TEXAS AGRILIFE SERVER MANAGEMENT PROGRAM

Policy Compliancy Checklist
July2012

The server management responsibilities described within are required to be performed per University, Agency or State policy. Each server manager is accountable for performance of these responsibilities as well as timely creation and delivery of any required documentation to the AgriLife Information Security Officer. Questions or inability to perform the below responsibilities should be communicated to the Information Security Officer.

Index

Server Management Program Overview …….. 2

New Server Implementation Check List …… 3

Server Management Task and Documentation Requirements…….. 4,5

Server Management Program Overview

The server management program (SMP) has been developed and implemented within Texas AgriLife Extension Service, Texas AgriLife Research and the College of Agriculture and Life Sciences for the purpose of ensuring the safety, security, and availability of data. This program has been developed in accordance with all current state and university policies regarding the operation of computing resources, as well as responsible IT practices in general.

The SMP effort applies to all server computing resources regardless of function, funding resource or owner. Each server owner and the designated resource managers are accountable for performance of the duties outlined within this document. The SMP is comprised of the following overall components and responsibilities:

- **Server Operations Management Tasks**

  This set of tasks must be performed throughout the lifetime of the server based upon server classification

- **Server Operations Documentation Requirements**

  Some tasks require that documentation be created to formalize a process or activity related to the task. These documentation requirements are outlined along with each task description. All documentation related to ALL servers is required to be filed with the office of the Information Security Officer within AgriLife (no exceptions).

- **Monthly participation in the Information System Security Meetings**

  AgriLife IT conducts a monthly Information System Security (ISS) meeting the 2nd Thursday of each month at 1:30 pm. A server manager or business owner is required to attend each of these meetings in order to meet compliancy rules regarding timely formal and documented reviews of system security updates and patches. These meetings can be attended in person or via Microsoft Lync.

- **Receipt and remediation of automated monthly Nessus Vulnerability Scans**

  AIT will provide automated monthly Nessus Vulnerability reports to each server manager resource. These reports are to be used to manage and document system vulnerability issues as required by state, system and agency policies. Additionally an automated on demand service function is provided.

- **Formal Server Inventory Status Management**

  Each unit or center location that operates a server is required to notify the AgriLife Information Security Officer of each server added or removed from operation regardless of owner or purpose.

- **Centrify Active Directory Integration for all LINUX and MAC servers**

  AIT will provide Centrify licenses to facilitate centralized Active Directory account management for all Linux and MAC servers (Initial allocation, provided by AIT, will not exceed 5 licenses per unit. Additional licenses may be purchased, via AIT, on an as need basis). When possible all existing Windows Servers should be brought up to the standardized Windows Server Platform (currently Server 2008 R2) status and joined to the AGNET domain.

New Server Implementation Check List

The following can be facilitated by the Enterprise Centrify solution is used vs. local accounts on the server:

- ✓ Ensure passwords are updated at a maximum of 180days
- ✓ Ensure passwords meet complexity standards (Comprised of at least three of the following – numeric, upper/lower case and special characters)
- ✓ Ensure password length a minimum of 8 characters.
- ✓ Ensure the logon banner is present for all server and workstation systems.
- ✓ Ensure password history enabled
- ✓ Ensure password changes are logged to the specific IP with time/date stamp.
- ✓ Ensure credentials are hashed and not viewable in plain text when stored on the server.
- ✓ Implement time activated logon ID lock
- ✓ Ensure logging enabled to record when a last successful login took place.
- ✓ Ensure session timeouts in place.

The following items apply to all servers:

- ✓ Ensure DNS resolution performed by a dedicated DNS server.
- ✓ Ensure Anti-Virus solution (Sophos) is installed on the server.
- ✓ Disable or change passwords for all default IDs
- ✓ Ensure logging is enabled for IDs that have root permissions.
  - o IF SUDO installed and users instructed to utilize that feature instead of logging in with the root ID.
- ✓ Ensure SSH is used for all interactive and FTP connections[1]
- ✓ Ensure file sharing disabled (If not, limit only to specific IP's or subnet range)
- ✓ Ensure authentication only providing the minimum amount of information required.
- ✓ Ensure anonymous binds are disabled for LDAP.
- ✓ Ensure all remote console functions are managed through VPN services.
- ✓ Verify that only the required ports are open through the University or regional center firewall.
- ✓ Ensure all services are turned off that are not required and document those services that are required.
- ✓ Perform a vulnerability scan BEFORE putting system into full production mode.

