Idaho Technology Authority (ITA)

ENTERPRISE GUIDELINES – G590 SECURITY PROCEDURES

Category: G590A – Server Operating System; Initial Security Requirements

---

CONTENTS:

I. DEFINITION

Gold Disk – A CD-ROM provided by the Defense Information Systems Agency (DISA) to evaluate the security posture of servers. The Gold Disk also evaluates services such as Internet Information Service (IIS) and Structured Query Language (SQL) services.

Web Server – System that hosts content published for the world-wide web.

DMZ – Area of the state network that separates the public outside network from the internal private network.

VMS – DISA's Vulnerability Management System

II. RATIONALE

The purpose of this guideline is to provide a security baseline for State of Idaho server administrators to use in hardening their servers. The parameters in this guideline are widely accepted by the global security community as prudent and effective. Each of the items in the guideline can be implemented using Microsoft Active Directory Group Policy or the Local Security Policy.

III. GUIDELINE

This is the first guideline in the G590 series and it addresses an initial hardening of the Windows Server 2003 Operating System. This guideline is to be implemented to better secure all state-owned Windows Server 2003 servers overtime in accordance with ITA Standard, S3230. Reporting from all agencies on this will be in accomplished via the form shown below. The initial report is due six months after this Guideline is approved

and an annual report is due every year to be turned in with each agency's annual IT plan.

G590A – Server Operating System; Initial Security Requirements Initial Report													
Agency:							IT Point of Contact:						
Questions													Yes (Y) or No (N)
1. Does your agency have public facing servers on the State's network?													
2. If yes, are any of these outside the enterprise DMZ?													
3. Do you regularly apply security patches to your server(s)? If not, please explain below.													
4. Do you have a process to monitor which patches have been applied to servers? If not, please explain below.													
5. The Defense Information Systems Agency has a "Gold Disk" program which will identify vulnerabilities on servers. The Office of IT Services (ITS) Security Team is making this available to agencies. Do you have a DISA "Gold Disk"?													
6. Would you like training using the DISA Gold Disk?													
Results of Gold Disk evaluation – Initial and Annual Report													
Tier of Server	Use Gold Disk?	Comply w/ G590A?	A	B	C	D	E	F	G	H	I	Explain any non-compliance	Comments
1	(Y or N)	(Y or N)											
2													
3													
4													

IV. Procedure Reference

A. Virus Scan Program

B. Restrict Anonymous Network Shares

C. User Rights – Act as part of operating system

D. Disable Administrator Automatic Logon

E. Deny Access from the Network

F. Disable Media Autoplay

G. Password Policy

H. Account Lockout

I. Rename Administrator Account

A. Virus Scan Program

1. **VMS 6 ID:** V0001074

2. **Details:** N/A

3. **Description:** This is a Phase 1 finding because virus scan programs are a primary line of defense against the introduction of viruses and malicious code that can destroy data and even render a computer inoperable. Utilizing the most current virus scan program provides the ability to detect this malicious code before extensive damage occurs. Updated virus scan data files can help protect a system, because new viruses are identified by the software vendors on a regular basis.

4. **Automatic Check:** Gold Disk V2

5. **Manual Fix:** Configure the system with a reputable antivirus solution.

6. **References and additional information:** Idaho Technology Authority (ITA) Standard – An ITA standard does not exists for server antivirus applications.

B. Restrict Anonymous Network Shares

1. **VMS 6 ID:** V0001093

2. **Details:** The registry value of System\CurrentControlSet\Control\Lsa\RestrictAnonymous should equal 1.

3. **Description:** This is a Phase 1 finding because it allows anonymous logon users (null session connections) to list all account names and enumerate all shared resources, thus providing a map of potential points to attack the system. By default, Windows allows anonymous users to list account names and enumerate share names.

4. **Automatic Check:** Gold Disk V2

5. **Manual Fix:** Edit the local computer policy or GPO - Computer Configuration -> Windows Settings -> Local Policies -> Security Options -> Network access: Do not allow anonymous enumeration of SAM accounts.

