Texas A&M AgriLife Research Procedures

29.01.03.A0.01 | Information Resource Procedures

Approved: July 3, 1998
Revised: August 25, 2003
February 10, 2005
September 13, 2007
March 31, 2010
August 1, 2011
August 24, 2012

Next Scheduled Review: August 24, 2014

PROCEDURE STATEMENT

This procedure establishes information resources security and management guidelines for all Texas A&M AgriLife Research (AgriLife Research) positions.

REASON FOR PROCEDURE

Under the Information Resources Management Act, TAC 202, Texas A&M University System (System) Regulations and Texas A&M University (University) Rules/Procedures, Information Resources are strategic assets of the State of Texas that must be managed as valuable state resources. These procedures are established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources;
- To establish prudent and acceptable practices regarding the use of information resources;
- To educate individuals who may use information resources with respect to their responsibilities associated with such use.

PROCEDURES AND RESPONSIBILITIES

1.0 GENERAL

1.1 Terms of use:

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of the agency are the property of the agency.

1.2 Violation of these procedures may lead to loss of access privileges to agency information resources and or disciplinary actions.

2.0 RESPONSIBILITIES

2.1 The Director of Texas A&M AgriLife (AgriLife) Information Technology (AIT) is responsible for the interpretation and administration of these procedures. The Director (or a designee, usually the Information Security Officer), Information Technology, must:

A. Develop and maintain written procedures necessary to ensure implementation of and compliance with these procedures.

B. Provide appropriate support and guidance to assist employees to fulfill their responsibilities under these procedures.

C. Develop and maintain a business continuity plan for mission critical IT resources so the effects of a disaster will be minimized.

D. Ensure processes are in place to verify the responsibilities of the custodian and data owner are being performed.

2.2 *Owners* (or designee) within organization must:

A. Identify IT services/resources critical to the operation of the business and convey that information to the custodians.

B. Approve access and formally assign custody of an information resource asset.

C. Approve, justify, document, and be accountable for exceptions to security controls. The owner shall coordinate exceptions of security controls with the Information Security Officer.

D. Determine an asset's value.

E. Protect Information Resource assets commensurate with the value of the asset.

F. Classify data being stored by the application or IT resource.

G. Specify data control requirements and convey them to the users and custodians.

H. Specify appropriate controls, based on risk assessment, to protect the state's information resources from unauthorized modification, deletion, or disclosure. Controls must extend to information resources outsourced by the state agency.

I. Confirm that controls are in place to ensure the confidentiality, availability, and integrity of data.

J. Ensure compliance with applicable controls.

K. Allow only authorized users to access confidential data.

L. Review access lists based on documented security risk management decisions.

M. Ensure all information resource procedures of this document are implemented.

2.3 *Custodians* must:

A. Ensure that all appropriate personnel are aware of and comply with these procedures.

B. Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe these procedures.

C. Implement the controls specified by the owner(s).

D. Schedule risk and vulnerability assessments as warranted by the importance of the data processed.

E. Provide technical, physical, and procedural safeguards for the information resources.

F. Assist owners in evaluating the cost–effectiveness of controls and monitoring.

G. Conduct reviews of physical security implementations and develop/update emergency procedures for physical security of IT resources at annual intervals.

H. Ensure information resources are protected from environmental hazards. Designated employees must be trained to monitor environmental control procedures and equipment. Designated employees must also be trained in desired response in case of emergencies or equipment problems.

I. Implement a written disaster recovery plan for information resources.

J. Implement system identification and logon banners in accordance with state requirements.

K. Implement the monitoring techniques and procedures for detecting, reporting, and investigating incidents. Incidents must be reported to securityhelp@ag.tamu.edu or via the web form at http://agrilifesirs.tamu.edu/.

L. Perform all operational procedures and documentation requirements for server computing platforms as described in the AgriLife Server Management Program.

L. Follow the AgriLife policy for e–mail account request/termination and data retention http://agrilifeas.tamu.edu/library/pdf/rules-procedures/290199a001.pdf.

N. Follow backup and recovery guidelines in section 7.1 of this document.

- Additionally, where applicable, follow enterprise file services use restrictions detailed at: http://agrilifeas.tamu.edu/library/pdf/rules-procedures/290199a002.pdf.

O. Follow network use restrictions detailed at: http://agrilifeas.tamu.edu/library/pdf/rules-procedures/290199a002.pdf.

P. Follow account management procedures detailed at: http://agrilifeas.tamu.edu/library/pdf/rules-procedures/290199a005.pdf.

