Center for Internet Security Benchmark for SQL Server v1.0

Table of Contents

Agreed Terms of Use

Background.

CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No representations, warranties and covenants.

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties or covenants of any kind.

User agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**we**") agree and acknowledge that:

1. No network, system, device, hardware, software or component can be made fully secure;

2. We are using the Products and the Recommendations solely at our own risk;

3. We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;

4. We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

5. Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of limited rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

1. Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

2. Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled “Grant of limited rights.”

Subject to the paragraph entitled “Special Rules” (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations (“**CIS Parties**”) harmless from and against any and all liability, losses, costs and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS’s right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special rules.

The distribution of the NSA Security Recommendations is subject to the terms of the NSA Legal Notice and the terms contained in the NSA Security Recommendations themselves (http://nsa2.www.conxion.com/cisco/notice.htm).

CIS has created and will from time to time create special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules.

CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of law; jurisdiction; venue.

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions.

We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Introduction

This document is derived from research conducted utilizing the SQL Server 2000 environment on Windows 2000 servers and desktops and Windows 2003 servers. This document provides the necessary settings and procedures for the secure installation, setup, configuration, and operation of an MS SQL Server 2000 system. With the use of the settings and procedures in this document, an SQL Server 2000 database may be secured from conventional “out of the box” threats. Recognizing the nature of security cannot and should not be limited to only the application; the scope of this document is not limited to only SQL Server 2000 specific settings or configurations, but also addresses backups, archive logs, “best practices” processes and procedures that are applicable to general software and hardware security.

1. Operating System and Network Specific Configuration

Item #	Configuration Item	Action / Recommended Parameters	Comments	Level
1.1	Physical security	Place the SQL Server in an area where it will be physically secure.	Place the server where only authorized personnel can obtain access.	1 (Ask)
1.2	Domain environment	If the SQL Server is in a domain that is trusted by other domains, document the access granted by the trust.	Ensure that the trusted domain has only the necessary rights to the SQL Server and its databases.	1 (Ask?)
1.3	SQL Servers accessed via Internet	If the SQL Server is being accessed via the Internet, place the SQL Server inside a DMZ with the Web Server.	Limit the database contents of this SQL Server to information meant for public dissemination only.	1 (Ask)
1.4	SQL Servers accessed via Internet	Put a firewall between your server and the Internet. In a multi-tier environment, use multiple firewalls to create more secure screened subnets.	Consider separating Web logic and business logic onto separate computers.	1 (Ask)
1.5	IPSEC	Use IPSEC policy filters to block connections to ports other than the configured SQL Server ports.	IPSEC offers authentication, integrity, confidentiality, and anti-replay services. SSL can provide these services for all database connections; however, IPSEC can allow these services to be configured on selected computers and ports. More information on IPSEC can be found in NSA's Microsoft Windows 2000 IPSEC Guide.	2 (Ask if implemented)
1.6	Encryption	Implement SSL. Use the fully-qualified DNS name of the server in the certificate to help prevent masquerading.	Note: If SSL is implemented, the service account must be a local administrator account. See items 1.13 – 1.17 for additional information on the service account.	2
1.7	Test and development servers	Maintain test and development servers on a separate network segment from the production servers.	Test patches carefully before applying them to production systems.	1 Ask
1.8	Dedicated Server	Install SQL Server on a computer that does not provide additional services, e.g., Web or Mail Services.	Vulnerabilities in other application services could lead to a compromise of the SQL Server.	1
1.9	OS Benchmark Configuration	Configure Windows 2000 Server Level II benchmark settings with the following modifications:		
1.9.1	Windows accounts	Make sure the Windows guest account is disabled		1
1.9.2	Volume / partition type	Format all volumes with NTFS		1

