UMZIMVUBU

LOCAL MUNICIPALITY

ICT SERVER BASELINE SECURITY POLICY

TABLE OF CONTENT

This policy outlines the steps you should take to improve the security of computers running Windows 2008 Server either on their own or as part of a Windows NT, or Windows 2008, or Windows Server 2003 domain. These steps apply to Windows 2008 Server and Windows 2008 Advanced Server.

1. PURPOSE

The purpose of this policy is to give instructions for configuring a baseline level of security with Windows 2008 Server computers. Security settings can be configured and applied to local servers through the Security Configuration Tool Set. Domain security policies can be created by using the Security Configuration Tool Set and distributed and applied through Group Policy. This guide outlines recommended security settings for Windows 2008.

This policy contains information about editing the registry. Before you edit the registry, make sure you understand how to restore it if a problem occurs. For information about how to do this, view the "Restoring the Registry" Help topic in Regedit.exe or the "Restoring a Registry Key" Help topic in Regedt32.exe.

2. WINDOWS 2008 SERVER R2

Windows 2008 Server Configuration Windows 2008 Server Configuration policy Details

WINDOWS 2008 SERVER CONFIGURATION

	Steps
☐	Verify that all disk partitions are formatted with NTFS
☐	Verify that the Administrator account has a strong password
☐	Disable unnecessary services
☐	Disable or delete unnecessary accounts
☐	Protect files and directories
☐	Make sure the Guest account is disabled
☐	Protect the registration from anonymous access
☐	Apply appropriate registry ACLs
☐	Restrict access to public Local Security Authority (LSA) information
☐	Set stronger password policies
☐	Set account lockout policy
☐	Configure the Administrator account
☐	Revoke the Debug programs user right
☐	Remove all unnecessary file shares
☐	Set appropriate ACLs on all necessary file shares
☐	Enable security event auditing
☐	Set log on warning message
☐	Install anti-virus software and updates
☐	Install service packs and critical patches
☐	Automate patch deployment
☐	Scan system with the Baseline Security Analyzer
☐	Additional security settings
☐	Install the latest Service Pack
☐	Install the appropriate post-Service Pack security hotfixes

3. Verify that all Disk Partitions are Formatted with NTFS

NTFS partitions offer access controls and protections that aren't available with the FAT, FAT32, or FAT32x file systems. Make sure that all partitions on your server are formatted using NTFS. If necessary, use the *convert* utility to non-destructively convert your FAT partitions to NTFS.

Warning: If you use the convert utility, it will set the ACLs for the converted drive to everyone: Full Control. Use the fixacls.exe utility from the Windows NT Server Resource Kit to reset them to more reasonable values.

4. Verify that the Administrator Account has a Strong Password

Windows 2008 allows passwords of up to 127 characters. In general, longer passwords are stronger than shorter ones, and passwords with several character types (letters, numbers, punctuation marks, and non-printing ASCII characters generated by using the ALT key and three-digit key codes on the numeric keypad) are stronger than alphabetic or alphanumeric-only passwords. For maximum protection, make sure the Administrator account password is at least nine characters long and that it includes at least one punctuation mark or non-printing ASCII character in the first seven characters. In addition, the Administrator account password should not be synchronized across multiple servers. Different passwords should be used on each server to raise the level of security in the workgroup or domain.

5. Disable Unnecessary Services

After installing Windows 2008 Server, you should disable any network services not required for the computer. In particular, you should consider disable the following services if possible:

5.1 (Internet Information Server) IIS services: FTP Publishing Service, IIS Admin Service, Network News Transport Protocol (NNTP), Simple Mail Transport Protocol (SMTP), and the World Wide Web Publishing Service.

5.2 Server service. Disable if server is not being used for file and print sharing.

5.3 SNMP service. Disable if SNMP monitoring is not required.

You should also avoid installing applications on the server unless they are absolutely necessary to the server's function. For example, don't install e-mail clients, office productivity tools, or utilities that are not strictly required for the server to do its job.