2.4 *Users* (including staff, guests, consultants, or visitors) must:

A. Follow requirements for physical security in section 3.1 of this document.

B. Follow requirements for computer software use and Installation, copyrights, and license agreements documented in section 13 of this document.

C. Follow requirements for Internet and e–mail use in section 5.1 and 5.2 of this document.

D. Follow network use restrictions detailed at: http://agrilifeas.tamu.edu/library/pdf/rules-procedures/290199a003.pdf.

E. Follow acceptable use regulations in section 5.3 of this document.

F. Follow unacceptable use rules in section 5.4 of this document.

G. Follow computer virus protection requirements in section 6.2 of this document.

H. Where applicable, follow backup and recovery guidelines in section 7.1 of this document and enterprise file services use restrictions detailed at: http://agrilifeas.tamu.edu/library/pdf/rules-procedures/290199a002.pdf.

I. Follow Portable computing guidelines in section 9.5 if applicable.

2.5 Information Security Officer (ISO)

Each institution of higher education head or his or her designated representative(s) shall designate an information security officer to administer the institution of higher education information security program. The ISO reports to executive management.

ISO responsibilities include:

A. Develop and recommend policies and establish procedures and practices, in cooperation with information owners and custodians, necessary to ensure the security of information resource assets against unauthorized or accidental modification, destruction, or disclosure.

B. Document and maintain an up–to–date information security program. The information security program shall be approved by the institution of higher education head or designated representative(s).

C. Monitor the effectiveness of defined controls for mission critical information.

D. Report, at least annually, to the institution of higher education head or designated representative(s) the status and effectiveness of information resources security controls.

E. Issue exceptions to information security requirements or controls in this chapter (with the approval of the institution of higher education head or designated representative). Any such exceptions shall be justified, documented, and communicated as part of the risk assessment process.

F. Review of the institution of higher education's information security program for compliance with these standards. The review will be performed at least biennially, based on business risk management decisions, by individual(s) independent of the information security program and designated by the institution of higher education head or his or her designated representative(s).

G. Incident Management

Security incidents shall be promptly reported to immediate supervisors and the AgriLife ISO. As warranted, the AgriLife ISO will report the condition to the Chief Information Security Officer for the University.

3.0 PHYSICAL SECURITY

It is agency policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

3.1 User Responsibilities:

A. Protect information resources in proportion to the value.

B. Physical access to all agency information resources (including workstations) classified as mission critical and or that store confidential data must be documented and managed.

C. Access to agency Information resource facilities must only be granted to currently employed personnel, vendors, and other authorized personnel whose job responsibilities require access to the facility.

D. Security access codes, access cards, and or keys to agency information resource facilities must not be shared or loaned to others.

E. Appropriate personnel responsible for the physical security of agency information resources must review access rights for the facility on a periodic basis, and revoke access for individuals that no longer require such access.

F. Diskettes, CDs, tapes, or DVDs must be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.

G. Diskettes, CDs, tapes, or DVDs must be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.

H. Mission critical computer equipment such as file servers or network servers (and if applicable, workstations) must be protected by an uninterruptible power supply (UPS). Other computer

equipment should be protected by a UPS or a surge suppressor if at all possible. The UPS equipment should be monitored and the batteries replaced at regular, prudent intervals.

I. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold must be avoided.

J. Users must exercise care to safeguard the valuable electronic equipment assigned to them. Users who neglect this duty may be accountable for any loss or damage that may result.

4.0 COMPUTER RESOURCE SECURITY ACCESS PROCEDURES

4.1 Users are responsible for all computer transactions that are made with his/her User ID and password.

4.2 Users shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords must not be recorded where they may be easily obtained.

4.3 Users must use passwords that will not be easily guessed by others.

4.4 Users must log out or activate a password protected screen saver when leaving a workstation for an extended period. AIT recommends that an inactivity period of no more than 10 minutes be used before a keyboard lock takes place.

5.0 GENERAL INTERNET AND E–MAIL USE PROCEDURES

The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide. One popular feature of the Internet is e–mail. Access to the Internet is provided to users for the benefit of the agency and its customers. Users are able to connect to a variety of educational information resources around the world.

The Internet is also replete with risks and inappropriate material. To ensure that all users are responsible and productive and to protect agency interests, users will adhere to the guidelines when using the Internet and e–mail:

5.1 Users who access the Internet for e–mail must:

A. Follow all email retention and procedures detailed at: http://agrilifeas.tamu.edu/library/pdf/rules-procedures/290199a001.pdf.

