Proposed Solutions for Security Issues Identified in the Management Review Reports

May 26, 2009

This document is intended to provide recommendations for managing accounts, resources and data created at **Texas AgriLife Extension Service** and **Texas AgriLife Research** Centers. While there could be exceptions, under normal circumstances, the data is not considered *mission critical* or *confidential*.

These guidelines are intended to be distributed to all employees to inform them of security practices for properly protecting state resources. These recommendations were created in response to the findings of the Management Review Team that performed security reviews of existing IT implementations. This document was created by the Information Security Officer for Extension and Research.

Section 202.22 (http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=22) of the Texas Administrative Code under the Department of Information Resources, require a risk assessment at least at biennial intervals for state agencies information resources.

Additionally, University and agency Information Resources require protection from malicious software that can exploit operating/application vulnerabilities. To assist in that effort, these procedures were compiled based on the University Standard Administrative Procedures (SAPs) available at http://rules-saps.tamu.edu/TAMURulesAndSAPs.aspx. The University SAPs for Information Resources are under the heading of Risk Management (http://rules-saps.tamu.edu/TAMURulesAndSAPs.aspx#24)

AgIT has been utilizing these practices in the management of the servers we support for Extension and Research customers.

If you have local IT support within your center, the AgIT staff can assist them in implementing these solutions. If no or limited local IT support is available, AgIT can still assist you in addressing any exposures that were identified in the Management Review report.

The procedures for Extension and Research will be reviewed and updated at annual intervals or as changes are made to the University SAPs (whichever is more frequent).

Resident/Center Directors have the ability to authorize exceptions to these recommendations based on their needs. The Information Security Office strongly suggests that these exceptions be identified and documented for each research center. Please provide a copy of these exceptions to the Information Security Office via e-mail at securityhelp@ag.tamu.edu

While the context of these terms is left up to each Resident Director, the general definitions are as follows:

Definitions

Mission Critical:

Applications are not considered *mission critical* if the operation of the agency can continue if data access was unavailable for the period of time when restoration is performed without any impact other than inconvenience. An application SHOULD be considered *mission critical* if one of the following applies: Some essential mission of the University, agency or department would not be able to be continued, a significant financial loss would be incurred, institutional embarrassment would take place, an inability to comply with federal regulations or legal obligation would occur, or the possible closure of a agency or University department could happen, if access to the data was unavailable.

Confidential data:

The term *confidential data* is applicable for any 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 grades, credit card, social security, or drivers' license numbers.

In general, desktop computers should not be used to store data that is confidential or mission critical for Center Operations. Additionally, removable media (such as thumb drives) should not be used to work on confidential data from home or any location other than approved business office unless authorization is provided by the Resident Director for the agency or center. The allowed use of confidential data on home systems presents a problem at the time of employee departure/termination. Employees who have been provided the ability to retain confidential data on systems owned by the employee should be required (in writing) that no content has been retained on the system (or any removable media in their possession) at the time of employee departure.

Research data:

It is recognized that Primary Investigators often use desktop workstations for the creation and storage of research data. While not prohibited, it is discouraged. If such a practice is used, good backup and restoration procedures must also be implemented and tested annually. It is up to the discretion of the Resident Director to authorize such activity and to ensure that data backup and recovery procedures are in place.

Procedures

Acceptable use

All AgriLife staffs are expected to comply with applicable *Terms of Use* documents at http://agrilifeit.tamu.edu/security/AgriLife-security-procedures.htm - Extension, and http://agrilifeit.tamu.edu/security/TAES-Procedure-21_99_10_X1_01.html - Experiment Station.

Administrator logons

All users should logon with administrator privileges only when required. General accounts with power user privileges should be used at all other times.

The Information Security Office recommends using the *runas* (for Windows) feature to authenticate as an administrator as needed. Mac or Linux users should also use the *SU* or *SUDO* options when functions are needed that require privileged authorization.

Administrator/Special access

Passwords that are used for **server systems** should be changed at intervals of 180 days, be at least 11 characters in length and utilize all four of the following: Numeric, 'special', upper and lower case characters. Passwords for servers should also be changed when an employee or vendor (who has knowledge of the password) departs the organization.

Account management

Default passwords for installed applications should be changed at the time of installation. New passwords should be based on the password complexity format identified within these guidelines. Guest logon IDs or anonymous logons should not be used. Access authorization controls should be modified as account holder's employment or job responsibilities change.

Logon ID provisioning

Logon accounts for all employees should be authorized in writing by a supervisor. Logon access should be removed at the time of employee departure. Some employees identified as retired or emeritus can continue to receive e-mail services at the discretion of the supervisor. Logon IDs should be unique and each is associated with a specific individual. If a “generic” access account is needed, justification must be given and signed by the supervisor. See the network user form at http://agrilifeit.tamu.edu/network/ntfrm112.pdf for details

Logon banners prior to authentication

All systems (including workstations) should present a logon banner identifying them as state owned equipment and users of said equipment will be subject to monitoring and must comply with authorized use guidelines. A logon banner is available at http://agrilifeit.tamu.edu/eit-logon-banner.shtml

Security Awareness Training

All employees are required to complete Security Awareness Training provided by the Budget, Payroll and Personnel (BPP) Office via the http://hrconnect.tamu.edu application at annual intervals.

