MS Windows Server 2012 R2 Baseline Security Standards

Version 1.3

References: 6.100 – Information Technology and Security Policy
6.101 – Use of County Information Technology Resources

Developed: Host Strengthening & Isolation Work Group, Mitigation of Cyber Terrorism

RELEASE NOTES AND HISTORY LOG

The content in this document will be periodically updated to reflect the changes in the County environment as well as the Microsoft Windows Server 2012 software features and capabilities. In addition, this document will be constantly maintained to capture industry best practices as the technology and standards continues to evolve.

DATE	NEW VERSION NUMBER	MODIFIED BY	DESCRIPTION of CHANGE
11/14/2014	1.0	C. Hinton (ISD-ITSS)	1) SET team developed initial document.
12/15/2014	1.1	C. Hinton	1) Remove Password Section and Workstation Section
2/17/2015	1.2	C. Hinton	1) Update Member Server Section
4/01/2015	1.3	C. Hinton	1) Added User Account Control value 2) Re-numbered all sections
4/29/2015		C. Hinton	Confirmation of settings applied on live server from Anthony Phung, ISD – Mid-Range Computing.

Table of Contents

1 Purpose

The purpose of this document is to establish baseline security standards specific to host strengthening. These standards identify the baseline security settings when using Microsoft Windows Server 2012.

2 Overview

This document, with accompanying Windows Server 2012 Security Checklists, outlines the settings that are to be implemented to provide a baseline level of security for each server running Microsoft Windows Server 2012 either stand alone or as part of a Windows Active Directory/Domain Group Policy. Descriptions of the settings are found in the Microsoft Windows Server 2012 Security Guide, Version 3.0 and the Center for Internet Security's Microsoft Windows Server 2012 R2 Benchmark v 1.1.

The settings are divided into categories that correspond to the intended role of the Windows Server. The roles being configured are as follows:

- Member Server Policy
- User Policy
- DHCP Services
- DNS Services
- Web Service

Microsoft recommends using a new core installation of the operating system to start your configuration work so that Server Manager optimally configures just the roles and features that you select. However, if you cannot perform a new installation, ensure to check the following common security configurations before you start a role-specific setup. This approach helps to minimize the possibility of settings from previous configurations interfering with the server's security settings for its new role.

The settings in this standards document are grouped into two categories, "Mandatory" and "Recommended." These categories are defined as follows:

Mandatory – All Mandatory settings (in **red**) must be applied with no exception.

Recommended – All Recommended settings must be applied unless the business operation is severely impacted. Exceptions to settings in this category must have documented justification for the exception and Department management approval.

3 WINDOWS SERVER 2012 IT SECURITY POLICY CHECKLIST – MEMBER SERVER POLICY

This checklist notes the steps needed to secure servers running Windows Server 2012 through the use of Group Policies. The Microsoft Windows Server 2012 Security Guide Version 1.0 and the Center for Internet Security's Microsoft Windows Server 2012 R2 Benchmark v 1.1 provides detailed explanation of these settings. Copies of this completed checklist may prove useful for long-term documentation of preventative measures.