Item #	Configuration Item	Action / Recommended Parameters	Comments	Level
1.9.3	Disk subsystem	Use RAID for critical data files	Raid Level 10 is recommended. Use the level of RAID which will provide the best reliability and performance for your environment.	1
1.9.4	Separate partitions	Create separate volumes for SQL program files and SQL data files		1
1.10	Services	Disable the following services on a SQL Server machine	The disabling of services has to be balanced with application requirements, since certain applications require the use of certain services to function correctly.	1
1.10.1		Alerter		1
1.10.2		Clipbook Server		1
1.10.3		Computer Browser		1
1.10.4		DHCP Client		1
1.10.5		Distributed Transaction Service		1
1.10.6		Distributed File System		1
1.10.7		Fax Service		1
1.10.8		Internet Connection Sharing		1
1.10.9		IPSec policy agent	Unless IPSec policies will be used	1
1.10.10		License Logging Service		1
1.10.11		Logical Disk Manager Administrator Service		1
1.10.12		Messenger		1
1.10.13		NetMeeting Remote Desktop Sharing		1
1.10.14		Network DDE		1
1.10.15		Network DDE DS DM		1
1.10.16		Print Spooler		1
1.10.17		Remote Access Connection Manager		1
1.10.18		Remote Registry Service	Unless network management software requiring remote registry access will be used	1
1.10.19		Removable Storage		1
1.10.20		RunAs Service		1
1.10.21		Smart Card		1
1.10.22		Smart Card Helper		1
1.10.23		Task Scheduler	Unless batch jobs scheduled with the SQL Server Agent or scheduled tasks will be used	1
1.10.24		Telephony		1
1.10.25		Telnet		1
1.10.26		Windows Installer		1
1.11	MSSQL Server Service Account	Use a low-privileged Local or Domain account for the MSSQLServer service.	If SSL is implemented, the service account must be a local administrator. See 1.6.	2

Item #	Configuration Item	Action / Recommended Parameters	Comments	Level
1.12	SQLServerAgent Service Account	Use a low-privileged domain account for SQLServerAgent if replication, DTS, or other inter-server connection is required.	Replication and other inter-server communications require the SQLServerAgent service account to be a domain account. Proxy Account usage requires that the SQLServer Agent be run under a local admin account (post sp3a).	1
1.13	Local users group membership	Assign the local service account a member of only the Users group		1
1.14	Domain users group membership	Make a domain service account a member of only the Domain Users group		1
1.15	SQL Server services account rights	Grant the SQL Server services account(s) the following rights: Log on as a service, Act as part of the operating system, Lock pages in memory, Bypass traverse checking, Increase Quotas, Access this Computer from the network and Replace a process level token.	These rights may be assigned by default. Possibly, the Logon as a Batch job will be needed.	1
1.16	SQL Server services account rights	Deny the service account the “Log on locally” right.	The service accounts do not have a need to log on to the console. This will prevent a brute force attack on the service account.	1
1.17	SQL Server services account rights	If a service account is a domain account, configure the account to “Log on to” the database server only.	This, combined with the recommendation in item 1.16, will prevent an attempt to logon to any domain computer using the services account.	1