B. Ensure that all communications are for professional reasons, and that they do not interfere with their productivity.

C. Be responsible for the content of all text, audio, or images that they place or send over the Internet. All official external communications must have the employee's name and contact information included as a signature block. If the communications is personal in nature, the message must include a disclaimer statement indicating that the content of the message does not represent AgriLife programs.

D. Not transmit copyrighted materials without permission.

E. Run a virus scan on any file(s) received through the Internet.

F. Not click on any e–mail attachment that is sent from an unknown source.

G. Avoid transmission of private customer or employee information. If it is necessary to transmit private information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.

H. Understand that e–mail is not a private or secure form of communication, and may be viewed in accordance with paragraph 11.3.

5.2 Users accessing the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the agency and/or legal action by the copyright owner.

5.3 Acceptable Use:

Users accessing the Internet are representing the agency. Users are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

A. Using Web browsers to obtain educational information from commercial, governmental, and educational Web sites.

B. Accessing databases for information as needed to support official business.

C. Using e–mail for official business communication.

D. Using web browsers to access agency databases and reporting systems.

5.4 Unacceptable Use:

Users must not access the Internet for purposes that are illegal, unethical, harmful to the agency or non–productive. Examples of unacceptable use are:

A. Using an e–mail system other than agency Exchange Mail System operated by AgriLife IT for agency business.

B. Sending or forwarding chain e–mail, i.e., messages containing instructions to forward the message to others.

C. Using agency resources for personal use, except to the extent allowed as incidental personal use as defined in System Policies & Regulations.

D. Using agency resources to promote, or give the appearance of promoting, a personal business; e.g., providing a hypertext link to a family member's business.

E. Transmitting any content that is offensive, harassing, or fraudulent; e.g., pornographic, sexually harassing, or 'get rich quick' materials.

F. Using Peer–to–Peer or File Sharing applications except where a justified business case has been submitted (and approved) by the employee's supervisor and the Agrilife ISO.

G. Use or access any e–mail system unless that system uses virus scanning for e–mail.

H. Use any Internet chat or instant message software capable for transferring files unless they have installed and keep up–to–date the latest virus scanning software and security patches available for that software.

6.0 COMPUTER VIRUS PROTECTION AND WORKSTATION SECURITY/INTEGRITY

6.1 Computer viruses, trojans, worms, spyware, and other such malicious applications are programs designed to make unauthorized changes to programs and data, and therefore, can cause destruction or disclosure of agency resources. While technically not the same, the term antivirus will be used below to refer to this general class of destructive software.

It is important to know that:

A. Computer viruses are much easier to prevent than to cure.

B. Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus–scanning software.

C. A computer account with limited permissions (such as one not classified as an administrator) can reduce the likely–hood of a computer virus infection being successful.

6.2 Users Shall:

A. Use the Enterprise Sophos Anti–Virus software on all agency computer systems.

B. Ensure all installed workstation software is updated to address security vulnerabilities (also known as patched) at regular intervals (at least monthly).

C. Not load diskettes or any removable media (such as thumb–drives/memory sticks) of unknown origin.

D. IMMEDIATELY disconnect workstations from any network to which they may be connected, run available up–to–date virus scanning software, and notify appropriate computer support personnel if it is suspected that their workstations have been infected by viruses.

E. Any agency computer resources used as a training system or for temporary use by a non–employee should be properly secured or re–imaged upon return to avoid any security issues potentially created by the temporary user.

F. Any unused local accounts on computer workstations must be removed when no longer in use.

7.0 BACKUP AND RECOVERY

All electronic information considered of institutional value must be copied onto backup storage media on a regular basis (i.e., backed up) for disaster recovery and business continuity purposes. This section outlines the minimum requirements for the creation and retention of backups. Special backup needs identified through risk analysis which exceed these requirements should be accommodated on an individual basis.

7.1 Users are individually responsible for providing adequate primary backups to ensure the recovery of institutional data and systems in the event of failure or loss. These backup provisions allow agency business processes to be resumed in a reasonable amount of time with minimal loss of data.

7.2 General Guidelines:

A. Backups of institutional data must be retained such that critical operational data is fully recoverable. This may be achieved using a combination of image copies, incremental backups, differential backups, transaction logs, or other techniques.

B. The frequency of backups is determined by the volatility of the data; the retention time for backup copies is determined by the criticality of the data. At a minimum, backups must be retained for 14 days.

C. Backups that have confidential or sensitive data must be encrypted.

D. At a minimum, one fully recoverable version of all mission critical data and any required restoration and application software must be stored in a secure, off–site location. Off–site location means any location which is not likely to be subject to the same catastrophic event (fire, flood, tornado, etc.) as the primary site.