Organization Name:____Date: ______
Contact Information: ____

	Computer Configuration (Enabled)	**Mandatory**	**Recommended**
3.0	**Local Policies/Audit Policy**		
3.0.1	Audit account logon events – Success, Failure	**X**	
3.0.2	Audit account management – Success, Failure	**X**	
3.0.3	Audit logon events – Success, Failure	**X**	
3.0.4	Audit policy change – Success	**X**	
3.0.5	Audit system events – Success *and Failure	**X**	
3.1	**Local Policies/User Rights Assignment**		
3.1.1	Access credential manager as a trusted caller – No One*	**X**	
3.1.2	Access this computer from the network – Administrators, Authenticated Users		**X**
3.1.3	Act as part of the operating system – No One*		**X**
3.1.4	Adjust memory quotas for a process – Administrators, Local Service, Network Service*		**X**
3.1.5	Allow log on locally – Administrators		**X**
3.1.6	Allow log on through Remote Desktop Services – Administrators, Remote Desktop Users*		**X**
3.1.7	Back up files and directories - Administrators		**X**
3.1.8	Change the system time – Administrators, Local Service*		**X**
3.1.9	Change the time zone – Administrators, Local Service*		
3.1.10	Create a pagefile – Administrators*		**X**
3.1.11	Create a token object – No One*		**X**
3.1.12	Create global objects – Administrators, Local Service, Network Service, Service*		**X**
3.1.13	Create permanent shared objects – No One*		**X**
3.1.14	Create symbolic links – Administrators*		**X**
3.1.15	Debug programs – Administrators*		**X**
3.1.16	Deny access to this computer from the network – Guests	**X**	
3.1.17	Deny log on as a batch job – Guests	**X**	
3.1.18	Deny log on as a service – Guests	**X**	
3.1.19	Deny log on locally – Guests*	**X**	
3.1.20	Deny log on through Remote Desktop Services – Guests	**X**	
3.1.21	Enable computer and user accounts to be trusted for delegation – No One*		**X**
3.1.22	Force shutdown from a remote system – Administrators*		**X**
3.1.23	Generate security audits – Local Service, Network Service*		**X**
3.1.24	Impersonate a client after authentication – Administrators, Local Service, Network Service, Service*		**X**
3.1.25	Increase scheduling priority – Administrators*		**X**
3.1.26	Load and unload device drivers – Administrators*		**X**

3.1.27	Lock pages in memory – No One*		X
3.1.28	Manage auditing and security log – Administrators*		X
3.1.29	Modify an object label – No One		X
3.1.30	Modify firmware environment values – Administrators*		X
3.1.31	Perform volume maintenance tasks – Administrators*		X
3.1.32	Profile single process – Administrators*	X	
3.1.33	Profile system performance – Administrators, NT Service\WdiServiceHost*	X	
3.1.34	Replace a process level token – Local Service, Network Service*		X
3.1.35	Restore files and directories – Administrators		X
3.1.36	Shutdown the system - Administrators	X	
3.1.37	Take ownership of files or other objects – Administrators*		X
3.2	**Local Policies/Security Options**		
3.2.1	**Accounts**		
3.2.1.1	Block Microsoft accounts - Users can't add or log on with Microsoft accounts		X
3.2.1.2	Guests account status – Disabled*	X	
3.2.1.3	Limit local account use of blank passwords to console logon only – Enabled*	X	
3.2.1.4	Rename administrator account	X	
3.2.1.5	Rename Guest account		X
3.2.2	**Audit**		
3.2.2.1	Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings - Enabled		X
3.2.2.2	Shut down system immediately if unable to log security audits – Disabled*		X
3.2.3	**Devices**		
3.2.3.1	Allowed to format and eject removable media – Administrators*		X
3.2.3.2	Prevent users from installing printer drivers – Enabled*	X	
3.2.4	**Domain Member**		
3.2.4.1	Digitally encrypt or sign secure channel data (always) – Enabled*		X
3.2.4.2	Digitally encrypt secure channel data (when possible) – Enabled*		X
3.2.4.3	Digitally sign secure channel data (when possible) – Enabled*		X
3.2.4.4	Disable machine account password changes – Disabled*	X	
3.2.4.5	Maximum machine account password age – 30 days or fewer	X	
3.2.4.6	Require strong (Windows 2000 or later) session key – Enabled	X	
3.2.5	**Interactive Logon**		
3.2.5.1	Do not display last user name – Enabled	X	
3.2.5.2	Do not require CTRL+ALT+DEL – Disabled*	X	
3.2.5.3	Machine inactivity limit – 300 to 600 seconds	X	
3.2.5.4	Message text for users attempting to log on –		X
	This computer system, including all related equipment, networks, and networked devices, are the property of Los Angeles County. This computer system is intended for authorized use only, and is being monitored for all lawful purposes. All information received, sent or stored on Los Angeles County computer systems may be, examined, recorded, copied, and used for authorized purposes. Evidence of illegal or unauthorized use may be used for criminal, administrative, or other adverse action. Unauthorized users are subject to prosecution. Click OK if you agree to the above terms.		
3.2.5.5	Message title for users attempting to log on – Not Defined		X

