities and details of any vendor management involvement in university security incident management shall be specified in the contract.
 - 3.8. The vendor must follow all applicable university change control processes and procedures. Regular work hours and duties shall be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate university management.
- CONTACT OFFICE: Information Security Officer; 936/261-9351

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

29.01.06.P1.15 Information Resources – Authorized Software

Approved: (May 26, 2009)

Next Scheduled Review: (May-2012)

1. PURPOSE

- 1.1 Authorized software, also called licensed software, is any software that is acceptable for use within the University. Software licensed for use at Prairie View A&M University has end-user license agreements, which protect intellectual assets and inform faculty, staff, and students of their rights and responsibilities under existing intellectual property laws. This procedure is intended to inform University computer users of the rules for authorized software on University information resources.
- 1.2 This University Administrative Procedure (UAP) applies to all University information resources. The purpose of this procedure is to provide a set of measures that will mitigate information security risks associated with Authorized Software. The intended audience is users of University information resources.

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 Software - A computer program, which provides the instructions, which enable the computer hardware to work. System software, such as Windows or Mac OS, operate the machine itself, and applications software, such as spreadsheet or word processing programs, provide specific functionality.
- 2.3 Information Resource Owner - an entity responsible for:
 - 2.3.01 a business function; and,
 - 2.3.02 determining controls and access to information resources supporting that business function.

3. PROCEDURES AND RESPONSIBILITIES

- 3.1 System Regulation 21.99.10, Use of Licensed Commercial Software guides the procedures for appropriate use of authorized software for all University users of University information resources.

Contact Office: Information Security Officer; 936/261-9351

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

29.01.06.P1.16 Information Resources – Portable Computing

Approved: (May 26, 2009)

Next Scheduled Review: (May-2012)

1. PURPOSE

1.1 This University Administrative Procedure (UAP) provides specific guidance on the responsibilities of information resource owners to adequately protect data residing on portable devices. Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to individuals using the devices.

1.2 This UAP applies to all portable computing and storage devices that utilize information resources, especially those which process, store, or transmit confidential information. The purpose of this procedure is to have a set of measures that will mitigate information security risks associate with portable computing.

2. DEFINITIONS

2.1 Confidential Information - Information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.

2.2. Sensitive Personal Information_– An individual’s first name or first initial and last name in combination with any one or more of the following items:

- Social Security Number;
- Driver’s license number or government-issued identification number (including UIN or Student ID)
- Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual’s financial account

2.3 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.

2.4 Internet Service Provider (ISP) - A company that provides access to the internet.

2.5 Portable Computing Device - An easily portable device that is capable of capturing, processing, storing, and transmitting data to and from PVAMU information resources. This includes, but is not limited to: laptops, Personal Digital Assistants (PDAs), and smart phones.

2.6 Portable Storage Device - An easily portable device that stores electronic data. This includes, but is not limited to: flash/thumb drives, iPods, CD-Rs/CD-RWs, DVDs, and removable disk drives.

2.7 Remote Access - The act of using a computing device to access another computer/network from outside of its established security realm (e.g., authentication mechanism, firewall, or encryption).

2.8 Information Resource Owner - an entity responsible for:

- a. a business function; and,
- b. determining controls and access to information resources supporting that business function.

3 PROCEDURES AND RESPONSIBILITIES

PRAIRIE VIEW A&M UNIVERSITY
Administrative Procedures Manual

- 3.1 Portable computing and storage devices, containing confidential information, shall be protected from unauthorized access by passwords or other means.
- 3.2 Any confidential or sensitive personal information stored on portable computing or storage device shall be encrypted with an appropriate encryption technique. It is highly recommended that no confidential or sensitive personal information be stored on any portable computing or storage device but to a PVAMU network share for which this data can be accessed through VPN if required.
- 3.3 All remote access (e.g., dial in services, cable/DSL modem, etc.) to confidential information from a portable computing device shall utilize encryption techniques, such as Virtual Private Network (VPN), secure File Transfer Protocol (FTP), or Secure Sockets Layers (SSL).
- 3.4 Confidential and sensitive personal information shall not be transmitted via wireless connection to, or from, a portable computing device unless encryption methods that appropriately secure wireless transmissions, such as Virtual Private Network (VPN), Wi-Fi Protected Access (WPA) or other secure encryption protocols are utilized.
- 3.5 Unattended portable computing or storage devices, containing confidential information, shall be kept physically secure using means appropriately commensurate with the associated risk.
- 3.6 Where appropriate, keep portable computing devices patched/updated, and install anti-virus software and a personal firewall.