E. Mission critical information used on workstations should be placed on networked file server drives to allow for secondary backup.

F. Derived data (i.e., data calculated from a raw data source) must be backed up only if restoring it is more efficient than recreating it from the original source.

G. Backup documentation must include identification of mission critical data, programs, documentation, and support items necessary to perform essential tasks during a recovery process.

H. Documentation of the restoration process must include procedures for the recovery from single–system or application failures or loss as well as a total center or department disaster scenario.

I. Backup and recovery documentation must be reviewed and updated periodically to account for new technology, business changes, and migration of applications to alternative platforms.

J. Recovery procedures must be tested on a periodic basis, but no less than annually. Tests results must be used to update applicable disaster recovery documentation.

7.3 Enterprise File Services

Where applicable, all users should follow operation procedures outlined in the enterprise file service operation procedures: http://agrilifeas.tamu.edu/library/pdf/rules-procedures/290199a002.pdf

8.0 DATA CLASSIFICATION/PROTECTION

In accordance with the definitions applied to confidential and sensitive data in the Definitions section of this document, security controls must be implemented to protect data appropriate to data value or risk (of use by another party).

Whereas the data owner is most familiar with the type and value of data being stored, the owner is ultimately responsible for determining how it must be protected. Regardless of where the data is stored, confidential and also (in some cases) sensitive data must be protected using encryption procedures. It is suggested that the data owner contact and consult with the data custodian (or the senior IT staff for the department) for assistance in implementing data protection as needed.

8.1 Data on all agency systems is to be classified as one of the following: mission critical, confidential, sensitive, or public.

8.2 Access to confidential or sensitive data must not be permitted with a User ID (or logon ID) alone.

8.3 Scanning for social security numbers (SSNs) is to be performed at least annually. When SSN data is found, it is to be removed or appropriate risk mitigation measures applied (for assistance in this function, please contact AIT Security at securityhelp@ag.tamu.edu).

A. As confidential or sensitive data is identified, risk mitigation measures using encryption must be implemented. Resources are available at http://itim.tamu.edu/encryption/ to assist in the data encryption process.

1. Risk mitigation measures include the following procedures:

- Support a minimum of AES 256 bit encryption.
- Do not use proprietary encryption algorithms.
- Include the recovery of encryption keys in business continuity planning.
- Performing data sanitization (of hard–drives and media) in accordance with TAC 202.78 when hardware retirement is performed to prevent unauthorized exposure
- Encrypting data transmission or using an encrypted tunnel using VPN or SSL when confidential or sensitive data is transmitted to or from an off-site location.
- Encrypting confidential or sensitive data when transmitted via e–mail (including web e–mail programs).

- Encrypting confidential or sensitive data that is stored on removable media (including thumb drives) or backups.
- Encrypting confidential or sensitive data when being transmitted via Instant Message programs.
- Encryption of confidential or sensitive data when accessed remotely from a shared network.
- Use secure Internet transfer protocols (https or secure–FTP) when transferring confidential or sensitive information over the Internet.

9.0 MANAGEMENT CONTROLS

9.1 Change Management

A. General—Change management procedure describes the requirements for managing changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow–up evaluation to reduce negative impact to the user community and to increase the value of information resources.

B. Controls and Responsibilities

1. Every change to agency information resources such as computing hardware, networks, and applications is subject to the change management procedure.
2. Users must be notified for each scheduled or unscheduled change.
3. Confirmation that the change will not negatively impact overall system security.
4. A review must be performed for each change, whether scheduled or unscheduled, and whether successful or not.
5. A change management log must be maintained for all changes made to mission critical resources. The log must contain, but is not limited to:
    - Date of change.
    - Nature of the change.
    - Indication of success or failure.
    - Identity of the individual that implemented the change.
6. In addition to the change log, other documentation that must be provided includes:
    - Updates to relevant operational documentation.
    - Relevant documentation associated with the review/approval process including but not limited to:
        - Review of change related details including code review by the individual(s) responsible for approving the change or their designates.
            - For changes involving code revision, review and approval must be performed by someone other than the developer.
        - Review of logs for previous change implementations.
        - Formal, documented approval or rejection of the change implementation.

- Analysis and corrective/preventative actions (also known as lessons learned) for changes that experienced any of the following:
  - Deviated unexpectedly from the plan.
  - Resulted in an unplanned disruption of service (including service outages that extended longer than expected).
  - Corruption of data.
  - Disclosure of confidential information.

7. The Agency Director delegates responsibility to all unit heads or their equivalent to ensure that agency change management security procedures are implemented in their respective divisions.

