Idaho Technology Authority (ITA)

ENTERPRISE GUIDELINES G590 – SECURITY PROCEDURES

Category: G590B – PUBLIC-FACING SQL SERVER SETUP

CONTENTS:

I. DEFINITIONS

A. SQL Server – Sequential Query Language system also referred to as a Database Server.

B. Public-Facing (or DMZ) – Area of the state network that separates the public outside network from the internal private network.

II. RATIONALE

The purpose of this guideline is to provide a security baseline for State of Idaho server administrators to use in hardening their SQL servers. The parameters in this guideline are widely accepted by the global security community as prudent and effective.

III. GUIDELINE

This guideline is part of the G590 series and it addresses hardening of the SQL server environments. Implementing this guideline will better secure all state-used SQL servers in accordance with *ITA Enterprise Standard S3230 – Server Security Requirements*.

IV. PROCEDURE REFERENCE

The following pages will address best practices for these procedures:

A. SQL Server Versions.
B. SQL Server and Web Server on Different Servers.
C. Install only components and Features that will be immediately needed.
D. SQL Service Accounts.
E. Auditing.
F. Registry Keys.
G. Server Role Security.
H. Data Storage Security.
I. SA Account Security.
J. Password Policy.
K. Windows Authenticated and SQL Server Authenticated.
L. Encrypted Connections.
M. Network Connectivity.
N. Microsoft Baseline Security Analyzer and SQL Server Best Practices Analyzer.

A. SQL Server Versions.

1. **Summary:** Upgrade to the latest major version of SQL, if possible. Install approved service pack and patches. Consider testing new service packs and patches on development servers before installing on production servers.

2. **Details:** New versions contain security improvements. Security patches help fix and prevent published and known security flaws. Newer versions of SQL are normally backwards compatible but need testing before upgrading production databases. Check software license agreements before upgrading.

3. **Solution:** New versions of SQL usually require a reboot. Occasionally, patches will require a reboot.

4. **References:**

   a. Microsoft Server 2005 Security Best Practices – Operational and Administrative Tasks p. 29 http://msdn.microsoft.com/en-us/sqlserver/bb895845

   b. Security best practices checklist (Latest version and service pack) http://technet.microsoft.com/en-us/library/cc966456.aspx

B. SQL Server and Web Server on Different Servers

1. **Summary:** Never install SQL Server on a Web Server. Apply all service packs and patches immediately following the initial installation. Recommend not using server running SQL to browse the Internet.

2. **Details:** Web servers may be directly accessible to the public, which makes them more vulnerable to hacking. If SQL server is installed on a web server and the web server is compromised, all of the data on that server is compromised. Impersonation and delegation policies do not apply on the same server. Visiting infected websites is a primary source of malware. Browsing from the server may expose server to malware.

3. **Solution:** Whenever possible, do not install SQL Server and Web Server on the same hardware. If separation is not possible, keep confidential information out of SQL databases. Replicate only required information from internal SQL servers to your externally available SQL/WEB server. Download patches and fixes from workstations, then transfer to the server and apply.

4. **References**:

   a. Microsoft Server 2005 Security Best Practices – Operational and Administrative Tasks p. 10-13 http://msdn.microsoft.com/en-us/sqlserver/bb895845

   b. Security considerations for a SQL Server Installation (Enhance Physical Security http://msdn.microsoft.com/en-us/library/ms144228.aspx

C. Install Only Components and Features that will be immediately needed.

1. **Summary:** Installing only the components that you will immediately use. Additional components can always be installed as needed. Disable or leave disabled optional features unless absolutely necessary.

2. **Details:** Every service and feature has its own vulnerabilities. Limiting exposure also limits the possibility of a compromise against the vulnerabilities.

3. **Solution:** Do not install these components unless they will be used:

   - SQL Server Integration Services (SSIS)
   - SQL Server Analysis Services (SSAS)
   - SQL Server Reporting Services (SSRS)
   - Notification Services

   Consider disabling or leaving disabled these features
   - xp_cmdshell -
   - Remote Procedure Call (RPC)
   - OLE Automation Calls (sp_OA* stored procedures) – SP_Config
   - Common Language Runtime (CLR)

4. **References:**

   a. Microsoft Server 2005 Security Best Practices – Operational and Administrative Tasks p. 4-6 http://msdn.microsoft.com/en-us/sqlserver/bb895845

   b. SQL Server Security 2008 Security Overview for Database Administrators – white paper - Surface area configuration (Secure by default) http://www.microsoft.com/sqlserver/2008/en/us/wp-sql-2008-security.aspx

D. SQL Service Accounts

1. **Summary:** The SQL Service Account should not be a member of the Domain Administrators group and should only have the minimum privileges needed.