3.2.5.6	Number of previous logons to cache (in case domain controller is not available) – 4 logon or fewer	X	
3.2.5.7	Prompt user to change password before expiration – 14 days*	X	
3.2.5.8	Smart card removal behavior – Lock Workstation		X
3.2.6	**Microsoft Network Client**		
3.2.6.1	Digitally sign communications (always) – Enabled		X
3.2.6.2	Digitally sign communications (if server agrees) – Enabled*		X
3.2.6.3	Send unencrypted password to third-party SMB servers – Disabled*	X	
3.2.7	**Microsoft Network Server**		
3.2.7.1	Amount of idle time required before suspending session – 15 minutes*		X
3.2.7.2	Digitally sign communications (always) – Enabled		X
3.2.7.3	Digitally sign communications (if client agrees) – Enabled		X
3.2.7.4	Disconnect clients when logon hours expire - Enabled*		X
3.2.7.5	Server SPN target name validation level – Accept if provided by client		X
3.2.8	**Network Access**		
3.2.8.1	Allow anonymous SID/Name translation – Disabled*	X	
3.2.8.2	Do not allow anonymous enumeration of SAM accounts – Enabled*	X	
3.2.8.3	Do not allow anonymous enumeration of SAM accounts and shares – Enabled	X	
3.2.8.4	Let Everyone permissions apply to anonymous users – Disabled*	X	
3.2.8.5	Named Pipes that can be accessed anonymously – None*		
3.2.8.6	Remotely accessible registry paths - * System\CurrentControlSet\Control\ProductOptions Systems\CurrentControlSet\Control\Server Applications, Software\Microsoft\Windows NT\CurrentVersion		X
3.2.8.7	Remotely accessible registry paths and sub-paths – * System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog.		X
3.2.8.8	Restrict anonymous access to Named Pipes and Shares – Enabled*	X	
3.2.8.9	Shares that can be accessed anonymously – None*	X	
3.2.8.10	Sharing and security model for local accounts – Classic – local users authenticate as themselves*		X
3.2.9	**Network Security**		
3.2.9.1	Allow Local System to use computer identity for NTLM - Enabled		X
3.2.9.2	Allow LocalSystem NULL session fallback - Disabled		X
3.2.9.3	Allow PKU2U authentication requests to this computer to use online identities – Disabled*	X	
3.2.9.4	Configure encryption types allowed for Kerberos – RC4\AES128\AES256\Future types		X
3.2.9.5	Do not store LAN Manager hash value on next password change – Enabled*	X	

3.2.9.6	Force logoff when logon hours expire - Enabled		**X**
3.2.9.7	LAN Manager authentication level – Send NTLMv2 response only. Refuse LM & NTLM	**X**	
3.2.9.8	LDAP client signing requirements – Negotiate signing*		**X**
3.2.9.9	Minimum session security for NTLM SSP based (including secure RPC) clients – Require NTLMv2 session security Require 128-bit encryption	**X**	
3.2.9.10	Minimum session security for NTLM SSP based (including secure RPC) servers – Require NTLMv2 session security Require 128-bit encryption	**X**	
3.2.10	**Recovery Console**		
3.2.10.1	Allow automatic administrative logon – Disabled*	**X**	
3.2.10.2	Allow floppy copy and access to all drives and all folders – Disabled*		**X**
3.2.11	**Shutdown**		
3.2.11.1	Allow system to be shut down without having to log on – Disabled*	**X**	
3.2.12	**Cryptography**		
3.2.12.1	Use FIPS compliant algorithms for encryption, hashing, and signing - Disabled		**X**
3.2.13	**System Objects**		
3.2.13.1	Require case insensitivity for non-Windows subsystems – Enabled*		**X**
3.2.13.2	Strengthen default permissions of internal system objects (e.g., Symbolic Links) – Enabled*		**X**
3.2.14	**System Settings**		
3.2.14.1	Optional subsystems – None		**X**
3.2.14.2	Use Certificate Rules on Windows Executables for Software Restriction Policies – Enabled		**X**
3.2.15	**User Account Control**		
3.2.15.1	Admin Approval Mode for the Built-in Administrator account - Enabled		**X**
3.2.15.2	Allow UIAccess application to prompt for elevation without using the secure desktop – Disabled*		**X**
3.2.15.3	Behavior of the elevation prompt for administrators in Admin Approval Mode – Prompt for consent on the secure desktop		**X**
3.2.15.4	Behavior of the elevation prompt for standard users – Automatically deny elevation requests		**X**
3.2.15.5	Detect application installation and prompt for elevation – Enabled*		**X**
3.2.15.6	Only elevate UIAccess applications that are installed in secure locations – Enabled*		**X**
3.2.15.7	Run all administrators in Admin Approval Mode – Enabled*		**X**
3.2.15.8	Switch to the secure desktop when prompting for elevation – Enabled*		**X**
3.2.15.9	Virtualize file and registry write failures to per-user locations – Enabled*		**X**
3.2.16	**Event Log**		
3.2.16.1	Maximum application log size – 32,768 KB		**X**
3.2.16.2	Maximum security log size –196,608 KB		**X**
3.2.16.3	Maximum system log size –32,768 KB		**X**
3.2.16.4	Retention method for application log – As needed		**X**
3.2.16.5	Retention method for security log – As needed		**X**
3.2.16.6	Retention method for system log – As needed		**X**

