AgriLife Information Technology Custodian Procedures and Best Practices

July 30, 2010

TABLE OF CONTENTS

INTRODUCTION

What is the objective of this document?

- Ensure AgriLife and College of Agriculture and Life Sciences IT staff are aware of the requirements to properly administer University and Agency resources in accordance with State, University, and AgriLife Agency rules, regulations and procedures.

Who is the audience for this document?

- University or Agency employees that are responsible for supporting IT services within an Academic Department, AgriLife Research or AgriLife Extension Service area of operation. These staff are also known as System administrators or custodians.

Who/What is a custodian?

- A custodian is typically an IT manager/resource 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.

CUSTODIAN REQUIREMENTS

Custodians are required to perform the following within their assigned areas of operation. If these requirements are not fulfilled by the custodian, the department or unit head shall be responsible for identifying alternative resources to fulfill these duties.

These requirements apply to all computing and information resources located within Texas A&M University facilities and Texas AgriLife Research or Extension Service locations regardless of funding source or owner of the system.

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

- It is recommended that the custodian assist the unit head in communicating an annual reminder for computer resource use procedures.
- Distribute the AgriLife Best Practices Guideline document to employees annually.
- Unit heads should guarantee custodians are familiar with and practice all the following requirements to maintain University or Agency based computing resources.

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

Processes and procedures that should be implemented include:

- A documented logon ID creation process that ensures accounts are authorized before being issued.
- Ensuring controls are in place to verify account and password regulations are in compliance.
- Employee exit procedures that ensure computing logon IDs and access controls are disabled at the time of employee departure/termination.
- Implement regular monitoring of logon IDs to ensure that accounts that have not been used in more than 45 days are deactivated and eventually removed.
- A verification process to ensure that operating system and application patches are applied to all IT resources at the earliest possible convenience.
- Perform regular scans of servers and workstations to identify and protect all confidential and sensitive data.

Note: It is suggested that random workstation scans be conducted at quarterly intervals. This requirement is more restrictive than the annual scanning requirement imposed by the University SAPs. All workstations that are used by personnel supporting accounting or HR functions should be scanned at quarterly intervals. Confidential data that is identified must either be removed or encrypted. Scanning tools can be obtained from the following sources:

- Identity Finder: http://sell.tamu.edu/Departments/Departmental_Software_List_H-O/Identity_Finder.php
- Cornell Spider http://www2.cit.cornell.edu/security/tools/ Spider

Utilize the Sophos "Data Control Events" report to monitor movement of Confidential information to portable computing devices. The report is available through the Sophos enterprise console. Please contact AgriLife IT if you need assistance in utilizing Sophos Data Control Event functionality.

C. Schedule risk and vulnerability assessments at required frequency by the importance of the data processed.

- All custodians will participate in either the University or AIT facilitated ISSAC assessment process.

- Utilize the vulnerability scanning resources available via mysecurity.tamu.edu to ensure all software vulnerabilities are identified and remediated

Note: Risk assessments must be performed at least annually on all systems, but we recommend systems with mission critical or confidential data be assessed at a minimum twice per year.

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

- Technical: Conduct timely patch management of computing systems.

Note: AIT Recommends a monthly review of all patches for servers and workstations and that critical patches be applied as soon as possible. It is highly recommended that you document the review of patches as well as document the application of these patches (date, systems patched). Auditors typically request this information during system IT audits.

- Physical: Assure computing systems are secure (physically and logically) and that backup media (onsite and offsite) are properly secured.

- Procedural: Establish and document unit based account and data management procedures. (i.e. how workstations hard drive data is removed or destroyed before surplus or re-issue)

E. Assist owners in evaluating the cost-effectiveness of controls and monitoring.

- Custodian and data owner must determine the value of the data and implement appropriate, cost effective, security safeguards to ensure the protection of the data.

F. Conduct reviews of physical security implementations and develop/update emergency procedures for physical security of IT resources

- Annually review physical security implementations and develop or update emergency procedures for physical security of IT resources.

Note: These procedures should be written and include what steps to take and who to contact in an emergency (see Section H for training requirements).

G. Review access permissions and remove access for individuals who are no longer employed or no longer require access to IT resources.

- At a minimum of twice annually, custodians must review access permissions and remove access for individuals who are no longer employed or no longer require access to IT resources.

Note: AIT strongly suggests that you develop a workflow process that disables and removes accounts as employees no longer require access.

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 procedures in case of emergencies, equipment or facilities problems.