2. **Details:** If the SQL Service Account is a Domain Administrator, then any sysadmin essentially becomes a Domain Administrator and will be able to exec scripts under this account. If the service account became compromised then the domain becomes compromised.

3. **Solution:** Create a SQL Service Account with Local Administrative privileges to only one server. Additional SQL installations should use separate Service Accounts.

4. **References:**

   a. Microsoft Server 2005 Security Best Practices – Operational and Administrative Tasks p. 6-8 http://msdn.microsoft.com/en-us/sqlserver/bb895845

   b. Security Considerations for a SQL service installation (Isolate services) http://msdn.microsoft.com/en-US/library/ms144228

E. Auditing.

1. **Summary:** Enable SQL Server login auditing. Monitor Windows Event Viewer and SQL Server logs for unsuccessful login attempts.

2. **Details:** Unsuccessful logs should be monitored in order to identify hacking attempts or unauthorized application access.

3. **Solution:** To enable SQL Auditing start SQL Server management Studio, right click on the server, select Properties/Security and under Login Auditing – click on the button 'Failed logins only'.

4. **References:**

   a. Microsoft Server 2005 Security Best Practices – Operational and Administrative Tasks p. 27-29 http://msdn.microsoft.com/en-us/sqlserver/bb895845

   b. Overview of the SQL Server Security Model and Security Best Practices http://www.sql-server-performance.com/articles/dba/sql_security_p4.aspx

   c. Security Administration (Auditing) http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v

F. Registry Keys.

1. **Summary:** Secure SQL specific registry keys by group policy.

2. **Details:** Prevent local administrators from modifying SQL settings, such as Windows/Mixed mode, by securing the SQL registry keys.

3. **Solution:** Go to HKLM|Software|Microsoft|Microsoft SQL Server Permssions Advanced. If physical control is outside your group, you may want to add [Domain]\Domain Admins as a group, granting them Full Control.

   If INHERITABLE Permissions is checked, Select Replace Permission Entries….and Apply.

   Double Click Administrators. Unslect all permissions under the ALLOW column and Apply.

4. References:

a. Security Administration (Registry Security) https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44ver2.pdf

b. Group Policy Security Settings – Registry Policies http://technet.microsoft.com/en-us/library/cc960657.aspx

G. Server Role Security.

1. **Summary:** Remove built-in-Administrators windows groups from the SQL sysadmin Server Role. Add only Database Administrators and SQL Service Account to the sysadmin role.

2. **Details:** Isolate SQL Server access from local admins. Prevents access from other low level services running under built in admin accounts.

3. **Solution:** Open SQL Server Management Studio. Go to Security. Go to Server Roles. Open sysadmin. Remove BUILTIN\Administrators.

4. **References:**

   a. Security Administration (Server Role Security) https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44ver2.pdf

   b. Security Best Practices Checklist (Secure Operation) – Administrator Reduction http://technet.microsoft.com/en-us/library/cc966456.aspx

H. Data Storage Security

1. **Summary:** The SQL Server database data storage needs to be secured including live databases, database copies, and backup files.

2. **Details:** Data storage files need to be secured in order to protect against data theft from stealing or loss of physical hardware. Developers should not make local database copies on their work stations unless they follow the security standards.

3. **Solution:** Secure data storage files by implementing any of the following.

   Secured physical location

   Encrypting data backups

   Bitlocker or equivalent for hard drive media encrypting

4. **References:**

   a. Security Considerations for Backup and Restore (SQL Server) http://technet.microsoft.com/en-us/library/ms190964(SQL.100).aspx

   b. Security Best Practices Checklist (Secure Operation) – Administrator Reduction http://technet.microsoft.com/en-us/library/cc966456.aspx

   c. Securing SQL Server (Physical Security) http://msdn.microsoft.com/en-us/library/bb283235.aspx

I. SA Account Security.

1. **Summary:** The SA account should be renamed and used only for emergency administrative functions.

2. **Details:** The SA account is a common target for hacking. Renaming the SA account makes it more difficult exploit.

