Operating System Standard – Windows Server Configuration

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: Internal*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX.

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Industry Configuration Standards 3

1.5 Related Documents / References 3

2. Standard Statements 4

2.1 Windows Server Configuration Baseline 4

3. Standard Compliance & Enforcement 21

3.1 Compliance Measures 21

3.2 Enforcement 21

4. Exception Process / Glossary 22

4.1 Exception Process 22

4.2 Glossary / Acronyms 22

5. Document Management 23

5.1 Document Revision Log 23

5.2 Document Ownership 23

5.3 Document Coordinator 23

5.4 Document Approvers 23

5.5 Document Distribution 23

# Introduction

## Document Definition

This document is a Standard.

For a full description of document types, see XXXX-POL-ALL-001 - Information Security Policy Framework.

## Objective

Security is complex and constantly changing. The objective of this standard is to provide a minimum baseline of Window Server Security and to help Administrators avoid some of the common configuration flaws that could leave systems more exposed.

## Scope

### Applicability to employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This Standard applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Standard statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This Standard applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Industry Configuration Standards

* Centre for Internet Security (CIS): http://www.cisecurity.org/
* Security Technical Implementation Guides (STIGs): http://iase.disa.mil/stigs

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*

# Standard Statements

## Windows Server Configuration Baseline

Account Policies

|  |  |  |
| --- | --- | --- |
| **1.1** | **Account Policies** | **Setting** |
| 1.1.1 | Enforce password | 24 remembered; not required to set for local accounts |
| 1.1.2 | Maximum password age | 90 days (maximum) |
| 1.1.3 | Minimum password age | 1 day or more |
| 1.1.4 | Minimum password length | 10 characters |
| 1.1.5 | Password must meet complexity requirements | Enabled |
| 1.1.6 | Store passwords using reversible encryption | Disabled |
| 1.1.7 | Account lockout duration | 10 minutes (minimum) |
| 1.1.8 | Account lockout threshold | 3 attempts |
| 1.1.9 | Reset account lockout counter after | 30 minutes (minimum) |
| 1.1.10 | Enforce user logon restrictions | Enabled |
| 1.1.11 | Maximum tolerance for computer clock synchronization | 5 |
| 1.1.12 | Maximum lifetime for service ticket | 600 |
| 1.1.13 | Maximum lifetime for user ticket renewal | 7 days |
| 1.1.14 | Maximum lifetime for user ticket | 10 |

Audit Policies

|  |  |  |
| --- | --- | --- |
| **1.2** | **Audit Policy** | **Setting** |
| 1.2.1 | Audit Account Logon Events | Success and Failure |
| 1.2.2 | Audit Account Management | Success and Failure |
| 1.2.3 | Audit Directory Service Access | No Auditing |
| 1.2.4 | Audit Logon Events | Success and Failure |
| 1.2.5 | Audit Object Access | Failure (minimum) |
| 1.2.6 | Audit Policy Change | Success (minimum) |
| 1.2.7 | Audit Privilege Use | Failure (minimum) |
| 1.2.8 | Audit Process Tracking | No Audit |
| 1.2.9 | Audit System Events | Success (minimum) |
| 1.2.10 | Audit: Shut down system immediately if unable to log security audits | Disabled |
| 1.2.11 | Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings | Enabled |

Detailed Security Auditing

|  |  |  |
| --- | --- | --- |
| **1.3** | **Detailed Security Auditing** | **Setting** |
| 1.3.1 | Audit Policy: System: IPsec Driver | Success and Failure |
| 1.3.2 | Audit Policy: System: Security State Change | Success and Failure |
| 1.3.3 | Audit Policy: System: Security System Extension | Success and Failure |
| 1.3.4 | Audit Policy: System: System Integrity | Success and Failure |
| 1.3.5 | Audit Policy: Logon-Logoff: Logoff | Success |
| 1.3.6 | Audit Policy: Logon-Logoff: Logon | Success and Failure |
| 1.3.7 | Audit Policy: Logon-Logoff: Special Logon | Success |
| 1.3.8 | Audit Policy: Object Access: File System | Failure |
| 1.3.9 | Audit Policy: Object Access: Registry | Failure |
| 1.3.10 | Audit Policy: Privilege Use: Sensitive Privilege Use | No auditing |
| 1.3.11 | Audit Policy: Detailed Tracking: Process Creation | Success |
| 1.3.12 | Audit Policy: Policy Change: Audit Policy Change | Success and Failure |