   If the value for “Network access: Do not allow anonymous enumeration of SAM accounts and shares” is not set to “Enabled”, then this is a finding.

6. **References and additional information:**
   a) Microsoft Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP -V2.0, Chap 5, p. 90-92
   b) Microsoft Windows Vista Security Guide -Appendix A, p. 48 Microsoft Windows Server 2008 Security Guide -Appendix A, pp. 42 – 46

C. User Rights – Act as part of operating system

1. **VMS 6 ID:** V0001102

2. **Details:** Edit the local computer policy or GPO - Computer Configuration -> Windows Settings -> Local Policies -> User Rights Assignment -> Act as part of operating system.

3. If any user accounts or groups (to include administrators) are granted this right, then this is a finding.

4. **Description:** This is a Phase 1 finding because users and user groups that are assigned this right can bypass all security protective mechanisms that apply to all users, including administrators.

   Some applications require this right to function. Exceptions need to be documented.

5. **Automatic Check:** Gold Disk v2

6. **Manual Fix:** Configure the system to prevent unauthorized users to "Act as part of the operating system".

7. **References and additional information:**
   a) MS Windows 2003/XP Threats and Countermeasures Guide V2.0, Chap 4, p. 34-35
   b) DISA Windows 2003/XP/2000/Vista Addendum, V6.1, Section 5

D. Disable Administrator Automatic Logon

1. **VMS 6 ID :** V0001145

2. **Details:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\DefaultUserName. If this key exists, this is a finding.

3. **Description:** This is a Phase 1 finding because it will directly log on to the system with administrator privileges when the machine is rebooted. This would give full access to any unauthorized individual who reboots the computer.

   By default this setting is not enabled. If this setting exists, it should be disabled. If this capability exists, the default password will also be present in the registry, and must be removed.

4. **Automatic Check:** Gold Disk V2

5. **Manual Fix:** Configure the system to disable automatic administrator logon.

6. **References and additional information:**

E. Deny Access from the Network

1. **VMS 6 ID:** V0001155

2. **Details:** Edit the local computer policy or GPO - Computer Configuration -> Windows Settings -> Local Policies -> User Rights Assignment -> Deny access to this computer from the network

3. Account: Guest, ANONYMOUS LOGON, built-in local Administrator account, built-in support accounts, all service accounts

4. **Description:** This is a Phase 1 finding because allowing network logins by the built-in guest accounts, which are a member of the Everyone group and Guests group, with all the rights and permissions associated with that group, could provide anonymous access to system resources to unauthorized users. Anonymous Logon and Support_388945a0 are also included in applicable Windows versions.

5. **Automatic Check:** Gold Disk V2

6. **Manual Fix:** Configure the system to give the right "Deny access to this computer from the network" to the Accounts/Groups specified in the Manual Check.

7. **References and additional information:**
   a) Microsoft Windows Server 2008 Security Guide -Appendix A, pp. 9 -21
   b) Microsoft Windows Vista Security Guide -Appendix A, p. 22
   c) Microsoft Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP -V2.0, Chap 4, p. 43-44
   d) Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set ¬Chapter 4, p. 31-35

F. Disable Media Autoplay

1. **VMS 6 ID:** V0002374

2. **Details:** Registry Key-SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun does not exist.

3. **Description:** Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the music on audio media starts immediately. By default, Autoplay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives. If you enable this policy, you can also disable Autoplay on all drives.

4. **Automatic Check:** Gold Disk V2

5. **Manual Fix:** Configure the policy value for Computer Configuration /Administrative Templates/System/ “Turn off AutoPlay” to “Enabled:All Drives”.

   Note: This was previously configured in the checklist using the Security Option setting “MSS: (NoDriveTypeAutorun) Disable Autorun on all drives” set to “255, disable Autorun for all drives”. This updates the same registry value (NoDriveTypeAutorun) as the Administrative Template setting.