2. SQL Server Installation and Patches

Item #	Configuration Item	Action / Recommended Parameters	Comments	Level
2.1	SQL Server install platform	Avoid installing SQL Server on a domain controller.	If SQL Server were installed on a domain controller, a successful attack against the database could potentially compromise the entire network.	1
2.2	Patches and hotfixes	Ensure the Current SQL Server service pack and hotfixes are installed.	It would be counter productive to state specific patch levels and hotfixes in this document. Since they can change fairly often, the versions stated here might be outdated by the time this document is used. Check Microsoft’s website for the latest service pack/hotfix for SQL Server 2000. In multiple instance environments, updates must be applied to each SQL Server instance.	1
2.3	SQL Server Ports	Change SQL Server default ports from 1433 and 1434		1
2.4	Naming conventions	In naming SQL Server instances, limit the instance name to less than 16 characters with no reference to a version number or other sensitive information.	Version or other sensitive information in the server name makes it easier for an attacker to develop an attack strategy against the server.	1
2.5	SQL Server instances	Keep an inventory of all versions, editions and languages of SQL Server.	Include instances of MSDE. SQL Scan and SQL Check are some of the tools that can be used to scan for instances of SQL Server within a domain.	1 (Ask)
2.6	Authentication mode	Select Windows authentication mode during installation.	A strong password for the “sa” login account is required regardless of which mode is chosen.	1
2.7	Sample databases	Delete all sample databases.	e.g., Northwind and Pubs	1
2.8	Registry editing tools	Remove Registry editing tools from the SQL Server machine, if possible.	Remove Regedit.exe from the server.	1
2.9	Initialization parameter	Allow Updates - Set to 0 (disabled)	Specifies if direct updates should be allowed to system tables.	1
2.10	Initialization parameter	C2 Audit Mode– Set to 1 if no custom defined audit trace is enabled	Specifies whether automatic auditing of security events is enabled.	1
2.11	Initialization parameter	Remote Access– Set to 0 unless replication is being used or the requirement is justified	Allows logons from remote servers.	1
2.12	Initialization parameter	Scan for Startup Procedures– Set to 0 unless justified	Sets SQL Server to scan for startup procedures when the service starts.	1

3. SQL Server Settings

Item #	Configuration Item	Action / Recommended Parameters	Comments	Level
3.1	SQL Server Network Utility	Do not enable Named Pipes protocol.	If Named Pipes is required, change the name to something other than \\.\pipe\sql\query	1
3.2	SQL Server Properties	On the Propeties of the SQL Server, the following settings are recommended for security:	Accessed in Enterprise Manager	1
3.2.1	General tab of SQL Server Properties window	Select Auto restart SQL Server	Alternatively, configure the registry key HKLM\SOFTWARE\Microsoft\MSSQLServer\SQL ServerAgent\RestartSQLServer = 1	1
3.2.2	General tab of SQL Server Properties window	Select Auto restart SQL Server Agent, if the agent is required.	Alternatively, configure the registry key HKLM\SOFTWARE\Microsoft\MSSQLServer\SQL ServerAgent\MonitorAutoStart = 1	1(Ask)
3.2.3	General tab of SQL Server Properties window	Autostart Distributed Transaction Coordinator = Off		1
3.2.4	General tab of SQL Server Properties window	Disable cross database-ownership chaining	Use sp_dboption to check for databases for which cross-database ownership chaining is enabled.	1
3.2.5	Security tab of SQL Server Properties window	Authentication: Windows Only	Weak encryption is used to protect passwords in SQL Server authentication. If SQL Server Login IDs and passwords are required, implement SSL.	1
3.2.6	Security tab of SQL Server Properties window	Audit level: Failure or All	SQL Server audit level to “All” or “failure” – writes successful/failed SQL login attempts to the SQL log and the Windows event log	1
3.2.7	Connections tab of SQL Server Properties window	Verify remote server connections are not enabled (selected)	Used for replication and remote stored procedures	1 (ignore if replication is configured)
3.2.8	Server Settings tab/Server behavior of SQL Server Properties window	Do not enable direct modifications to the system catalogs		1
3.2.9	Database Setting Tab	Backup/Restore – Timeout period = try for 5 minutes		1
3.2.10	Database Settings Tab	Default backup media retention = at least 1 day		1
3.3	Data Directory	Default data directory = dedicated data partition		1
3.4	Data Directory	Default log directory = dedicated partition separate from all programs and data		1