9.2 Incident Management

A. General—This section describes the requirements for dealing with computer security incidents. Security incidents include, but are not restricted to:

- Changes to system hardware, firmware, or data without the agency's effective consent.
- Malicious code detection.
- Unauthorized use of computer accounts and computer systems.
- Theft of computer equipment or theft of information.
- Accidental or planned disruption or denial of service.
- Complaints of improper use of information resources as outlined in the security monitoring procedures, the intrusion detection procedures, the internet/intranet procedures, and the acceptable use procedures.

B. Controls and Responsibilities

1. Whenever a security incident is suspected, the appropriate incident management procedures must be followed. Incidents involving AgriLife IT services, must be reported at http://agrilifesirs.tamu.edu/
2. The ISO is responsible for notifying the agency director and initiating the appropriate action including restoration as defined in the incident management procedures.
3. The ISO is responsible for initiating, completing, and documenting the incident investigation.
4. The ISO must report the security incidents that may involve criminal activity under Texas Penal Code Chapters 33 (Computer Crimes) or 33A (Telecommunications Crimes) to the AgriLife Assistant Vice Chancellor for Administration.
5. If fraud or theft is suspected as part of security incident detection, the person detecting the incident must follow System Policy 21.04, *Control of Fraud and Fraudulent Actions*.
6. The ISO is responsible for reporting the incidents to Department of Information Resources as outlined in Texas Administrative Code 202.

9.3 Intrusion Detection

A. General—Intrusion detection plays an important role in implementing and enforcing an organizational security policy. As information systems grow in complexity, effective security

systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed 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. Feedback—Information as to the effectiveness of other components of the 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.

2. Trigger—A mechanism that determines when to activate planned responses to an intrusion incident.

B. Controls and Responsibilities.

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

2. Alarm and alert functions and audit logging of any firewalls and other network perimeter access control systems must be enabled.

3. Audit logs from the perimeter access control systems must be monitored and reviewed periodically by the system administrator.

4. System integrity checks of the firewalls and other network perimeter access control systems must be performed on a routine basis.

5. Audit logs for servers and hosts on the internal, protected, network must be reviewed on a routine basis.

6. All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported according to the incident management procedures.

9.5 Portable Computing

A. General—Portable computing devices (laptop computers, phones, removable storage devices) are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices. However, the portability offered by these devices may increase the security exposure. The purpose of portable computing security procedures is to establish the process for the use of mobile computing devices and their connection to the network.

B. Controls and Responsibilities.

1. Portable computing devices must be protected from unauthorized access by passwords or other means where possible.

2. All sensitive (including confidential) data stored on portable computing devices (including thumb drives) must be encrypted using approved encryption techniques.

3. Data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are used.

4. Non–agency computer systems that require network connectivity must conform to network connectivity standards.

5. Unattended portable computing devices must be kept physically secure.

6. Where appropriate, keep portable computing devices patched/updated, and install anti–virus software and a personal firewall.

9.6 Security Monitoring

A. General—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 recovery logs, automated intrusion detection system logs, etc. The purpose of the security monitoring policy 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. The security monitoring procedure applies to all individuals that are responsible for the installation of new information resources, the operations of existing information resources, and individuals charged with information resources security.

B. Controls and Responsibilities.

1. Where possible automated tools must provide real time notification of detected wrong–doing and vulnerability exploitation. Where possible a security baseline must be developed, and the tools must report exceptions. These tools must be deployed to monitor:

    - Electronic mail traffic.
    - LAN traffic, protocols, and device inventory.
    - Operating system security parameters.

2. Where possible, the following files must be checked for signs of wrong–doing and vulnerability exploitation at a frequency determined by risk:

    - Automated intrusion detection system logs.
    - Firewall logs.
    - User account logs.
    - Network scanning logs.
    - System error logs.
    - Application logs.
    - Data backup and recovery logs.

3. Where possible, the following checks must be performed at least annually by assigned individuals:

    - Password strength.
    - Unauthorized web servers.
    - Unauthorized file sharing.
    - Operating system and software license.

4. Any significant security issues discovered and all signs of wrong–doing must be reported according to incident management procedure.

9.7 Platform Hardening

A. General—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. The purpose of server hardening procedures is to describe the requirements for installing a new server in a secure fashion and maintaining the integrity of server and application software.

B. Controls and Responsibilities.

1. System Administrators must only install the operating system after they have verified the source is legitimate. Practices to ensure the source is legitimate include the following:

   - Certificates of Authenticity– http://www.microsoft.com/howtotell/content.aspx?pg=coa&displaylang=en.