For Servers with Web Servers:

- ✓ Utilize only the latest version of web and database server software
- ✓ Verify *http track and trace* are disabled.
- ✓ Ensure directory traversal has been disabled in the web service configuration.
- ✓ Confirm that web statistics are only viewable to those requiring the information.
- ✓ Verify that all authentications for web application *form*s use encrypted protocols and auto-fill is turned off
- ✓ Verify that uploads are limited to an authenticated directory and restricted to acceptable file formats.
- ✓ Verify *directory indexing* is turned off
- ✓ Verify *form field validation* is implemented to prevent buffer overflows.
- ✓ Verify that *Escaped* or *parameterized input fields* are used to avoid SQL injection
- ✓ Ensure all test and development code is removed

[1] For details on securing FTP please see the follow URL - http://forums.iis.net/t/1147827.aspx

Server Management Tasks	Frequency	Non-Production	Production Non-Mission Critical	Production Mission Critical	Task/Other Requirements	Non-Production	Production Non-Mission Critical	Production Mission Critical	Annual Update/Copy to ISO	Documents	Special Requirements
Account Management	Employee creation, termination or at time of a change in job responsibilities*		*	*	Login ID's should all be unique and not shared		*	*	Update	Account Management Process*	*If not utilizing Agnet Active Directory/AgriLife APM system the indicated documentation is required
			*	*	Access of accounts must be modified appropriately per user employment and responsibilities and modified if any change in job duties necessitates a change.		*	*	Update	Documentation for each account creation, change and deletion*	
			*	*	Named accounts must be used for systems storing confidential or mission critical information						
			*	*	Account must be removed by the timelines indicated in the agency or college Account Management Rules & Procedure						
Backups/Data Restoration-Recovery	Daily		*	*	Backup		*	*	Update	Documented process of backup procedure	"R" Denotes Recommended Task
			R	*	Store backup in an off-site location		*	*	Update	Documented process of recovery procedure	
	Monthly		*	*	Testing of backups (minumum)			*	Update	Documented findings of recovery test	
	Annually			*	Testing of Recovery Process						
Change Management	At Occurrence		R	*	Manually performed change tasks must be logged after each action.		R	*	Update	Documented change management log	All server change entries (hardware, application) must be documented as having been performed and must include What, Who, Date and Time
	At Occurrence		R	*	Automated changes logged by servicing provider (Red Hat Service Monitor, WSUS server, etc.)		R	*	Update	Documented process of change management procedure	
(R denotes Recommended Tasks/Documents)											If a critical update or operation is deferred it should be documented and approved by unit head as to the reason and acceptance of the risk associated by deferral
Disaster Recovery	Annually		R	*	Redundancies should be assessed to maintain higher level of continual service		R	*		DR plan filed with AIT DR Database (http://eit-data.tamu.edu/DisRec/slog/)	*Documentation must be created for all testing results and submitted to the department or unit head for signature and a copy provided to the Information Security Officer
(R denotes Recommended Tasks/Documents)	Annually		R	*	Testing of the disaster recovery process		R	*	Update	Documented Testing Routine	
							R	*	Update	Documented findings of testing routine and mitigation/remediation actions performed*	
							R	*		Password escrow maintained with unit or center head	
Incident Management	As Identified	*	*	*	All secuirty incidents on ANY server platform should be reported immediately to AgriLife Information Security Officer via the Security Incident Reporting web site http://agrilifesirs.tamu.edu/ or via email at securityhelp@ag.tamu.edu						
Malicious Software	Ongoing	*	*	*	Install Sophos Anti-virus and Data Leakage projection client	*	*	*		All non-Enterprise Sophos system managers must submit a monthly electronic report, per specifications, to the AgriLife Information Security Officer by the 1st of each month	
	Ongoing	*	*	*	Manage client status and automatic updates through Sophos Management console						
Confidential Information Scanning	Annually	*	*	*	Scan of all data on servers required to identify any confidential information	*	*	*	Copy	Documented findings, of server scan, and rememdiation steps for each server	*All servers requiring the persistence of confidential information **must be authorized** by the Information Security Officer and the Texas A&M University System Information Security Officer per System policy prior to storing confidential information
	At Occurrence	*	*	*	Following authorization*, all confidential information existing on any server should be encrypted as per guidelines provided by the Information Security Officer						
	Annually	*	*	*	Perform due diligence to ensure "shelved" media (.e.g CDs, DVDs, external HDDs, etc.) scanned and cleared of confidential information						