Item #	Configuration Item	Action / Recommended Parameters	Comments	Level
3.5	Replication	Do not enable replication.	Section 7 covers security recommendations if replication is required.	1
3.6	Other SQL Server Configuration Options	Scan for startup procedures = 0 (disabled)		1
3.7	Other SQL Server Configuration Options	Save a maximum of 14 SQL error logs .	Truncate logs on a regular schedule, weekly, bi-weekly etc. to prevent oversize logs.	1
3.8	Other SQL Server Configuration Options	Do not enable SQlAgent Mail.	As an alternative consider SMTP agent with less vulnerability than Outlook.	1
3.9	Trace Messages	Error Log/Include execution trace messages = off		1
3.10	User-defined stored procedures	Ensure that all user-defined stored procedures are stored in encrypted format .		1
3.11	User-defined extended stored procedures	Avoid using user-defined extended stored procedures		1
3.12	SQLMail extended stored procedures	Delete the sqlmap70.dll file that implements the SQLMail extended stored procedures.		1
3.13	Extended stored procedures	Drop the following extended stored procedures:	The dropping of stored procedures has to be balanced with application requirements, since certain applications require the use of external stored procedures to either export or import data. In the case where stored procedures need to be left on the server, document this information and note as an exception.	
3.13.1		xp_available media		1
3.13.2		xp_cmdshell		1
3.13.3		xp_dirtree		1
3.13.4		xp_dsninfo		1
3.13.5		xp_enumdsn		1
3.13.6		xp_enumerrorlogs		1
3.13.7		xp_enumgroups		1
3.13.8		xp_eventlog		1
3.13.9		xp_fixeddrives		1
3.13.10		xp_getfiledetails		1
3.13.11		xp_getnetname		1
3/13.12		xp_logevent		1
3.13.13		xp_loginconfig		1
3.13.14		xp_msver		1
3.13.15		xp_readerrorlog		1
3.13.16		xp_servicecontrol		1

Item #	Configuration Item	Action / Recommended Parameters	Comments	Level
3.13.17		xp_sprintf		1
3.13.18		xp_sscanf		1
3.13.19		xp_subdirs		1
3.13.20		xp_unc_to_drive		1
3.14	SQLmail extended stored procedures	Drop the following SQLMail extended stored procedures:		
3.14.1		xp_deletemail		1
3.14.2		xp_findnextmsg		1
3.14.3		xp_get_mapi_default_profile		1
3.14.4		xp_get_mapi_profiles		1
3.14.5		xp_readmail		1
3.14.6		xp_sendmail		1
3.14.7		xp_startmail		1
3.14.8		xp_stopmail		1
3.15	WebTask extended stored procedures	Drop the following WebTask extended stored procedures. Delete the xpweb70.dll file that implements the following Web Task extended stored procedures:		
3.15.1		xp_cleanupwebtask		1
3.15.2		xp_convertwebtask		1
3.15.3		xp_dropwebtask		1
3.15.4		xp_enumcodepages		1
3.15.5		xp_makewebtask		1
3.15.6		xp_readwebtask		1
3.15.7		xp_runwebtask		1
3.16	SNMP extended stored procedures	Drop the following SNMP extended stored procedures:		
3.16.1		xp_snmp_getstate		1
3.16.2		xp_snmp_raisetrap		1
3.17	OLE Automation stored procedures	Drop the following OLE Automation stored procedures:		
3.17.1		sp_OACreate		1
3.17.2		sp_OADestroy		1
3.17.3		sp_OAGetErrorInfo		1
3.17.4		sp_OAGetProperty		1
3.17.5		sp_OAMethod		1
3.17.6		sp_OASetProperty		1

Item #	Configuration Item	Action / Recommended Parameters	Comments	Level
3.17.7		sp_OAStop		1
3.18	Registry access extended stored procedures	Drop the following Registry access extended stored procedures:		
3.18.1		xp_regaddmultistring		1
3.18.2		xp_regdeletekey		1
3.18.3		xp_regdeletevalue		1
3.18.4		xp_regenumvalues		1
3.18.5		xp_regremovemultistring		1
3.18.6		xp_regwrite		1
3.19	Advanced Setting	SQL Server Event forwarding/Forward events to a different server = off		1