After installing Windows 2008 Server, you should disable any network services not required for the server role. In particular, you should consider whether your server needs any IIS components and whether it should be running the Server service for file and print sharing.

You should also avoid installing applications on the server unless they are absolutely necessary to the server's function. For example, don't install e-mail clients, office productivity tools, or utilities that are not strictly required for the server to do its job.

6. Disable or Delete Unnecessary Accounts

You should review the list of active accounts (for both users and applications) on the system in the Computer Management snap-in, and disable any non-active accounts, and delete accounts which are no longer required.

7. Protect Files and Directories

Clean-installed Windows 2008 systems have secure default ACLs on the file system. However, upgrades from previous versions (e.g., Windows NT 4.0) do not modify the previous security settings and should have the default Windows 2008 settings applied.

8. Make Sure the Guest Account is Disabled

By default, the Guest account is disabled on systems running Windows 2008 Server. If the Guest account is enabled, disable it.

9. Protect the Registry from Anonymous Access

The default permissions do not restrict remote access to the registry. Only administrators should have remote access to the registry, because the Windows 2008 registry editing tools support remote access by default. To restrict network access to the registry:

9.1 Add the following key to the registry:

Hive	HKEY_LOCAL_MACHINE \SYSTEM
Key	\CurrentControlSet\Control\SecurePipeServers
Value Name	\winreg

9.2 Select winreg, click the Security menu, and then click Permissions.

9.3 Set the Administrators permission to Full Control, make sure no other users or groups are listed, and then click OK.

The security permissions (ACLs) set on this key defines which users or groups can connect to the system for remote registry access. In addition, the AllowedPaths subkey contains a list of keys to which members of the Everyone group have access, notwithstanding the ACLs on the winreg key. This allows specific system functions, such as checking printer status, to work correctly regardless of how access is restricted via the winreg registry key. The default security on the AllowedPaths registry key grants only

Administrators the ability to manage these paths. The AllowedPaths key, and its proper use, is documented in Microsoft Knowledge Base article 153183.

10. Apply Appropriate Registry ACLs

Clean-installed Windows 2008 systems have secure default ACLs on the registry. However, upgrades from previous versions (e.g., Windows NT 4.0) do not modify the previous security settings and should have the default Windows 2008 settings applied. Refer to Default Access Control Settings in Windows 2008 document on the Microsoft TechNet Security Web site for details on about the default Windows 2008 registry ACLs and how to make any necessary modifications.

11. Restrict Access to Public Local Security Authority (LSA) Information

You need to be able to identify all users on your system. Therefore, you should restrict anonymous users so that the amount of public information they can obtain about the LSA component of the Windows NT Security Subsystem is reduced. The LSA handles aspects of security administration on the local computer, including access and permissions. To implement this restriction, create and set the following registry entry:

Hive	HKEY_LOCAL_MACHINE \SYSTEM
Key	CurrentControlSet\Control\LSA
Value Name	RestrictAnonymous
Type	REG_DWORD
Value	1

12. Set Stronger Password Policies

Use the Domain Security Policy (or Local Security Policy) snap-in to strengthen the system policies for password acceptance. Microsoft suggests that you make the following changes:

12.1 Set the minimum password length to at least 8 characters. Recommended value: 8.

12.2 Set a minimum password age appropriate to your network (typically between 1 and 7 days). Recommended value: 2.

12.3 Set a maximum password age appropriate to your network (typically no more than 42 days). Recommended value: 42.

12.4 Set a password history maintenance (using the "**Remember passwords**" option) of at least 6. Recommended value: 24.

12.5 Set a password complexity requirement (using the **Passwords must meet complexity requirements** option.

12.6 Disable the **Store passwords using reversible encryption** option (disabled by default).

13. Set Account Lockout Policy

Windows 2008 includes an account lockout feature that will disable an account after an administrator-specified number of logon failures. This decreases the risk of an attacker using a brute-force method to identify valid login credentials by trying a large number of possible passwords. However, it creates a denial-of-service vulnerability: an attacker could cause accounts to be locked out, causing legitimate users to be denied access.