   - Downloading the source code from one location and a checksum from an alternate location.

2. System administrators must apply vendor supplied patches.

3. System administrators must remove unnecessary software, system services, and drivers.

4. System administrators must set security parameters, file protections, and enable audit logging.

5. System administrators must disable or change the password of default accounts.

6. System administrators must implement system identification and logon banners that include the following statements:

   - Unauthorized use is prohibited.

   - Usage may be subject to security testing and monitoring.

   - Misuse is subject to criminal prosecution.

   - No expectation of privacy except as otherwise provided by applicable privacy laws.

7. System Administrators should review and follow all guidelines noted in the Server Management Program related to “New Server Implementation Check List.”

9.8 Systems Development and Acquisition

A. General—The purpose of the system development procedure is to describe the requirements for developing and/or implementing new application software. This procedure is designed according to Texas Administrative Code Rule 202.70 Information Resources Security Safeguards, section Security Policies.

B. Controls and Responsibilities

1. AIT is responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC) plan for system development projects. All software developed in–house which runs on production systems must be developed according to the SDLC plan. At a minimum, this plan must address the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; general design; detail design; development; quality assurance and acceptance testing; implementation; and post implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used for critical information.

2. All production systems must have designated owners and custodians for the critical information they process. Custodians must perform annual risk assessments of production systems to determine whether the controls employed are adequate.

3. All production systems must have an access control system to restrict who can access the system, as well as restrict the privileges available to these users. A designated access control administrator, who is not a regular user of the system in question, must be assigned for all production systems.

4. Where resources permit, there must be a separation between the production, development, and test environments. This ensures that security is rigorously maintained for the production system, while the designated software developers accessing the development and test environments can maximize productivity with fewer security restrictions. Where these distinctions have been established, development and test staff must not be permitted to have access to production systems.

9.9 Vendor Access

A. General. Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors can remotely view, copy and modify data and audit logs, 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 loss of revenue, liability, loss of trust, and embarrassment to the agency. The purpose of vendor access procedures is to establish the process for vendor access to agency information resources and support services (A/C, UPS, PDU, fire suppression, etc.), vendor responsibilities, and protection of information. The vendor access procedure applies to all individuals who are responsible for the installation of new information resources assets, and the operations and maintenance of existing information resources and who do or may allow vendor access for maintenance, monitoring and troubleshooting purposes.

B. Controls and Responsibilities.

1. Vendors must comply with all applicable system policies, practice standards and agreements, including, but not limited to:

   - Safety Policies.
   - Privacy Policies.
   - Security Policies.
   - Auditing Policies.
   - Software Licensing Policies.
   - Acceptable Use Policies.
   - Non–disclosure Policies.

2. To assure compliance with section A above, Information Resource owners, or designees, entering into a contract for services with a vendor must obtain or create documentation indicating that the vendor will have access to mission critical information and must have contracts that specify:

   - Information the vendor must have access to.
   - How information is to be protected by the vendor.
   - Acceptable methods for the return, destruction or disposal of information in the vendor's possession at the end of the contract.

- The identified vendor must only use information and information resources for the purpose of the business agreement.
- Vendors must comply with terms of applicable non–disclosure agreements.
- Any other information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others.

3. Must 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 these policies.

4. Each vendor must provide a list of all employees working on the contract. The list must be updated and provided within 24 hours of staff changes.

5. Vendor personnel must report all security incidents directly to the designated Information Resources point of contact

6. If vendor management is involved in security incident management, the responsibilities and details must be specified in the contract.

7. Regular work hours and duties must be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate management personnel.

10.0 TRAINING AND ACKNOWLEDGMENT

New employees will receive training on information security measures and requirements and be required to acknowledge receipt and acceptance of the provisions of this rule, by signing AgriLife Form AG-415*, Employee Acknowledgment*. All employees are expected to review and acknowledge the provisions of this rule every two years, and will do so through classes offered in HRConnect, the online HR site of the Texas A&M University System (TAMUS). Non–employee users of information resources will be issued a copy of these information security guidelines and required to sign an acknowledgment form prior to being granted access.

11.0 ADMINISTRATOR/SPECIAL ACCESS

Technical support staff, security administrators, system administrators, and others may have special access account privilege requirements compared to typical users. Administrator accounts and other special access accounts have extended privileges in comparison with typical users. Thus, the granting, controlling, and monitoring of these accounts is important to an overall security program. The purpose of the administrator/special access management procedure is to establish the process for the creation, use, monitoring, control, and removal of accounts with special access privilege.