3. **Solution:** Execute SQL alter login script. ALTER LOGIN sa WITH NAME = [sa_newname]:

4. **References:**

   a. Security Administration (SA Accounts) http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v

   b. SQL Server Best Practices Article (Disabling or Renaming the Built-in SA Account http://technet.microsoft.com/en-us/library/cc966485.aspx

J. Password Policy.

1. **Summary:** Mandate a strong password policy for all accounts. Enforce local network password policy and enable “Enforce Password Policy” on all user accounts:

2. **Details:** Integrated, automatically requires local network password policy. SQL account should manually enforce the local network policy.

3. **Solution:** When creating accounts… Click “Enforce password Policy”

4. **References:**

   a. Microsoft Server 2005 Security Best Practices – Operational and Administrative Tasks p. 14 http://msdn.microsoft.com/en-us/sqlserver/bb895845

   b. SQL Server Security 2008 Security Overview for Database Administrators – white paper – Password Policy Enforcement p. 4 http://www.microsoft.com/sqlserver/2008/en/us/wp-sql-2008-security.aspx

   c. Security best practices checklist (Strong Passwords) http://technet.microsoft.com/en-us/library/cc966456.aspx

K. Windows Authenticated and SQL Server Authentication.

1. **Summary:** Use Windows authentication whenever possible.

2. **Details:** SQL Authentication transmits unsecured login passwords across the network unless network traffic is encrypted. Only Dot Net 2.0 and above applications can use windows authentication. Some programs like DotNetNuke may not be able to use Windows Authentication.

3. **Solution:** Set authentication mode to mixed mode during installation. This mode can be changed later if needed.

4. **References:**

   a. Checklist for Security best practices – Best practices for SQL Server http://technet.microsoft.com/en-us/library/bb735870.aspx

   b. Microsoft Server 2005 Security Best Practices – Operational and Administrative Tasks p. 9 http://msdn.microsoft.com/en-us/sqlserver/bb895845

   c. Security Administration (Authentication) https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44ver2.pdf

L. Encrypted Connections.

1. **Summary:** Applications and users connecting to SQL should use Encrypted Connections.

2. **Details:** This will encrypt traffic sent across the network and prevent man-in-the-middle attacks from occurring. If possible, enable "Forced Encryption" for the server.

3. **Solution:** A trusted certificate authority should be used rather than SQL Server self-signed certificates.

4. **References:**

   a. Microsoft Server 2005 Security Best Practices – Operational and Administrative Tasks p. 13 http://msdn.microsoft.com/en-us/sqlserver/bb895845

   b. Security Administration (Network Security) https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44ver2.pdf

M. Network Connectivity.

5. **Summary:** Enable only network protocols that are needed. Disable Named Pipes.

6. **Details:** Each protocol has its own vulnerability. Limiting protocols reduces the number of possible vulnerabilities.

7. **Solution:** Use SQL Server Configuration Manager to modify SQL Server Network Configuration protocols. Enable TCP/IP and disable others if not needed.

8. **References:**

   a. Microsoft Server 2005 Security Best Practices – Operational and Administrative Tasks p. 13 http://msdn.microsoft.com/en-us/sqlserver/bb895845

   b. Best-Practices for Administering Network and Sharing Center http://technet.microsoft.com/en-us/library/cc732044(WS.10).aspx

N. Microsoft Baseline Security Analyzer and SQL Server Best Practices Analyzer.

9. **Summary:** Run Baseline Security Analyzer periodically to scan for common insecurities in the SQL Server configuration.

10. **Details:** Microsoft Analyzers offer a quick review of vulnerable services and features.

11. **Solution:** Install and run periodically, at least once per year.

12. **References:**

    a. Microsoft Server 2005 Security Best Practices – Operational and Administrative Tasks p. 29 http://msdn.microsoft.com/en-us/sqlserver/bb895845
    b. Security best practices Checklist (Recommended Periodic Administrative Procedures) – Microsoft baseline Security Analyzer http://technet.microsoft.com/en-us/library/cc966456.aspx

V. REFERENCE DOCUMENTS

In addition to this guideline, the following documents apply:

A. *ITA Enterprise Standard S3230 – Server Security Requirements*

B. *ITA Enterprise Guideline G590A – Server Operating System*

C. *ITA Enterprise Guideline G590C – Public-Facing Web Server Setup*

VI. CONTACT INFORMATION

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

VII. REVIEW CYCLE

Twelve (12) months

VIII. TIMELINE

Date Established:	April 27, 2011
Last Reviewed:	
Last Revised:	
Last ITRMC Approval:	April 27, 2011

IX. REVISION HISTORY

07/23/25 - Revised for ADA compliance

07/01/13 – Changed “ITRMC” to “ITA”.