4. Access Controls

Item #	Configuration Item	Action / Recommended Parameters	Comments	Level
4.1	Permissions on OS tools	Restrict access to the executables in the System32 directory eg. Explorer.exe and cmd.exe.	Remove the Users group's permission (if any) to executables. Assign Administrators Full Control.	1
4.2	SQL Server install directory permissions	Modify the permissions to the [Drive]:\Program Files\Microsoft SQL Server directory.	Assign the SQL Server service account Full Control. Remove the Users group's permission.	1
4.3	SQL Server database instance directory permissions	Delete or secure old setup files. Protect files in the <system drive>:\Program Files\Microsoft SQL Server\MSSQL$<instance name>\Install folder, e.g., sqlstp.log, sqlsp.log and setup.iss.	If the current system was upgraded from SQL Server version 7.0, check setup.iss in the %Windir% folder and the sqlstp.log in the Windows Temp folder for passwords. Microsoft distributes a free utility called Killpwd, which will locate and remove passwords found in these setup files from your system.	1
4.4	NTFS Permissions	Verify and set NTFS permissions as follows:	SQL Server Setup grants the service account(s) and the Administrators group Full Control to these files and directories	
4.4.1		SQL Server Program directory SQL Server service account – Full Control System and Administrators –Full Control	\Program Files\Microsoft SQL Server\ is the default	1
4.4.2		Database files (.mdf, .ndf, and .ldf) SQL Server service account –Full Control System and Administrators –Full Control	Use the SQL Server restricted service account to encrypt sensitive database files with EFS.	1
4.4.3		SQL log files volume SQL Server service account – Change Auditing user account – Read	Dedicate this volume to log files only	1
4.5	Registry permissions	Assign MSSQLServer and SQLAgent service account(s) the following: Assign only the Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, and Read Control permissions for the service account on the following keys:		
4.5.1		HKEY_LOCAL_MACHINE\Software\Microsoft\MSSQLServer		1
4.5.2		HKEY_LOCAL_MACHINE\Software\Microsoft\MSSQLServer\ $InstanceName	For a named instance	1

Item #	Configuration Item	Action / Recommended Parameters	Comments	Level
4.5.3		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Perflib		1
4.5.4		HKEY_LOCAL_MACHINE\System\CurrentControlset\Services\MSSQLServer		1
4.5.5		HKEY_LOCAL_MACHINE\System\CurrentControlset\Services\SQLServerAgent		1
4.5.6		HKEY_LOCAL_MACHINE\System\CurrentControlset\Services\MSSQL$InstanceName	For a named instance	1
4.6	Registry permissions	Remove the “Everyone” group and grant the database administrators group Full Control permissions on these registry keys:	SQL Server Setup grants the service account(s) and the Administrators group Full Control permissions to these registry keys by default.	
4.6.1		HKEY_LOCAL_MACHINE\Software\Microsoft\MSSQLServer		1
4.6.2		HKEY_LOCAL_MACHINE\Software\Microsoft\MSSQLServer\$InstanceName	For a named instance	1
4.6.3		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Perflib		1
4.6.4		HKEY_LOCAL_MACHINE\System\CurrentControlset\Services\MSSQLServer		1
4.6.5		HKEY_LOCAL_MACHINE\System\CurrentControlset\Services\SQLServerAgent		1
4.6.6		HKEY_LOCAL_MACHINE\System\CurrentControlset\Services\MSSQL$InstanceName	For a named instance	1
4.7	Assigning System Administrators role	When assigning database administrators to the System Administrators role, map their Windows accounts to SQL logins, then assign them to the role.	Assign only authorized DBAs to the SQL Server System Administrators role.	1 (Report)
4.8	SQL Logins	Remove the default BUILTIN\Administrators SQL login.	Do not remove BUILTIN\Administrators until another account has been assigned the System Administrators role.	1
4.9	SQL Logins	Ensure that the sa account and all SQL Logins have strong passwords.	Verify that the passwords are not blank and cannot be easily compromised.	1
4.10	OS Guests access	Deny database login for the Guests OS group.	EXEC sp_denylogin 'Computer_Name\Guests'	1
4.11	Fixed Server Roles	Only use the fixed server roles sysadmin, serveradmin, setupadmin etc., to support DBA activity.	Avoid assigning these roles to application database user accounts, application administrator accounts, application developer accounts or application roles.	1 (Report)
4.12	SQL Server Database Users and Roles	Remove the guest user from all databases except master and tempdb.		1
4.13	Statement Permissions	Grant statement permissions to only the database owner, not individual users.	DBO has all statement permissions for the database by default	1