Contact Office

Information Security Officer; 936/261-9351

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

29.01.06.P1.17 Information Resources – Change Management

Approved (May 26, 2009)

Next Scheduled Review: (May-2012)

4 PURPOSE

- 4.1 The information resource infrastructure at TAMU is expanding. As the interdependency among information resources grows, the need for an effective change management process is essential.

From time to time, information resources require a service disruption for planned upgrades, maintenance or fine-tuning. Additionally, such activities may result in unplanned service disruptions. Managing these changes is a critical part of providing a robust and valuable information resource infrastructure.

The goal of change management is to ensure that the intended purpose of the change is successfully accomplished while eliminating or minimizing any negative impact to the users of the resources as a result of the change. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce the negative impact to the user community.

- 4.2 This University Administrative Procedure (UAP) applies to multi-user systems storing or processing mission critical and/or confidential information.

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this SAP are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this SAP. All exclusions must be in accordance with SAP 24.99.99.M1.27 Exclusions from Required Risk Mitigation Measures.

The intended audience is information resource owners and system administrators of University information resources that store or process mission critical and/or confidential information.

5 DEFINITIONS

- 5.1 Confidential Information - information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.

- 5.2 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.

- 5.3 Custodian - The person responsible for implementing owner-defined controls and access to an information resource. The custodian is responsible for the processing and storage of information and is normally a provider of services.

- 5.4 Change:

5.4.01 Any implementation of new functionality

5.4.02 Any interruption of service

5.4.03 Any repair of existing functionality; and

5.4.04 Any removal of existing functionality

- 5.5 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

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

embarrassment, failure to comply with regulations or legal obligations, or closure of the University or department.

- 5.6 Owner of an Information Resource - an entity responsible for:
 - 5.6.01 a business function; and,
 - 5.6.02 determining controls and access to information resources supporting that business function.

6 PROCEDURES AND RESPONSIBILITIES

6.1 A consistent process is to be used for the implementation of information resource changes. The degree to which change management activities and processes are employed is dependant on the projected inherent risk of the change (i.e., potential for unplanned disruption of service, corruption/loss of data, or disclosure of confidential information resulting from the change implementation). Where appropriate, the process should include: preparation, notification/awareness, approval and documentation.

6.2 Preparation includes:

6.2.01 Review results of previously implemented changes to prevent repetitive mistakes or negative impacts.

6.2.02 Determine the following:

6.2.02.1 the best time/date for implementation (to minimize the impact to users);

6.2.02.2 the net impact to other systems or impact to normal operation during and following the change implementation (inherent risk);

6.2.02.3 the risk associated with the change implementation (to minimize the risk of disruption of service caused by the change); and,

6.2.02.4 the concurrence of the resource owner for implementation of the change.

6.2.03 Ensure that the changes do not negatively impact the overall system security

6.3 Notification includes a forum or notification process that informs users of changes planned for implementation. Typically, user notification may include e-mail in addition to an announcement posted on the web. Notification should include relevant details indicated in the documentation section (see 3.4 below).

6.4 Approval and audit of application/software changes includes:

6.4.01 review of the code revision to be implemented which shall be performed by someone other than the developer;

6.4.02 approval of the implementation of code revision performed by someone other than the developer; and,

6.4.03 review of logs for previous change implementations.

6.5 Documentation and change include:

6.5.01 Documentation: any issues identified during the preparation phase that require special considerations or a revision to the implementation plan.

6.5.02 Change details for documentation include:

PRAIRIE VIEW A&M UNIVERSITY
Administrative Procedures Manual

- 6.5.02.1 date/time of change;
- 6.5.02.2 expected duration or length of time required to implement the change;
- 6.5.02.3 nature of the change (a brief description of the net effect);
- 6.5.02.4 developer's name for the modification if newly developed or modified code is involved;
- 6.5.02.5 implementer's name of the modification;
- 6.5.02.6 an indication of successful or unsuccessful completion of the change; and,
- 6.5.02.7 an analysis and "lessons learned" (corrective/preventative actions) for changes that deviated unexpectedly from the plan, resulted in an unplanned disruption of service, corruption of data, or disclosure of confidential information.