The recommended configuration settings for maximum security against brute force attacks that compromise user credentials are: enable lockout after 3three to 5five failed attempts, reset the count after not less than 30 minutes, and set the lockout duration to 30 minutes. The recommended configuration for maximum security against denial of service attacks is to disable account lockout entirely.

Windows 2008 includes an account lockout feature that will disable an account after an administrator-specified number of logon failures. For maximum security, enable lockout after 3 to 5 failed attempts, reset the count after not less than 30 minutes, and set the lockout duration to "Forever (until admin unlocks)."

The Windows NT Server Resource Kit includes a tool that allows you to adjust some account properties that aren't accessible through the normal management tools. This tool, passprop.exe, allows you to lock out the administrator account:

- The */adminlockout* switch allows the administrator account to be locked out

14. Configure the Administrator Account

Because the Administrator account is built in to every copy of Windows 2008, it presents a well-known objective for attackers. To make it more difficult to attack the Administrator account, do the following both for the domain Administrator account and the local Administrator account on each server:

14.1 Rename the account to a nonobvious name (e.g., not "admin," "root," etc.).

14.2 Establish a decoy account named "Administrator" with no privileges. Scan the event log regularly looking for attempts to use this account.

14.3 Enable account lockout on the real Administrator accounts by using the pass prop utility

14.4 Disable the local computer's Administrator account.

15. Revoke the Debug Programs User Right

By default, Windows 2008 grants administrators the **Debug programs** user right. This right can be exploited by Trojans to capture sensitive system information from the system memory, such as hashed passwords. Microsoft suggests that you revoke this right for all users except specific user accounts that require debug privileges

16. Remove all Unnecessary File Shares

All unnecessary file shares on the system should be removed to prevent possible information disclosure and to prevent malicious users from using the shares as an entry to the local system.

17. Set Appropriate ACLs on all Necessary File Shares

By default all users have Full Control permissions on newly created file shares All shares that are required on the system should have the ACL restricted such that users have the appropriate share-level access (e.g., Everyone = Read).. All shares that are required on the system should be ACL'd such that users have the appropriate share-level access (e.g., Everyone = Read).

Note: The NTFS file system must be used to set ACLs on individual files in addition to share-level permissions.

18. Enable Security Event Auditing

By default, Windows 2008 server does not log successful or failed login attempts. Logging these attempts is useful for proactively determining that an attack is occurring, and reactively determining how and when an attack took place. It is tempting to enable all types of auditing; however, that configuration results in unmanageable log files and a performance impact. Microsoft recommends enabling only **Success** and **Failure** auditing for the **Audit account logon events** policy.

With auditing enabled, event log size and retention policies should be adjusted. The size of all event logs should be set so that they can retain several weeks of events. Microsoft recommends the maximum security log size be set to a value of 184,320 KB,; the maximum application log size be set to 10,240 KB,; and the maximum system log size to 10,240 KB. For all event logs, set the retention method for event logs to **Overwrite events as needed**.

19. Set Log on Warning Message

Though setting a log on warning message does not technically restrict an attacker, it significantly increases an organization's ability to prosecute attacks. Not displaying a warning message reduces the liability assumed by an attacker, which can increase an attackers comfort when initiating attacks. The specific wording of the message should be provided by your legal counsel; however, Microsoft recommends the following:

19.1 Set **Message text for users attempting to log on** to the following message value: This system is restricted to authorized users. Individuals attempting unauthorized access will be prosecuted. If unauthorized, terminate access now! Clicking on OK indicates your acceptance of the information in the background.

19.2 Set **Message title for users attempting to log on** to: IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORIZATION.

20. Install Antivirus Software and Updates

It is imperative to install antivirus software and keep up-to-date on the latest virus signatures on all Internet and intranet systems.