Item #	Configuration Item	Action / Recommended Parameters	Comments	Level
4.14	Database Owners Permissions	Ensure the database owner (dbo) owns all user-created database objects.	Avoid changing the ownership of system-created objects in the system databases. These objects may be owned by INFORMATION_SCHEMA and SYSTEM_FUNCTION_SCHEMA. Changes to these objects could severely impact applications.	1 (Report)
4.15	Low-privileged users	Do not grant object permissions to PUBLIC or GUEST.	Do not grant the REFERENCES object permission to an application user, application administrator, or application role.	1 (Report)
4.16	PUBLIC's permissions	Remove PUBLIC's permissions to the system tables in each database.		1
4.17	Stored Procedure Permissions	Grant execute permissions on stored procedures to database roles (not users).		1 (Report)
4.18	Use of Roles	Assign roles to local groups for database permissions.	Create Local groups for database users, assign Global group from Domain to Local group. If there are different classes of users use separate groups for them.	1
4.19	Using the GRANT option	Do not assign the GRANT option of object permission to a user or role.		1
4.20	Limit Job Steps	Restrict the use of CmdExec and Active Scripting job steps to DBAs		1
4.21	User-defined Database Roles	Create user-defined database roles to assign permissions to objects in the database when a pre-defined database role does not supply the appropriate permissions to a group of users.		1
4.22	Database Roles	Avoid nesting database roles.		1
4.23	Users and Roles	Ensure that the members of the roles exist as users / groups or other roles in the target database.		1
4.24	Application Roles	Use application roles to limit access to data to users of specific applications. Use encryption to protect the role name and password in the connection string.	The password for the application role is embedded in the connection string, so the user is unaware of the password and can only access the data when using the specific application that initiates the connection string.	1
4.25	Use of Predefined Roles	Avoid assigning predefined roles to PUBLIC or GUEST.		1
4.26	Linked or Remote Servers	Use linked servers rather than remote servers.	Remote servers are available for backward compatibility purposes only. Applications that must execute stored procedures against remote instances of SQL Server should use linked servers instead.	1

Item #	Configuration Item	Action / Recommended Parameters	Comments	Level
4.27	Linked or Remote Servers	Configure linked or remote servers to use Windows authentication.	When linking SQL Server databases, the user’s current identity will be used to authenticate the connection.	1
4.28	Linked Server logins	Allow linked server access only to those logins that need it.		1 (Report)
4.29	Ad Hoc Data Access	Disable ad hoc data access on all providers except SQL OLE DB, for all users except members of the sysadmin fixed role. Use network segmentation to prevent or limit desktop clients making direct adhoc connections.	Allow ad hoc data access only to trusted providers. Limit adhoc connections using MS Office applications (Excel, Access, Word, etc.).	1