|  |  |  |
| --- | --- | --- |
| **1.3** | **Detailed Security Auditing** | **Setting** |
| 1.3.13 | Audit Policy: Policy Change: Authentication Policy Change | Success |
| 1.3.14 | Audit Policy: Account Management: Computer Account Management | Success and Failure |
| 1.3.15 | Audit Policy: Account Management: Other Account Management Events | Success and Failure |
| 1.3.16 | Audit Policy: Account Management: Security Group Management | Success and Failure |
| 1.3.17 | Audit Policy: Account Management: User Account Management | Success and Failure |
| 1.3.18 | Audit Policy: DS Access: Directory Service Access | No Auditing |
| 1.3.19 | Audit Policy: DS Access: Directory Service Changes | No Auditing |
| 1.3.20 | Audit Policy: Account Logon: Credential Validation | Success and Failure |

Event Log

|  |  |  |
| --- | --- | --- |
| **1.4** | **Event Log** | **Setting** |
| 1.4.1 | Application: Maximum Log Size (KB) | 32768 KB or greater |
| 1.4.2 | Application: Retain old events | Disabled |
| 1.4.3 | Security: Maximum Log Size (KB) | 81920 KB or greater |
| 1.4.4 | Security: Retain old events | Disabled |
| 1.4.5 | System: Maximum Log Size (KB) | 32768 KB or greater |
| 1.4.6 | System: Retain old events | Disabled |

Windows Firewall

|  |  |  |
| --- | --- | --- |
| 1.5.1 | Windows Firewall: Allow ICMP exceptions (Domain) | Disabled |
| 1.5.2 | Windows Firewall: Allow ICMP exceptions (Standard) | Disabled |
| 1.5.3 | Windows Firewall: Apply local connection security rules (Domain) | For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Configured. For the Member Server and Domain Controller profile(s), the recommended value is No. |
| 1.5.4 | Windows Firewall: Apply local connection security rules (Private) | For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Configured. For the Member Server and Domain Controller profile(s), the recommended value is No. |
| 1.5.5 | Windows Firewall: Apply local connection security rules (Public) | No |
| 1.5.6 | Windows Firewall: Apply local firewall rules (Domain) | For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Configured. For the Member Server and Domain Controller profile(s), the recommended value is No. |
| 1.5.7 | Windows Firewall: Apply local firewall rules (Private) | For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Configured. For the Member Server and Domain Controller profile(s), the recommended value is No. |
| 1.5.8 | Windows Firewall: Apply local firewall rules (Public) | No |
| 1.5.9 | Windows Firewall: Display a notification (Domain) | For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. For the Member Server and Domain Controller profile(s), the recommended value is Yes. |
| 1.5.10 | Windows Firewall: Display a notification (Private) | For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. For the Member Server and Domain Controller profile(s), the recommended value is Yes. |
| 1.5.11 | Windows Firewall: Display a notification (Public) | No |
| 1.5.12 | Windows Firewall: Firewall state (Domain) | On |
| 1.5.13 | Windows Firewall: Firewall state (Private) | On |
| 1.5.14 | Windows Firewall: Firewall state (Public) | On |
| 1.5.15 | Windows Firewall: Inbound connections (Domain) | Block |
| 1.5.16 | Windows Firewall: Inbound connections (Private) | Block |
| 1.5.17 | Windows Firewall: Inbound connections (Public) | Block |
| 1.5.18 | Windows Firewall: Prohibit notifications (Domain) | Disabled |
| 1.5.19 | Windows Firewall: Prohibit notifications (Standard) | Disabled |
| 1.5.20 | Windows Firewall: Protect all network connections (Domain) | Enabled |
| 1.5.21 | Windows Firewall: Protect all network connections (Standard) | Enabled |

|  |  |  |
| --- | --- | --- |
| 1.6.1 | Configure Automatic Updates | Enabled: 3 - Auto download and notify for install |
| 1.6.2 | Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box | Disabled |
| 1.6.3 | Reschedule Automatic Updates scheduled installations | Enabled |