   In addition to the above, Microsoft has released patches to correct issues with this setting. The patches from either Microsoft’s KB953252 (patch KB950582) or KB967715 must be installed. This will add the HonorAutorunSetting registry value and update the file referenced in the Check section.

6. **References and additional information:**

G. Password Policy

1. **VMS 6 ID :** V0001104, 0001105, 0001107, V0001150, V0006836

2. **Details:** Edit the local computer policy or GPO - Computer Configuration -> Windows Settings -> Account Policies ->
    - If the value for “Enforce password history” is less than 24 passwords, then this is a finding.
    - If the value for the “Maximum password age” is greater than 90 days, then this is a finding. If the value is set to 0 (never expires), then this is a finding.
    - If the value for the “Minimum password age” is less than one day, then this is a finding.
    - If the value for the “Minimum password length” is less than “8” characters, then this is a finding.
    - If the value “Password must meet complexity requirements” is not “Enabled”, then this would be a finding.

3. **Automatic Check:** Gold Disk V2

4. **Manual Fix:** This check verifies that the system’s password policy conforms to State standards. Open a Microsoft Management Console Security Configuration or Group Policy:
    a) Expand the “Security Configuration and Analysis” object in the tree window.
    b) Expand the “Account Policies” object and select “Password Policy”.

5. **References and additional information:**
    a) Microsoft Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP - V2.0, Chap. 2, p. 10
    b) Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set - Chap. 3, p. 24
    c) Guide to Securing Microsoft Windows NT Networks - Chap. 5, p. 30
    d) Microsoft Windows Server 2008 Security Guide - Appendix A, pp. 3 - 5
    e) Microsoft Windows Vista Security Guide - Appendix A, p. 3-4

H. Account Lockout

1. **VMS 6 ID:** V0001099, V0001097, V0001098

2. **Details:**
    a) If the “Account lockout duration” is not set to ‘0’, requiring an administrator to unlock the account then this is a finding.
    b) If the “Account lockout threshold” is “0” or more than three attempts, then this is a finding.
    c) If the “Reset account lockout counter after” value is less than 60 minutes, then this is a finding

3. **Automatic Check:** Gold Disk V2

4. **Manual Fix:** This check verifies that the system’s account lockout policy conforms to DISA standards.
    a) Expand the “Security Configuration and Analysis” object in the tree window.
    b) Expand the “Account Policies” object and select “Account Lockout Policy”.

5. **References and additional information:**
    a) Microsoft Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP - V2.0, Chap. 2, p. 15
    b) Guide to Securing Microsoft Windows NT Networks - Chap. 5, p. 32
    c) Microsoft Windows Server 2008 Security Guide - Appendix A, pp. 5 - 8 JTF-GNO Communications Tasking Order (CTO) - 07-015
    d) Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set - Chap. 3, p. 27
    e) Microsoft Windows Vista Security Guide - Appendix A, p. 6

I. Rename Administrator Account

1. **VMS 6 ID:** V0001115

2. **Details:** The built-in administrator account has not been renamed.

3. **Description:** The built-in administrator account is a known account that can be initialized with a blank password during the basic installation. This vulnerability can allow easy access to the system by unauthorized users. Renaming this account to an unidentified name improves the protection of this account and the system.

4. **Automatic Check:** Gold Disk V2

5. **Manual Fix:**
   - Configure the system to rename the Administrator account.
   - Expand the Security Configuration and Analysis tree view.
   - Navigate to Local Policies - Security Options.
   - If the value for “Accounts: Rename administrator account” is not set to a value other than “Administrator”, then this is a finding.

6. **References and additional information:**

   1. Microsoft Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP - V2.0, Chap 5, p. 63-64, Chap 11, p. 297

IV. PROCEDURE REFERENCE

ITA Standard *S3230 – Security – Server Security Requirements* specifies the requirement to follow this guideline.

V. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 605-4064.

REVISION HISTORY

07/01/2018 – Changed “OCIO” to “ITS”.

07/01/2013 – Changed “ITRMC” to “ITA”.

Approved by ITRMC June 23, 2010