Password Complexity (server AND workstation)
http://agrilifeit.tamu.edu/passwordinfo/passwords.htm

All passwords should meet the following criteria:

- be at least eight characters in length
- be changed at intervals of no greater than 180 days
- be made up of at least 3 of the following: Numeric, upper and lower case characters

Anti-virus Software

All systems should have anti-virus software installed. Additionally, anti-virus software should be configured to download updates automatically and scan for infections at daily intervals.

Several free solutions are available for Windows systems (such as http://free.grisoft.com/ and http://www.pctools.com/free-antivirus/). Solutions for Linux systems can be found at http://www.clamav.org/download/packages/packages-linux

Anti-malware/spyware

All desktop and laptop systems should utilize an anti-malware or anti-spyware solution.

Free solutions for Windows systems include Windows Defender (http://www.microsoft.com/athome/security/spyware/software/default.mspx) and Spyware Doctor (http://pack.google.com/intl/en/pack_installer.html).

A limited number of solutions are available for Mac and Linux systems. Additionally, these products might require purchase for use in non-home systems. Some information for anti-spyware for Macintosh systems at http://macs.about.com/od/softwareandutilities/a/optimizing_2.htm

If you have questions about anti-malware software for Linux systems please send e-mail to securityhelp@ag.tamu.edu

Firewall Safeguards

All systems should utilize firewall products. Firewall solutions are preinstalled on current Windows (XP and Vista) and Macintosh (10.5) systems or are available for download at no cost.

Physical Security

All workstations should have password protected screensavers implemented after 20 minutes of inactivity. Keyboards should be locked when employees are not present at the workstation.

Servers should be secured in areas that are not accessible to the public and require authorization to enter. Authorization should ideally be card access enabled. However, key access authorization is acceptable. If key access is used, the retrieval of all keys should be required when an employee is no longer associated with the organization.

Wireless security practices

IT staff at the center are expected to implement a standard practice to change the wireless authentication key at intervals of 180 days or when an employee leaves the organization (whichever is more frequent).

Vulnerability Assessments

All systems should undergo a regular vulnerability assessment process.

Tools for performing this can be obtained from Microsoft (for Windows products) at http://www.microsoft.com/technet/security/tools/mbsahome.mspx or at the Center for Internet Security - cisecurity.org (for a number of other products).

Please contact the Information Security Office if you need assistance for performing vulnerability assessments on Mac or Linux systems.

Incident Reporting

Security incidents should be reported to each employee's immediate supervisor. If the incident could involve a loss of data on state systems or be propagated to other state resources, it should be documented on the security incident web site at - http://shasta.tamu.edu/sirs/

Vendor/Guest access

Visitors to research and extension centers are expected to comply with the same practices as employees. This includes being current with software patches and also the use of anti-virus and anti-malware products. Temporary logon IDs should be disabled following the departure of guest visitors or vendors. Where applicable, wireless keys should be changed following the departure of guest visitors or vendors.

Software updates and patching

All workstations (both desktop and laptop systems) should have automatic update features turned on. Staff is encouraged to implement operating system and application patches as soon as possible. Procedures should be in place that ensure loaner laptop systems, are returned at least monthly to ensure that all patches have been applied. Server updates should be applied as rapidly as feasible. Testing of operating system and application patches should be performed prior to the implementation of the updates.

For the following operating systems: Windows 2000 SP3, Windows Server 2003, Windows XP and Vista, and for the following Office products: Office 2003, SQL Server, Exchange Server, Office XP and Office 2007, patches can be automatically provided to the system (server, desktop or laptop). The system will need to have an active-X plug-in installed. The plug-in is available from http://www.microsoft.com/protect/computer/updates/mu.mspx

Change Management

All changes to servers (such as web servers) or applications that support mission critical or store confidential data should be documented in a log or spreadsheet file that is retained near or on the server. If the content is stored on the server it should be password protected and includes the name of the change implementer. If the changes are documented in hardcopy form they should be accompanied by the initials of the employee who implemented the change. Also to be included in the documentation is the scheduled implementation date of the change, the developer of the modification, a brief description of the change and if the change was implemented as scheduled.

An involved change management procedure is not required for research data stored on workstation/desktop systems. Primary Investigators or researchers are encouraged to use some process for documenting major changes (such as operating system patches or updates) that are performed on workstations used to store research data. It is recommended that the documentation of the major changes be included on the same (remotely stored) media that is used for backups. This procedure would make it less likely that the change documentation was altered by an unauthorized party.

Installation of software

All installed software should be appropriately licensed, documented and have a University or agency business related function. IT administrators for the agency should have procedures in place to confirm that only appropriately licensed and business related software is installed on both servers and workstations.

Disaster Recovery

All systems essential to the operation of the center should have a disaster recovery plan documented in the disaster recovery web application at - https://eit-data2.tamu.edu/DisRec/slog/index.asp Disaster recovery testing will also be required for each essential system.

Backup and Recovery practices

All servers and desktop systems should have a scheduled backup routine in place. The routine should be documented and reviewed periodically. Additionally, the process should include a data recovery procedure that is tested at intervals no greater than once per year. At least one copy of backup media for all internally developed applications and data should be stored in an offsite location. At a minimum, the offsite location should be located in a different building where possible and for applications identified as 'mission critical' the location should be several miles away from the host system that was used to create the backup.

Media should be stored in an environmentally safe and locked facility that is only accessible University or agency personnel. Where applicable, backups for 'confidential' data should be encrypted and encryption keys be kept in a separate location.

Research data residing on workstation/desktop systems should also have a regular backup procedure in place. Where resources exist, backups for research data should be stored in remote locations.