Server Management Tasks	Frequency	Non-Production	Production Non-Mission Critical	Production Mission Critical	Task/Other Requirements	Non-Production	Production Non-Mission Critical	Production Mission Critical	Annual Update/Copy to ISO	Documents	Special Requirements
Password/ Authentication/ Inactivity/ Logout Applies only to servers not joined to the Agnet Active Directory system	Weekly			*	Monitor account activity logs		*	*	Copy	Documented audit log showing results of account activity log review	Passwords must conform to University/Agency standards Password management and automated password generation routines must have the capability to maintain auditable transaction logs that include: • Time/date of password change/expiration of administrative reset •Type of action performed • Source system that originally generated the password request
	Monthly		*		Monitor account activity logs						
	Not to exceed 180 days	*	*	*	Update passwords at routine intervals						
		R	*	*	Timer activated, password protected screen savers must be in place						
	At Occurrence		*	*	Accounts lock after a maximum of 5 bad attempts and remain locked a minimum of 15 minutes						
Physical Security	Ongoing	R	*	*	House server in secure, locked, limited access location		*	*	Quarterly Copy	Server location access log	
	Ongoing		*		Maintain log sheet for all access to server location if automated control system not in use						
Risk Assessment (ISAAC - University, ISAAC-S, Agencies)	Annually	*	*	*	Where present, IT managers of a UNIT or LOCATION must coordinate with server owners to complete an accurate ISAAC review for all servers in the UNIT	*	*	*	Copy (May 31)	Risk Assessment (ISAAC) form must be filled out for ALL servers within a unit or location REGARDLESS of the funding, owner or purpose of the server	
	Annually	*	*	*	Discovery of any remediation elements will require the establishment of remediation steps and resolve date documented with the office of the Information Security Officer	*	*	*	Copy	Documented remediation steps, for each server, including resolution date	
Patch Management For all servers that do not use the Agnet WSUS or Red Hat Subscription services	Monthly	*	*	*	Attend AgriLife Information Security Officer's Information Systems Security meeting*		*	*	Copy	Documented patch/update installation in Change Management log including dates/times actions performed	*Attendance to AgriLife ISO ISS Meeting can be made in person or via LYNC
	Monthly (at minimum)	*	*	*	Operating System and application software patches/updates applied and confirmed						
	As Identified	*	*	*	Critical updates and patches						
Security Monitoring	Weekly			*	Event logs must be generated and reviewed		*	*	Copy	Document review process and systems	
	Monthly		*		Event logs must be generated and reviewed		*	*	Quarterly Copy	Document /log detailing date, time and server log reviewed	
			*	*	Maintain event logs for minimum of 3 months						
	As Identified	*	*	*	Report all security events to the AgriLife Information Security Officer						
Vulnerability Assessment Required for all systems that are unreachable by the AIT Nessus Vulnerability scanner. For those systems monitored by the AIT Nessus Scanner a weekly report is automatically delivered to each unit.	Quarterly	*	*	*	Conduct Server Vulnerabiltiy Scan (Secunda, etc.)	*	*	*	Copy	If not scanned by the AIT-Nessus Scanner a documented Risk Assessment Review Report must be created and the latest kept on file.	NOTE: If you are not listed as an owner of the system in the University Domain Name server, please e-mail securityhelp@ag.tamu.edu and a solution will be identified that is appropriate for your needs
	As Identified	*	*	*	Discovery of any vulnerabilites will require the establishment of remediation steps and resolve by date with the Information Security Officer	*	*	*	Quarterly Update	Documented log of any remediation efforts	
Regional Center Network Requirements		*	*	*	Request server IP through AIT Network Group						
		*	*	*	Server IP NAT'd private address unless there is a public access requirement						
		*	*	*	Physical network interface card (NIC) use reviewed before implementation						
		*	*	*	No server should have DHCP or DNS service turned on						