5. Auditing and Logging

Item #	Configuration Item	Action / Recommended Parameters	Comments	Level
5.1	Auditing – General	Prepare a schedule for reviewing audit information regularly.		1 (Ask)
5.2	SQL Server Properties – Security Tab	Through the Enterprise Manager, enable auditing for SQL Server.	At a minimum, enable failed login attempts.	1
5.3	SQL Server Logs	SQL Server audit data must be protected from loss. The SQL Server and SQL Server Agent logs must be backed up before they are overwritten.	Adjust the number of logs to prevent data loss. The default is six.	1
5.4	SQL Profiler	Use SQL Profiler to generate and manage audit trails.	Ensure sufficient resources to support Profiler activity	1 (Ask)
5.5	Profiler Events	Capture the following events using SQL Profiler	A third-party auditing tool may be used in lieu of SQL Profiler.	
		Event	**Description of what the event records**	
5.5.1		Audit Add DB User	Addition and deletion of database users	1
5.5.2		Audit Add Login to Server Role	Addition or removal of login accounts to/from server roles	1
5.5.3		Audit Add Member to DB Role	Addition or removal of database users to/from database roles	1
5.5.4		Audit Add Role	Addition or deletion of database roles	1
5.5.5		Audit Add Login	Addition or deletion of SQL Server logins	1
5.5.6		Audit App Role Change Password	Password changes on application roles	1
5.5.7		Audit Backup/Restore	BACKUP and RESTORE actions	1
5.5.8		Audit Change Audit	AUDIT modifications	1
5.5.9		Audit DBCC	Issued DBCC commands	1
5.5.10		Audit Login	All new connection events since the trace was started	1
5.5.11		Audit Login Change Password	Password changes of SQL Server logins	1
5.5.12		Audit Login Change Property	Modifications to login properties (except passwords)	1
5.5.13		Audit Login Failed	Failed login attempts	1
5.5.14		Audit Login GDR	GRANT, DENY and REVOKE actions on Windows account login rights	1
5.5.15		Audit Logout	All new disconnected events since the trace was started	1

Item #	Configuration Item	Action / Recommended Parameters	Comments	Level
5.5.16		Audit Object Derived Permissions	CREATE, ALTER or drop command for a specific object	1
5.5.17		Audit Object GDR	GRANT, DENY and REVOKE actions on objects	1
5.5.18		Audit Object Permission	Successful or unsuccessful use of object permissions	1
5.5.19		Audit Server Starts and Stops	Shutdown, Start and Pause activities for services	1
5.5.20		Audit Statement GDR	Use of GRANT, DENY, REVOKE statements	1
5.5.21		Audit Statement Permission	Use of statement permissions	1

6. Backup and Disaster Recovery Procedures

Item #	Configuration Item	Action / Recommended Parameters	Comments	Level
6.1	Backups – General	Use Full database backups combined with differential or transaction log backups to restore the database to a specific point in time.	Database backups should be made to another server or disk that is not physically attached to the same server as the database. This will reduce the risk of total loss in case of disk failure.	1
6.2	System databases	It is important to include the system databases in your backup plan i.e. the master, msdb and model databases.	The tempdb database contains no permanent data and does not require backups.	1 (Ask)
6.3	Backing up Master database	Backup the master database when any of the following events occur: • A database is created or deleted • Login accounts are created, deleted or modified • Server-wide or database settings are modified		1 (Ask)
6.4	Backing up MSDB database	Backup the msdb database when any of the following events occur: • Alerts, jobs, schedules or operators are created, deleted or modified • Backups and restores are performed		1 (Ask)
6.5	Backup Media	Password protect the backup media.	This ensures that the data is protected from unauthorized restores or from being accidentally overwritten.	1 (check or ask)
6.6	Limiting Network Activity	To ensure backup files are protected, avoid performing activities such as backups and restores across the network.		1
6.7	Access to Backup Files	Restrict access to the backup files to System Administrators.		1
6.8	Access to Backup Files	Restrict restore permissions to DBAs and db_owners.		1
6.9	Recommended periodic administrative procedures	Run the Microsoft Baseline Security Analyzer weekly and follow the security recommendations as closely as possible		

Item #	Configuration Item	Action / Recommended Parameters	Comments	Level
6.10	Recommended periodic administrative procedures	Run the SQL Best Practices Analyzer regularly and note any changes to the environment.		
6.11	Periodic scan for password security	Periodically scan for accounts with NULL passwords and remove the accounts or assign a strong password.		1 (Report)
6.12	Periodic scan of Role Members	Periodically scan fixed server and database roles to ensure that only trusted individuals are members.		1 (Report)
6.13	Periodic scan of stored procedures	Verify stored procedures that have been set to AutoStart are secure.		1 (Report)