3.17	**Registry**		
	MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon		
3.17.1	**Permissions**		
3.17.1.1	Deny – BUILTIN\Users – Full control – This key and subkeys	**X**	
3.17.1.2	Allow – CREATOR OWNER – Full control – Subkeys only		**X**
3.17.1.3	Allow – NT AUTHORITY\SYSTEM – Full control – This key and subkeys		**X**
3.17.1.4	Allow – BUILTIN\Administrators – Full control – This key and subkeys		**X**
4.4	**Administrative Templates**		
4.4.1	**Systems/Internet Communication Management/Internet Communication Settings**		
4.4.1.1	Turn off the Windows Messenger Customer Experience Improvement Program - Enabled		**X**
4.4.4	**Windows Components/Terminal Services/Remote Desktop Connection Client**		
4.4.4.1	Do not allow passwords to be saved - Enabled	**X**	
4.5	**User Configuration (Disabled)**		
	Policies		
	Administrative Templates		
	Policy definitions (ADMX files) retrieved from the local machine		
4.5.1	**Windows Components/Attachment Manager**		
4.5.1.1	Notify antivirus programs when opening attachments - Enabled	**X**	

Document reviewed and approved by responsible Department manager:

Signature: ____**Date:** ___________________

4 WINDOWS SERVER 2012 IT SECURITY POLICY CHECKLIST – USER POLICY

This checklist notes the additional steps needed to secure servers running Windows Server 2012 through the use of Group Policies. The Windows Server 2012 Security Guide provides detailed explanation of these settings. Your Domain Controller should follow the checklist below in addition to or instead of Member Server Policies. Copies of this completed checklist may prove useful for long-term documentation of preventative measures.

Organization Name:___________________________________ **Date:** _________________________
Contact Information: ____

4.0	**General**	**Mandatory**	**Recommended**
4.1	**Delegation**		
	These groups and users have the specified permission for this GPO		
4.1.1	\Domain Admins – Edit settings, delete, modify security – Not inherited		**X**
4.1.2	\Enterprise Admins – Edit settings, delete, modify security – Not inherited		**X**
4.1.3	NT AUTHORITY\Authenticated Users – Read (from Security Filtering) – Not inherited		**X**
4.1.4	NT AUTHORITY\ENTERPRISE DOMAIN Controllers – Read – Not inherited		**X**
4.1.5	NT AUTHORITY\SYSTEM – Edit settings, delete, modify security – Not inherited		**X**
4.2	**Computer Configuration (Disabled)**		
4.3	**User Configuration (Enabled)**		
4.3.1	**Windows Settings/Internet Explorer Maintenance/URLs**		
4.3.1.1	Home page URL – Department discretion		**X**
4.3.1.2	Search bar URL – Not configured		**X**
4.3.1.3	Online Support page URL – Not configured		**X**

Document reviewed and approved by responsible Department manager:

Signature: ____ **Date:** __________________

5 WINDOWS SERVER 2012 IT SECURITY POLICY CHECKLIST – DHCP Hardening

This checklist notes the steps needed to secure servers running Windows Server 2012 through the use of Group Policies. The Windows Server 2012 Security Guide provides detailed explanation of these settings. Copies of this completed checklist may prove useful for long-term documentation of preventative measures. This checklist does not represent a complete solution, and should not be taken as such.