Recommended training procedures include:

- Action plans/procedures for power loss or disruption. At a minimum, documention should be provided to the department or unit head detailing the level of availability, computing resources will provide, in the event of power loss.
- Action plans/procedures for environmental hazards such as fire, or flood/water incursion. At a minimum, off site storage of mission critical information data should be provided. This includes regular testing and recovery procedures for this data.
- Action plans/procedures for disruptions in environmental controls such as cooling. At a minimum, a document should be provided to the department or unit head stating what level of availability will be for computer resources in the event of disrupted cooling.

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

- Custodians are required to document a Disaster Recovery plan (for all IT resources) with AgriLife IT and update the plan each August. (**Link:** AIT Disaster Recovery Documentation Application)
- Perform tests of Disaster Recovery procedures at annual intervals. Documentation must also be kept of these test events and their results (i.e. enhancements, changes, or issues noted). Where applicable, documentation should be revised to detail required changes identified from the testing procedures.

J. Implement system identification and logon banners in accordance with state requirements for all information resources (Windows, Mac, Linux, etc.). Registry modification files for Windows systems and instructions for implementing banners on Mac systems are available at the AIT Security page at - http://ait.tamu.edu/security.shtml

Required banner content MUST include:

- This computer system and all data herein are official State of Texas resources and as such are available only for authorized purposes by authorized users.
- Use for any other purpose may result in administrative or disciplinary actions or criminal prosecution against the user.
- Usage is subject to monitoring and security testing.
- The user should have no expectation of privacy except as otherwise provided by applicable privacy laws.

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/

- For Departments/Centers using Sophos, your Anti-Virus / MalWare reports will be automatically rolled into the ISO monthly DIR report. Departments not yet utilizing Sophos are required to submit a Monthly Anti-Virus / Malware report to the AIT Information Security Officer.
- All other security incidents should be reported to the ISO using the email and web site link above.

L. Perform a review of system logs at regular intervals for information resources performing mission critical or confidential operations.

- Utilize log scanning utilities to review system logs housing confidential information or performing mission critical operations. Server logs should be routinely monitored and reviewed for both operational quality assurance purproses as well as security. AIT recommends either a weekly or monthly scheduled procedure to perform this activity.

M. Verify that *User security guidelines* are distributed to all employees, understood by employees and are followed.

- AIT recommends distribution of the formal user guidelines to all staff at annual intervals.
- Annual distribution of the *User Best Practices* document to all staff.

N. Confirm that employees attaching *personal* systems to AgriLife (University or System) networks are following the same guidelines required for state owned systems. These include the following:

- Current and working Anti-virus/Anti-malware product installed

- Operating system and application patches are current.

- No peer-to-peer file sharing applications are installed that could be providing unlicensed copyrighted content.

  Note:
  - College: Peer-to-Peer file sharing applications are currently still approved by University procedures
  - Agencies: Peer-to-Peer file sharing applications have been prohibited without formal approval as of Feb 2010 (See Agency Computer Use Guidelines for details)

- Confidential and or personally identifiable information is identified and properly protected

- All user accounts have passwords that meet recommended password guidelines and are not set to auto-login
- Files and Folders on portable devices containing agency mission critical or confidential information are encrypted

O. Implement Management Controls described below.

The paragraphs below offer high level descriptions of management control strategies you should be aware of and implement. The titles of each are links to more specific information.

In addition to the University SAP reference, specific AgriLife restrictions or guidelines may exist. Please refer to Appendix C for references to the applicable agency procedures.

If additional clarification is needed, please contact the AgriLife Information Security Officer at Securityhelp@ag.tamu.edu

PHYSICAL SECURITY

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

ACCOUNTS AND PASSWORDS

The confidentiality and integrity of data stored on computer systems must be protected by access controls to ensure that only authorized users have access. This access must be restricted to only those capabilities that are appropriate to each user's job duties.

INTERNET AND E-MAIL

A variety of University SAPs and Agency procedures describe policies and controls that should be in place and administered regarding the use of Internet and e-Mail services. This access should be primarily restricted to those activities that are appropriate for each user's job duties.

COMPUTER VIRUS PROTECTION and WORKSTATION SECURITY/INTEGRITY

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.

Sophos is the formally supported and funded anti-virus, and data-leakage tool in Texas A&M AgriLife and the College of Agriculture and Life Sciences and is provided at no cost to all employees.

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 implemented on an individual basis.

DATA CLASSIFICATION/PROTECTION

In accordance with the definitions applied to Confidential and Sensitive data in the *Definitions* section of this document (Appendix A), security controls must be implemented to protect data appropriate to data value or risk (of access/use by another party).

CHANGE MANAGEMENT

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.