Contact Office: Information Security Officer; 936/261-9351

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

29.01.06.P1.18 Information Resources – Incident Management

Approved: (May 26, 2009)

Next Scheduled Review: (May-2012)

7 PURPOSE

- 7.1 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.
- 7.2 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.

8 DEFINITIONS

- 8.1 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.
- 8.2 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.](#)

9 PROCEDURES AND RESPONSIBILITIES

- 9.1 PVAMU system administrators have information security roles and responsibilities which can take priority over normal duties.
- 9.2 System administrators are responsible for notifying their Directors or Department Heads and initiating the appropriate action including restoration.
- 9.3 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.
- 9.4 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).
- 9.5 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.](#)
- 9.6 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

PRAIRIE VIEW A&M UNIVERSITY
Administrative Procedures Manual

action is urgently needed or via email to rvmoore@pvamu.edu and cmmolloy@pvamu.edu as soon as an incident is identified.

9.7 System administrators shall file an after-action incident report to the Information Security Officer.

9.8 The Information Security officer will be the responsible party to report the incident in the monthly DIR SIRS report.

Contact Office: Information Security Officer; 936/261-9351

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

29.01.06.P1.19 Information Resources – Account Management

Approved: (May 26, 2009)

Next Scheduled Review: (May-2012)

1. PURPOSE

- 1.1 Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Prairie View A&M University has developed rules and procedures that address acceptable use of information resources. The purpose of this University Administrative Procedure (UAP) is to identify those relevant policies and procedures.

This UAP applies to all University 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 acceptable use of University information resources. 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 will be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, 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 information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer.

- 1.2 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.

2. DEFINITIONS

- 2.1 Confidential Information - information that is accepted from disclosure requirements under the provisions Of applicable state or federal law, e.g. the Texas Public Information Act.
- 2.2 Account information - resource users are typically assigned logon credentials, which include, at the minimum, a unique user name and password.
- 2.3 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.
- 2.4 Information Security Officer (ISO) - responsible for administering the information security functions within Prairie View A&M University and reports to the Information Resources Manager (IRM).
- 2.5 Information Security Administrator - individuals granting access to university information resources
- 2.6 Logon ID - a user name that is required as the first step to logging into a secure system. Generally, a logon ID must be associated with a password to be of any use.
- 2.7 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, and failure to comply with regulations or legal obligations, or closure of the University or

PRAIRIE VIEW A&M UNIVERSITY
Administrative Procedures Manual

department.

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

3 PROCEDURES AND RESPONSIBILITIES

- 3.1 An approval process is required prior to granting access authorization to an information resource. The approval process shall document the acknowledgement of the account holder to follow all terms of use and the granting of authorization by the resource owner or their designee.
- 3.2 Each person is to have a unique Logon ID and associated account for accountability purposes. Role accounts (e.g., guest or visitor) are to be used in very limited situations, and must provide individual accountability when used to access mission critical and/or confidential information.
- 3.3 Access authorization controls are to be modified appropriately as an account holders employment or job responsibilities change.
- 3.4 Account creation processes are required to ensure that only authorized individuals receive access to information resources.
- 3.2 Processes are required to disable Logon IDs that are associated with individuals that are no longer employed by, or associated with the University. In the event that the access privilege is to remain active, the department (e.g., owner, department head) shall document that a benefit to the University exists.
- 3.6 All access privileges to information resources must be reviewed at least biannually by the owners (department heads or administrators), and documented as such.
- 3.7 Passwords associated with Logon IDs shall comply with the University Password.
- 3.8 Information Security Administrators or other designated staff:
- 3.8.1 Shall have a documented process for removing the accounts of individuals who are no longer authorized to have access to University information resources.
 - 3.8.2 Shall have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes.
 - 3.8.3 Shall have a documented process for periodically reviewing existing accounts for validity.

CONTACT OFFICE: Information Security Officer; 936/261-9351