Organization Name:____Date: ______
Contact Information: ____

5.0	General	Mandatory	Recommended
5.0.1	Dedicate a computer to running the DHCP Server role.		X
5.0.2	Deploy a Server Core installation of Windows Server 2012.		X
5.0.3	Use DHCPv6 functionality		X
5.0.4	Eliminate computers running rogue DHCP services.		X
5.0.5	Add DHCP reservation and exclusion ranges for IP Addresses	X	
5.0.6	Use NAP to enforce Computer Configuration Health		X
5.0.7	Restrict DHCP security group membership	X	
5.0.8	Configure DNS record ownership to help prevent stale DNS records		X
5.0.9	Relevant Group Policy Settings		
5.0.10	DHCP Administrators – Domain Admins	X	
5.0.11	DHCP Users – Not created		X

Document reviewed and approved by responsible Department manager:

Signature: ____ Date: ______________________

6 WINDOWS SERVER 2012 IT SECURITY POLICY CHECKLIST – DNS Hardening

This checklist notes the steps needed to secure servers running Windows Server 2012 through the use of Group Policies. The Windows Server 2012 Security Guide provides detailed explanation of these settings. Copies of this completed checklist may prove useful for long-term documentation of preventative measures. This checklist does not represent a complete solution, and should not be taken as such.

Organization Name:____Date: ____________
Contact Information: ____

6.0	General	Mandatory	Recommended
6.0.1	Deploy a Server Core installation of Windows Server 2012		X
6.0.2	Protect DNS zones in unsecured locations by using read-only domain controllers (RODCs).		X
6.0.3	Combine the DNS and AD DS server roles on the same server		X
6.0.4	Configure zones to use secure dynamic updates		X
6.0.5	Restrict zone transfers to specific server computers running DNS.	X	
6.0.6	Deploy separate server computers for internal and external DNS resolution.		X
6.0.7	Configure the firewall to protect the internal DNS namespace		X
6.0.8	Enable recursion to only the appropriate DNS servers.		X
6.0.9	Configure DNS to ignore non-authoritative resource records.		X
6.0.10	Configure root hints for the internal DNS namespace.		X

Document reviewed and approved by responsible Department manager:

Signature: ____ Date: __________________

7 WINDOWS SERVER 2012 IT SECURITY POLICY CHECKLIST – Web Services Hardening

This checklist notes the steps needed to secure servers running Windows Server 2012 through the use of Group Policies. The Windows Server 2012 Security Guide provides detailed explanation of these settings. Copies of this completed checklist may prove useful for long-term documentation of preventative measures. This checklist does not represent a complete solution, and should not be taken as such.

Organization Name:____ Date: _____________________
Contact Information: ____

7.0	General	Mandatory	Recommended
7.0.1	Deploy a Server Core installation of Windows Server 2012		X
7.0.2	Install the application development environment		X
7.0.3	Set the authentication mechanism		X
7.0.4	Remove unused IIS components	X	
7.0.5	Configure a unique binding		X
7.0.6	Move Root Directories to a separate data partition	X	
7.0.7	Configuring user account permissions	X	
7.0.8	Enable Secure Sockets Layers (SSL)		X
7.0.9	Consider additional specialized security configuration measures		
7.0.10	Access control list hardening by specifying particular users in the ACL for content directory instead of allowing all domain users access to the site.		X
7.0.11	Limit access to the Web site by using the built-in IIS7 URL Authorization feature		X
7.0.12	Restrict the IP Addresses of the client browsers you allow to connect to the Web server using the IPv4 Restriction Lists feature.		X
7.0.13	Control many HTTP features, such as HTTP verbs, HTTP headers and URL size using the Request Filtering feature.		X

Document reviewed and approved by responsible Department manager:

Signature: ____ Date: ___________________