User Rights

|  |  |  |
| --- | --- | --- |
| **1.8** | **User Rights** | **Setting** |
| 1.8.1 | Access this computer from the network | For the Enterprise Member Server and Member Server profile(s), the recommended value is Administrators, Authenticated Users. For the Enterprise Domain Controller and Domain Controller profile(s), the recommended value is Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS. |
| 1.8.2 | Act as part of the operating system | No one |
| 1.8.3 | Adjust memory quotas for a process | For the Member Server and Domain Controller profile(s), the recommended value is Administrators, LOCAL SERVICE, NETWORK SERVICE. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.8.4 | Back up files and directories | For the Member Server and Domain Controller profile(s), the recommended value is Administrators. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.8.5 | Bypass traverse checking | For the Enterprise Member Server profile(s), the recommended value is Administrators, Authenticated Users, Backup Operators, Local Service, Network Service. For the Enterprise Domain Controller profile(s), the recommended value is Not Defined. For the Domain Controller profile(s), the recommended value is Authenticated Users, Local Service, Network Service. For the Member Server profile(s), the recommended value is Administrators, Authenticated Users, Local Service, Network Service. |
| 1.8.6 | Change the system time | LOCAL SERVICE, Administrators |
| 1.8.7 | Create a pagefile | For the Enterprise Member Server, Member Server and Domain Controller profile(s), the recommended value is Administrators. For the Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.8.8 | Create a token object | No One |
| 1.8.9 | Create global objects | For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. For the Member Server and Domain Controller profile(s), the recommended value is Administrators, SERVICE, Local Service, Network Service. |
| 1.8.10 | Create permanent shared objects | No One |
| 1.8.11 | Debug programs | For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Administrators. For the Member Server and Domain Controller profile(s), the recommended value is No one. |
| 1.8.12 | Deny access to this computer from the network | Guests |
| 1.8.13 | Enable computer and user accounts to be trusted for delegation | No One |
| 1.8.14 | Force shutdown from a remote system | For the Member Server and Domain Controller profile(s), the recommended value is Administrators. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.8.15 | Impersonate a client after | For all profiles, the recommended state for this setting is Administrators, SERVICE, Local Service, Network Service. |
| 1.8.16 | Increase scheduling priority | For the Member Server and Domain Controller profile(s), the recommended value is Administrators. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.8.17 | Load and unload device drivers | Administrators |
| 1.8.18 | Lock pages in memory | For the Member Server and Domain Controller profile(s), the recommended value is No one. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.8.19 | Manage auditing and security log | For the Enterprise Member Server, Member Server and Domain Controller profile(s), the recommended value is Administrators. For the Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.8.20 | Modify firmware environment values | For the Enterprise Member Server, Member Server and Domain Controller profile(s), the recommended value is Administrators. For the Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.8.21 | Perform volume maintenance tasks | For the Member Server and Domain Controller profile(s), the recommended value is Administrators. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.8.22 | Profile single process | Administrators |
| 1.8.23 | Profile system performance | Administrators |
| 1.8.24 | Remove computer from docking station | Administrators |
| 1.8.25 | Replace a process level token | For all profiles, the recommended state for this setting is LOCAL SERVICE, NETWORK SERVICE. |
| 1.8.26 | Shut down the system | Administrators |
| 1.8.27 | Add workstations to domain | For the Enterprise Domain Controller and Domain Controller profile(s), the recommended value is Administrators. For the Enterprise Member Server and Member Server profile(s), the recommended value is Not Defined. |
| 1.8.28 | Allow log on locally | Administrators |
| 1.8.29 | Allow log on through Terminal Services | Do not disable; Limit via FW - Access via XXXX networks only |
| 1.8.30 | Change the time zone | For all profiles, the recommended state for this setting is LOCAL SERVICE, Administrators. |
| 1.8.31 | Create symbolic links | For the Member Server and Domain Controller profile(s), the recommended value is Administrators. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.8.32 | Deny log on locally | Guests |
| 1.8.33 | Deny log on through Terminal Services | Guests |
| 1.8.34 | Generate security audits | For the Enterprise Member Server, Member Server and Domain Controller profile(s), the recommended value is LOCAL SERVICE, NETWORK SERVICE.For the Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.8.35 | Increase a process working set | For the Member Server and Domain Controller profile(s), the recommended value is Administrators, Local Service.For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.8.36 | Log on as a batch job | For the Enterprise Domain Controller, Member Server and Domain Controller profile(s), the recommended value is No one.For the Enterprise Member Server profile(s), the recommended value is Not Defined. |
| 1.8.37 | Restore files and directories | For the Member Server and Domain Controller profile(s), the recommended value is Administrators.For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Administrators, Backup Operators. |
| 1.8.38 | Take ownership of files or other objects | Administrators |
| 1.8.39 | Access credential Manager as a trusted caller | No One |
| 1.8.40 | Synchronize directory service data | No One |