7. Replication

Item #	Configuration Item	Action / Recommended Parameters	Comments	Level
7.1	SQL Server Agent service account	The replication agents run under the SQL Server Agent service account.	This account must be a domain account. To use the Proxy Agent Service, the account must be a local administrator (post sp3a).	1
7.2	Replication administration roles	Avoid modifying replication administration permissions assigned to the roles by default. Only assign authorized application administrators and DBAs these roles.	The permissions needed to support and administer replication are assigned to sysadmin, db_owner and replmonitor by default..	1
7.3	Snapshot share folder	Store the snapshot folder, which houses a snapshot of the replicated changes, on an explicit share and not an administrative share.		1
7.4	Snapshot share folder permissions	Assign the following NTFS permissions: System and Administrators – FULL CONTROL SQL Server Agent service account – READ and WRITE		1
7.5	Publication Access List	The domain account used by the SQL Server Agent service must be entered in the Publication Access List so that all replication agents will be able to participate in the replication process.		1
7.6	Secure Communications	Use secure connections, such as VPN or proxy servers, for all replication over the Internet.		1
7.7	Database connections	Configure the database connections for replication agents to use Windows authenticated logons.		1
7.8	Filtering	Employ replication filters to protect the data.		1
7.9	Distribution databases	All distribution databases and snapshot files must be located in protected and audited locations.		1

8. Application Development Best Practices

Item #	Configuration Item	Action / Recommended Parameters	Comments	Level
8.1	Ownership Chaining	Use ownership chaining within as single database to simplify permissions management..	Avoid using cross database ownership.	
8.2	Role Assignments	Assign permissions to roles rather than users.	Ensure that roles, rather than users own objects to avoid application changes when a user is dropped.	
8.3	Encrypted connections	Enable encrypted connections between the user and the server.	Consider allowing only encrypted connections. When allowing SQL Server authentication, encrypt either the network layer with IPSec or the session with SSL	
8.4	Error Handling	Do not propagate errors back to the user.	Log errors or transmit them to the system administrator.	
8.5	User Input	Prevent SQL injection by validating all user input before transmitting it to the server.	Only permit minimally privileged accounts to send user input to the server.	
8.6	Developer awareness	Increase awareness of issues such as cross-site scripting, buffer overflows, SQL injection and dangerous APIs.		
8.7	Developer awareness	Identify categories of threats that apply to your application, such as denial of service, escalation of privileges, spoofing, data tampering, information disclosure and repudiation.		
8.8	Security reviews	Add security reviews to all stages of the application development lifecycle (from design to testing).		
8.9	Distributing MSDE	If you distribute MSDE, install MSDE using Windows security mode as the default.	Never install a blank sa password. Use the Microsoft Installer to install MSDE.	
8.10	Net-Libraries	If MSDE will operate as a local data store, disable the Server Net-Libraries.		
8.11	Customer awareness	Let your customers know that your product includes MSDE so that they can be prepared to install or accept MSDE-specific software updates.		
8.12	SQL Server Agent	Change the SQL Server Agent Startup Type to “Disabled”.	MSDE installs SQL Server Agent by default and the Service startup type is “Manual”.	

References

10 Steps to Help Secure SQL Server 2000. Microsoft Corporation. Last accessed at: http://www.microsoft.com/sql/techinfo/administration/2000/security/securingsqlserver.mspx

Database Security Technical Implementation Guide version 7, release1, October 2004. Developed by DISA for the DOD.

Guide to the Secure Configuration and Administration of Microsoft SQL Server 2000. Network Applications Team of the Systems and Network Attack Center (SNAC). August 26, 2003. National Security Agency.

SQL Server 2000 SP3 Security Features and Best Practices: Security Best Practices Checklist. May 2003. Microsoft Corporation. Last accessed at: http://www.microsoft.com/technet/prodtechnol/sql/2000/maintain/sp3sec04.mspx

SQL Server Security Checklist. Last accessed at: http://www.securitymap.net/sdm/docs/windows/mssql-checklist.html