21. Install Service Packs and Critical Patches

From time to time, Microsoft releases service packs and critical updates to resolve newly discovered security vulnerabilities in components included with Windows 2008. The Microsoft Update site is a tool for identifying critical updates not specifically identified in this document.

Apply all service packs and critical updates listed for your system at the Microsoft Update site. Microsoft Update may not be able to apply all critical updates at one time. If necessary, return to the site after rebooting the system and repeat the above process until all critical updates and service packs have been applied.

Each Service Pack for Windows includes all security fixes from previous Service Packs. Microsoft recommends that you keep up-to-date on Service Pack releases and install the correct Service Pack for your servers as soon as your operational circumstances allow. The current Service Pack for Windows 2008, SP2, is available on the Microsoft Web site.

Service Packs are also available through Microsoft Product Support. Information about contacting Microsoft Product Support is available on the Microsoft Web site.

22. Install the Appropriate Post-Service Pack Security Hotfixes Automate Patch Deployment

Use Automatic Updates to automatically notify you of the availability of new security fixes. If possible, configure Automatic Updates to automatically download updates and install then without manual intervention. Microsoft issues security bulletins through its Security Notification Service. When these bulletins recommend installation of a security hotfix, you should immediately download and install the hotfix on your member servers.

Larger organizations should use Microsoft Software Update Services, Microsoft Systems Management Server, or a similar solution to reduce the labor associated with deploying patches.

23. Scan System with the Baseline Security Analyzer

The Baseline Security Analyzer (BSA) evaluates your system's configurations and provides a report with specific recommendations to improve the security. BSA will recommend missing hotfixes and configuration changes related to both the core operating system and optional services such as Internet Information ServerIIS, SQL Server, and Internet Explorer. Use BSA to identify vulnerabilities in your systems initial configuration, and run it regularly to find new vulnerabilities.

When you run the Baseline Security Analyzer BSA after installing the security baseline described above, the BSA results will show many security fixes are not installed. This is true and expected. The document only provides only a baseline from which to start. It is recommended you take the necessary steps to ensure all the critical security patches are installed.

You should run this tool against all the computers that you are securing on a daily basis until you are confident that all the recommended fixes have been applied. You can lower the frequency, but should continue to check regularly to detect fixes that have been uninstalled or overwritten. As you deploy new security fixes, you should continue to run the tool to verify and detect missing security patches.

1. COMMENCEMENT OF THE POLICY

a) The policy will come into effect on the date signed by ICT Governance Champion

1.1. INTERPRETATION OF THE POLICY

a) All words contained in this policy shall have the ordinary meaning attached thereto, unless the definition or context indicates otherwise
b) Any dispute on interpretation of this policy shall be declared in writing by any party concerned.
c) The Municipal Manager shall give a final interpretation of this policy in case of written dispute.
d) If the party concerned is not satisfied with the interpretation, a dispute may then be pursued with the South African Local Government Bargaining Council.

1.2. PERMANENT/TEMPORAL WAIVER OR SUSPENSION OF THE POLICY

a) This policy may be partly or wholly waived or suspended by the ICT Governance Champion on temporary or permanent basis however the Municipal

Manager/Council may under circumstances of emergency temporarily waive this policy subject to reporting of such waiver or suspension to Council.

2. COMPLIANCE

a. Senior management is required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.
b. Failure to comply with this policy may result in disciplinary action, which may include termination of employment.
c. Any conduct that interferes with the normal and proper operation of the municipality's IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved IT policies.
d. The municipality management reserves the right to revoke the privileges of any user at any time

3. AMENDMENT AND/OR ABOLITION OF THIS POLICY

a) This policy may be amended or repealed by ICT Governance Champion**/** Council as it may deem necessary.

4. Document Owner and Approval

The Municipality is the owner of this document. The Executive Management of the Municipality is responsible for ensuring that this policy document is reviewed regularly to ensure that it remains relevant to the organisation.

This document was approved by the Executive Management and is issued on a version controlled basis under the signature of the ICT Governance Champion.

Every page of this document must also be initialled by the Governance Champion.