INCIDENT MANAGEMENT

This procedure describes the requirements for dealing with computer security incidents.

INTRUSION DETECTION

Intrusion detection plays an important role in implementing and enforcing an organizational security policy. Intrusion detection provides two important functions in protecting information resources:

AgriLife IT recommends that a weekly or monthly review be performed on all computing platforms if automated tools are not in use. All servers and workstations should have audit logging enabled for the purpose of creating and maintaining an activity log.

All suspected and/or confirmed instances of successful intrusions should be reported to the AgriLife IT Information Security officer.

NETWORK CONFIGURATION

The network configuration procedures establish a process for any expansion and use of the network infrastructure. AgriLife network infrastructure is provided by Texas A&M University and TTVN. It is important that the infrastructure, which includes cabling and the associated 'active equipment', continues to develop with sufficient flexibility to meet demands while remaining capable of exploiting developments in high speed networking. This approach allows for implementation of enhanced user services.

Note:

- College: All networking planning and updates should be coordinated with Texas A&M University CIS networking team in accordance with CIS policies and service regulations.

- Agencies: As of July 2010, all networking planning and updates should be coordinated with the AgriLife IT Network Engineer. This includes all changes to firewall, network switch, wireless access points, and routers.

PORTABLE COMPUTING

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

Note:

- All portable computing devices should be encrypted when handling confidential information.
- Portable devices possessing confidential information must be protected by a password login.
- All unattended portable devices containing confidential information must be physically secured.

SECURITY MONITORING

Security Monitoring is used to confirm the security practices and controls in place are 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.

PLATFORM HARDENING

Servers are relied upon to store and deliver data in a secure, reliable fashion. There must be assurance that data confidentiality, integrity and availability are maintained. One of the required steps is to ensure that the servers are installed and maintained to prevent 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. Documentation on server hardening is available at - http://ait.tamu.edu/security/Server-Security-Practices.pdf

SYSTEMS DEVELOPMENT AND ACQUISITION

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.

NOTE: Any third-party contractors or in-house software developers are required to meet all security policies when developing software for public access on State of Texas information resources. These policies and standards must be maintained on a regular basis. It is recommended that appropriate budget and resource plans be established for all custom web based software implementations. Inability to regularly maintain or meet these standards could result in an immediate "take-down" request from Texas A&M System or AgriLife IT administration.

VENDOR ACCESS

Vendors play an important role in the support of customer operations, hardware and software management. 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 AgriLife.

The purpose of vendor access procedures is to establish the process for vendor access to AgriLife 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.

TRAINING AND ACKNOWLEDGEMENT

New employees will receive training on information security measures and requirements and be required to acknowledge reception 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 TAMUS Human Resources office's online training venue. 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.

ADMINISTRATOR / SPECIAL ACCESS

Technical support staff, security administrators, custodians and others may have special access requirements.. 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.

PRIVACY

Privacy policies are used to establish the responsibilities and limits for custodians and users in providing AgriLife and TAMU information resources privacy . Authorized AgriLife IT staff have the right to examine information on information resources under the control or custody of any AgriLife agency or College of Agriculture and Life Sciences The general right to privacy is extended to the electronic environment as far as 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, custodians, and audits.