11.1 Departments/units must maintain a list(s) of personnel who have administrator, or special access accounts for departmental/unit information resources systems. The list(s) must be reviewed at least annually by the appropriate department/unit head or their designee.

11.2 Electronic files, including e–mail, created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of agency are not private and may be accessed by supervisors, administrative heads, authorized administrative personnel, and AIT employees during the course of their duties or when authorized by the owner or custodian at any time without knowledge of the user. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards. Information, including e–mail files may also be subject to disclosure under the Texas Public Information Act and/or during the discovery phase of a lawsuit.

11.3 Administrators with special access privileges may routinely access data to investigate events related to performance and/or security of information resources. Personnel from Computing and Information Services (CIS) [e.g., CIS Network Group] may also routinely investigate events related to the performance and secure operation of the Texas A&M University (TAMU) network. System administrators may at times also access user data in maintaining the operational integrity and security of information resources.

System administrators must, however, maintain the confidentiality of user data to the extent possible and not divulge user data except to authorized agency officials (such as described in section 4 below).

11.4 Use of special access privileges to conduct investigations related to user data must be directed by:

A. Appropriate agency management personnel (e.g., department/unit Head, Director, etc.);

B. System officials conducting investigations (e.g., System Internal Audit, Office of General Council, Designated Officer conducting inquiry investigating possible misconduct in the agency, investigating authority in a sexual harassment investigation, investigation of student rules violations, or representatives of Information Technology Issues Management (ITIM) of CIS, etc.).

Prior to conducting such investigations, the individual with administrator/special access will consult with Information Technology Issues Management (ITIM).

12.0 PRIVACY

Privacy policies are mechanisms used to establish the responsibilities and limits for system administrators and users in providing privacy in the agency and TAMU information resources. The agency has the right to examine information on information resources which are under the control or custody of the agency or TAMU. The general right to privacy is extended to the electronic environment to the extent possible. However, there should be no expectation of privacy beyond that which is expressly provided by applicable privacy laws. Privacy is limited by the Texas Public Information Act, administrative review, computer system administration, and audits.

12.1 Privacy of information must be provided to users of the agency or TAMU information resources consistent with obligations of Texas and Federal law and/or secure operation information resources.

12.2 In the normal course of their duties, system administrators may examine user activities, files, electronic mail, and printer listings to gather sufficient information to diagnose and correct problems with system software or hardware.

A. In order to protect against hardware and software failures, backups of all data stored on agency or TAMU information resources may be made. System administrators have the right to examine the contents of these backups to gather sufficient information to diagnose and correct problems with system software or hardware. It is the user's responsibility to find out retention policies for any data of concern.

B. The Agency Director or designee may designate certain individuals or functional areas that may monitor user activities and/or examine data solely to determine if unauthorized access to a system or data is occurring or has occurred. If files are examined, the file owner will be informed as soon as practical, subject to delay in the case of an on–going investigation.

C. Files owned by individual users are to be considered as private (to the degree noted in this procedure), whether or not they are accessible by other users. The ability to read a file does not imply consent or authorization to read that file. Under no circumstances may a user alter a file that does not belong to him or her without prior consent of the file's owner. The ability to alter a file does not imply consent to alter that file.

D. Some individually–owned files are by definition open access. Examples include Unix plan files, Web files made available through a system–wide facility and files made available on an anonymous FTP server. Any authorized user that can access these files may assume consent has been given.

12.3 If access to information is desired without the consent and/or knowledge of the file owner, or if inappropriate use of agency information resources is suspected, files may be reviewed without the consent and/or knowledge of the file owner or file user as identified in section 11.3 of this document.

12.4 If criminal activity is suspected, the University Police Department (UPD) or other appropriate law enforcement agency must be notified. All further access to information on the agency or TAMU information resources must be in accordance with directives from law enforcement agencies.

12.5 Information resource owners or custodians will provide access to information requested by auditors in the performance of their jobs. Notification to file owners will be as directed by the auditors.

12.6 Other than exceptions in sections 11.2, 11.3, 12.2, 12.3, 12.4 and 12.5, access to information by someone other than the file owner requires the owner's explicit, advance consent.

12.7 Unless otherwise provided for, individuals whose relationship with the agency or TAMU is terminated (e.g., student graduates; employee takes new job; visitors depart) are considered to cede ownership to the information resource custodian. Custodians must determine what information is to be retained and delete all other.

12.8 The agency and TAMU collect and process many different types of information from third parties. Much of this information is confidential and must be protected in accordance with all applicable laws and regulations (e.g., Gramm-Leach-Bliley Act, Texas Administrative Code 202).