Security Options

|  |  |  |
| --- | --- | --- |
| **1.9** | **Security Options** | **Setting** |
| 1.9.1 | Network security: Minimum session security for NTLM SSP based (including secure RPC) servers | For all profiles, the recommended state for this setting is Require NTLMv2 session security, Require 128-bit encryption. |
| 1.9.2 | Network access: Remotely accessible registry paths and sub-paths | For the Member Server and Domain Controller profile(s), the recommended value is: 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 Other Domain Controller profile(s), are Not Defined. |
| 1.9.3 | Accounts: Rename administrator account | For all profiles, the recommended state for this setting is any value that does not contain the term "admin". |
| 1.9.4 | Accounts: Rename guest account | For all profiles, the recommended state for this setting is any value that does not contain the term "guest". |
| 1.9.5 | Accounts: Guest account status | Disabled |
| 1.9.6 | Network access: Allow anonymous SID/Name translation | Disabled |
| 1.9.7 | Accounts: Limit local account use of blank passwords to console logon only | Enabled |
| 1.9.8 | Devices: Allowed to format and eject removable media | Administrators |
| 1.9.9 | Devices: Prevent users from installing printer drivers | Enabled |
| 1.9.10 | Devices: Restrict CD-ROM access to locally logged-on user only | For the Member Server and Domain Controller profile(s), the recommended value is Enabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.9.11 | Devices: Restrict floppy access to locally logged-on user only | For the Member Server and Domain Controller profile(s), the recommended value is Enabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.9.12 | Domain member: Digitally encrypt or sign secure channel data (always) | Enabled |
| 1.9.13 | Domain member: Digitally encrypt secure channel data (when possible) | Enabled |
| 1.9.14 | Domain member: Digitally sign secure channel data (when possible) | Enabled |
| 1.9.15 | Domain member: Disable machine account password changes | Disabled |
| 1.9.16 | Domain member: Maximum machine account password age | For all profiles, the recommended state for this setting is 30 day(s). |
| 1.9.17 | Domain member: Require strong (Windows 2000 or later) session key | Enabled |
| 1.9.18 | Domain controller: Allow server operators to schedule tasks | For the Enterprise Domain Controller and Domain Controller profile(s), the recommended value is Disabled. For the Enterprise Member Server and Member Server profile(s), the recommended value is Not Defined. |
| 1.9.19 | Domain controller: LDAP server signing requirements | For the Domain Controller profile(s), the recommended value is Require signing. For the Enterprise Member Server, Enterprise Domain Controller and Member Server profile(s), the recommended value is Not Defined. |
| 1.9.20 | Domain controller: Refuse machine account password changes | For the Enterprise Domain Controller and Domain Controller profile(s), the recommended value is Disabled. For the Enterprise Member Server and Member Server profile(s), the recommended value is Not Defined. |
| 1.9.21 | Interactive logon: Do not display last user name | Enabled |
| 1.9.22 | Interactive logon: Do not require CTRL+ALT+DEL | Disabled |
| 1.9.23 | Interactive logon: Number of previous logons to cache (in case domain controller is not available) | For all profiles, the recommended state for this setting is 1 logon. |
| 1.9.24 | Interactive logon: Prompt user to change password before expiration | 14 days (see netid.XXXX.edu) |
| 1.9.25 | Interactive logon: Require Domain Controller authentication to unlock workstation | Enabled |
| 1.9.26 | Interactive logon: Smart card removal behavior | Lock Workstation |
| 1.9.27 | Omitted |  |
| 1.9.28 | Omitted |  |
| 1.9.29 | Interactive logon: Require smart card | For the Member Server and Domain Controller profile(s), the recommended value is Enabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.9.30 | Microsoft network client: Digitally sign communications (always) | Enabled |
| 1.9.31 | Microsoft network client: Digitally sign communications (if server agrees) | Enabled |
| 1.9.32 | Microsoft network client: Send unencrypted password to third-party SMB servers | Disabled |
| 1.9.33 | Microsoft network server: Amount of idle time required before suspending session | 10 minutes |
| 1.9.34 | Microsoft network server: Digitally sign communications (always) | Enabled |
| 1.9.35 | Microsoft network server: Digitally sign communications (if client agrees) | Enabled |
| 1.9.36 | Microsoft network server: Disconnect clients when logon hours expire | Disabled |
| 1.9.37 | Network access: Do not allow anonymous enumeration of SAM accounts | Enabled |
| 1.9.38 | Network access: Do not allow anonymous enumeration of SAM accounts and shares | Enabled |