Appendix A - Definitions

A. 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.

B. 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.

C. 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.

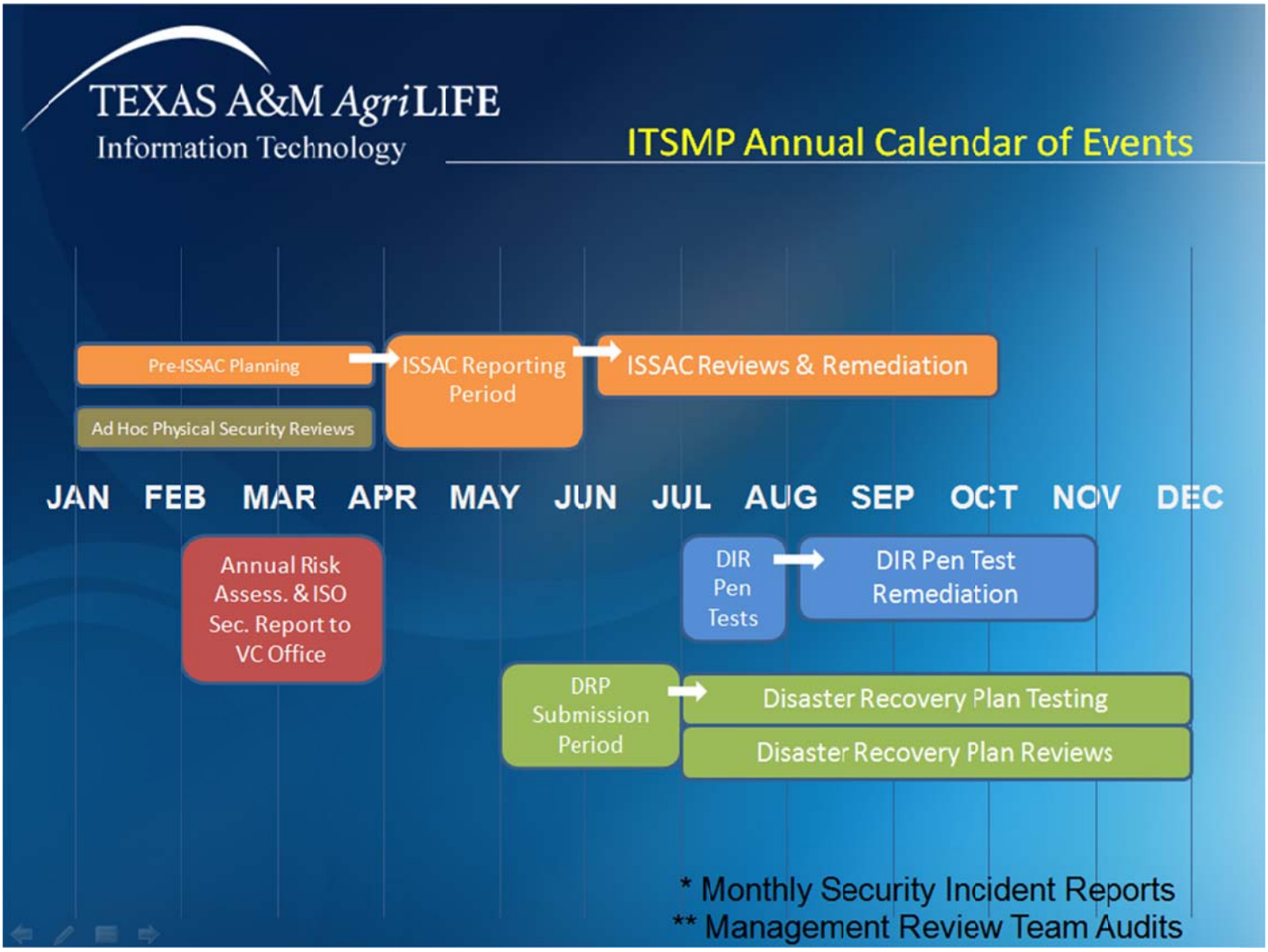
D. Confidential data - data that is excluded from disclosure under requirements from federal or state law. This can include but is not limited to: personnel records, health records, financial records, address information, student education records, credit card, social security, or drivers' license numbers.

E. Sensitive data - Sensitive data may be subject to disclosure or release under the Texas Public Information Act, however AgriLife or the data owner 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, internal communication.

F. 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 a agency or University department.

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

Appendix B - IT Security and Management Program Calendar of Events



Appendix C - Terms of use

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

Violation of these procedures may result in disciplinary action up to and including termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; or dismissal for interns and volunteers. Additionally, individuals are subject to loss of access privileges for AgriLife Information Resources, and potentially civil, or criminal prosecution.

Appendix D - Contact Information

AgriLife Information Technology Contacts

Chuck Braden

Information Security Officer
Email: jcbraden@ag.tamu.edu
Phone: 979.862.7254

Tom Lyster

IT Coordinator - College of Agriculture and Life Sciences, AgriLife Research
Email: tlyster@tamu.edu
Phone: 979.845.1439

Jim Segers

IT Coordinator - Texas AgriLife Extension Service
Email: j-segers@tamu.edu
Phone: 979.845.9341

Alan Kurk

IT Director - Texas A&M AgriLife
Email: akurk@tamu.edu
Phone: 979.845.9343

Appendix E - Related Statutes, Policies, or Requirements

- Texas Admin. Code Ch. 202, *Information Security Standards*
- Texas Admin. Code Ch. 206, *State Web Sites*
- Texas Admin. Code Ch. 213, *Electronic and Information Resources*
- System Policy 29.01, Information Resources
- System Regulation 29.01.03, Electronic Information Services Access and Security
- Texas AgriLife Research - Information Security, Computer Use, and Software Installation/Use (Rev 03-31-2010)
- Texas AgriLife Extension Service - Information Security, Computer Use, and Software Installation/Use (Rev 03-31-2010)