12.9 Individuals who have special access to information because of their position have the absolute responsibility to not take advantage of that access. If information is inadvertently gained (e.g., seeing a copy of a test or homework) that could provide personal benefit, the individual has the responsibility to notify both the owner of the data and the organizational unit head.

12.10 Any agency or TAMU Web sites available to the general public must contain a Privacy Statement.

12.11 Users of AgriLife or TAMU information resources must immediately contact the AgriLife ISO or Director of AIT to report any compromise of security which could lead to divulging confidential information including, but not limited to, posting social security numbers to the internet.

13.0 COMPUTER SOFTWARE USE AND INSTALLATION, COPYRIGHTS AND LICENSE AGREEMENTS

13.1 Users of agency information resources will comply with all laws regarding intellectual property. Further, installation and operation of certain non–business software, even if freeware or properly licensed, can result in poor performance of legitimate business software.

13.2 The agency is legally bound to comply with the Federal Copyright Act (Title 17 of the U. S. Code: http://www4.law.cornell.edu/uscode/17/), and all proprietary software license agreements. Non–compliance can expose the agency and the responsible user(s) to civil and/or criminal penalties.

13.3 This directive applies to all software that is owned by, licensed to, or developed using agency resources by employees or non–employee users of agency information resources.

13.4 Users Shall:

A. Install on agency computers only that software which is licensed to or owned by the agency and the license covers installation on the employee's specific computer.

B. Copy software only if authorized by the specific license agreement governing that software.

C. Install on agency computers only software which has a business or computer maintenance purpose.

D. Maintain documentation, original media, or other forms of evidence necessary to demonstrate that software installed on agency computers is properly licensed for the specific machines on which it is installed. For example, documentation or media could be stored in a binder, pocket file folder, zip lock bag, or other such storage device, and kept in the immediate vicinity of the computer. IT support personnel reserve the right to remove any unlicensed software from any computer system. If such action is taken, the support person will notify the employee and respective supervisor.

DEFINITIONS

Owner of an Information Resource—A person responsible for a business function and for determining controls and access to information resources supporting that business function. For example, the owner is typically the Unit head, Director, or their designee.

Custodian of an Information Resource—A person responsible for implementing owner defined controls and access to an information resource. Custodians may include state employees, vendors, and any third party acting as an agent of, or otherwise on behalf of the state entity. For example, the custodian is typically an IT manager or resource.

User of an Information Resource—An individual or automated application authorized to access an information resource in accordance with the owner defined controls and access rules.

Confidential Data—Data that is excluded from disclosure under requirements from federal or state law. This can include, but is not limited to: personnel records, health records, financial records, address information, student education records, credit card, social security, or drivers' license numbers.

Sensitive Data—Sensitive data may be subject to disclosure or release under the Texas Public Information Act, however the agency has decided that the data must have the same or equivalent level of protection as confidential data. Examples of sensitive data include: operational information, personnel records, information security procedures, and internal communications.

Mission Critical—Data, which if access to was unavailable, an essential mission of the University, agency, or department would not be able to be continued, and or would cause a significant financial loss to be incurred, would cause institutional embarrassment to take place, would cause an inability to comply with federal regulations or legal obligation, or could cause a possible closure of an agency or University department.

Portable Computing Device—Any device other than a desktop computer that can store data, access the Internet or AgriLife networks, e–mail systems or applications. Examples include notebook computers, internet enabled phones, net book computers, and portable memory devices such as USB drives and memory sticks.

RELATED STATUTES, POLICIES, OR REQUIREMENTS

1 Texas Administrative Code Ch. 202, *Information Security Standards*

1 Texas Administrative Code Ch. 206, *State Web Sites*

1 Texas Administrative Code Ch. 213, *Electronic and Information Resources*

System Policy 29.01, *Information Resources*

System Regulation 29.01.03, *Electronic Information Services Access and Security*

Copyright Law of the United States

System Regulation 29.01.02, *Use of Licensed Commercial Software*

AgriLife Server Management Program Guide

AgriLife Research Procedure 29.01.99.A0.01, *Email Retention and Service*

AgriLife Research Procedure 29.01.99.A0.02, *Enterprise File Service*

AgriLife Research Procedure 29.01.99.A0.03, *AgriLife Research Service Network Procedures*

AgriLife Research Procedure 29.01.99.A0.05, *Information Technology Account Management Procedures*

CONTACT OFFICE

For interpretation or clarification, please contact AgriLife Information Technology at 979-985-5737.