| 1.9.39 | Network access: Do not allow storage of credentials or .NET Passports for network authentication | For the Member Server and Domain Controller profile(s), the recommended value is Enabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.9.40 | Network access: Let Everyone permissions apply to anonymous users | Disabled |
| 1.9.41 | Network access: Named Pipes that can be accessed anonymously | For the Member Server profile(s), the recommended value is browser. For the Domain Controller profile(s), the recommended value is: netlogon, lsarpc, samr, browser. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.9.42 | Network access: Remotely accessible registry paths | For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. For the Member Server and Domain Controller profile(s), the recommended value is: System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion |
| 1.9.43 | Network access: Restrict anonymous access to Named Pipes and Shares | Enabled |
| 1.9.44 | Network access: Shares that can be accessed anonymously | None |
| 1.9.45 | Network access: Sharing and security model for local accounts | For all profiles, the recommended state for this setting is Classic - local users authenticate as themselves. |
| 1.9.46 | Network security: Do not store LAN Manager hash value on next password change | Enabled |
| 1.9.47 | Network security: LAN Manager authentication level | For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Send NTLMv2 response only. Refuse LM. For the Member Server and Domain Controller profile(s), the recommended value is Send NTLMv2 response only. Refuse LM & NTLM. |
| 1.9.48 | Network security: LDAP client signing requirements | Negotiate signing |
| 1.9.49 | Network security: Minimum session security for NTLM SSP based (including secure RPC) clients | Require NTLMv2 session security, Require 128-bit encryption |
| 1.9.50 | Recovery console: Allow automatic administrative logon | Disabled |
| 1.9.51 | Recovery console: Allow floppy copy and access to all drives and all folders | For the Member Server and Domain Controller profile(s), the recommended value is Disabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.9.52 | Shutdown: Clear virtual memory pagefile | Disabled |
| 1.9.53 | Shutdown: Allow system to be shut down without having to log on | Disabled |
| 1.9.54 | System objects: Require case insensitivity for non-Windows subsystems | Enabled |
| 1.9.55 | System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links) | Enabled |
| 1.9.56 | System cryptography: Force strong key protection for user keys stored on the computer | For the Member Server and Domain Controller profile(s), the recommended value is User must enter a password each time they use a key. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is User is prompted when the key is first used. |
| 1.9.57 | System settings: Optional subsystems | None |
| 1.9.58 | System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies | For the Member Server and Domain Controller profile(s), the recommended value is Enabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.9.59 | MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended) | Disabled |
| 1.9.60 | MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) | For all profiles, the recommended state for this setting is Highest protection, source routing is completely disabled. |
| 1.9.61 | MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes | Disabled |
| 1.9.62 | MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds | For the Member Server and Domain Controller profile(s), the recommended value is 5 minutes. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.9.62 | MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds | For the Member Server and Domain Controller profile(s), the recommended value is 5 minutes. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.9.63 | MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic | For all profiles, the recommended state for this setting is Only ISAKMP is exempt (recommended for Windows Server 2003). |
| 1.9.64 | MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers | Enabled |
| 1.9.65 | MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames (recommended) | Enabled |
| 1.9.66 | MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) | Disabled |
| 1.9.67 | MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended) | Enabled |
| 1.9.68 | MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) | 0 |
| 1.9.69 | MSS: (TCPMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | 3 |
| 1.9.70 | MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning | 90% or less |
| 1.9.71 | MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) | For all profiles, the recommended state for this setting is Highest protection, source routing is completely disabled. |
| 1.9.72 | MSS: (TCPMaxDataRetransmissions) IPv6 How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | 3 |

Terminal Services

|  |  |  |
| --- | --- | --- |
| 1.10.1 | Always prompt client for password upon connection | Enabled |
| 1.10.2 | Set client connection encryption level | Enabled: High Level |
| 1.10.3 | Do not allow drive redirection | For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Configured. For the Member Server and Domain Controller profile(s), the recommended value is Enabled. |
| 1.10.4 | Do not allow passwords to be saved | Enabled |

Internet Communications

|  |  |  |
| --- | --- | --- |
| **1.11** | **Internet Communication** | **Setting** |
| 1.11.1 | Turn off downloading of print drivers over HTTP | Enabled |
| 1.11.2 | Turn off the "Publish to Web" task for files and folders | Enabled |
| 1.11.3 | Turn off Internet download for Web publishing and online ordering wizards | Enabled |
| 1.11.4 | Turn off printing over HTTP | Enabled |
| 1.11.5 | Turn off Search Companion content file updates | Enabled |
| 1.11.6 | Turn off the Windows Messenger Customer Experience Improvement Program | Enabled |
| 1.11.7 | Turn off Windows Update device driver searching | For the Member Server and Domain Controller profile(s), the recommended value is Enabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |

Additional Security Settings

|  |  |  |
| --- | --- | --- |
|  |  |  |
| 1.12.1 | Do not process the legacy run list | For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Configured. For the Member Server and Domain Controller profile(s), the recommended value is Enabled. |
| 1.12.2 | Do not process the run once list | For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Configured. For the Member Server and Domain Controller profile(s), the recommended value is Enabled. |
| 1.12.3 | Registry policy processing | For the Enterprise Member Server and Member Server profile(s), the recommended value is Enabled (Process even if the Group Policy objects have not changed). For the Enterprise Domain Controller and Domain Controller profile(s), the recommended value is Not Defined. |
| 1.12.4 | Offer Remote Assistance | For the Member Server and Domain Controller profile(s), the recommended value is Disabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.12.5 | Solicited Remote Assistance | For the Member Server and Domain Controller profile(s), the recommended value is Disabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.12.6 | Restrictions for Unauthenticated RPC clients | For the Member Server and Domain Controller profile(s), the recommended value is Enabled: Authenticated. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.12.7 | RPC Endpoint Mapper Client Authentication | For the Member Server and Domain Controller profile(s), the recommended value is Enabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. |
| 1.12.8 | Turn off Autoplay | Enabled: All drives |
| 1.12.9 | Enumerate administrator accounts on elevation | For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Configured. For the Member Server and Domain Controller profile(s), the recommended value is Disabled. |
| 1.12.10 | Require trusted path for credential entry | Enabled |
| 1.12.11 | Disable remote Desktop Sharing | Enabled |

# Standard Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Standard can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Standard. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| Review the configuration settings on the windows server | * Confirm from the standard if the configuration settings on the server are the same |

## Enforcement

All staff of XXXX must comply with all Information Security Standards. Failure to comply with these standards may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Standard statements described in this document must be reviewed and approved in accordance with the Exception Process defined in *XXXX-POL-ALL-001 - Information Security Policy Framework*

## Glossary / Acronyms

|  |  |
| --- | --- |
| syslog | System Log |
| FTP | File Transfer Protocol |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |

## Document Ownership

This Standard is owned by the YYYY

## Document Coordinator

This Standard is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |
|  |  |  |

## Document Distribution

* *Information Security*
* *IT Department*