# 

**MS SQL Database Security Policy**

**TABLE OF CONTENTS**

Purpose 3

Scope 3

Patches & Updates 3

Services 3

Protocols 3

Account Security 3

For MS SQL Server 2005 only: 4

Filesystem Security 4

Ports 4

Registry Security 4

Auditing & Logging 4

Server Security 4

Database Objects 5

Review & Revision 6

Enforcement 6

Exceptions 6

## Purpose

The purpose of the ACME MS SQL Database Security Policy is to define the technical requirements needed to secure the Microsoft SQL Server database environment.

## Scope

* The scope includes all production MS SQL Server 2000 and MS SQL Server 2005 databases within ACME. MS SQL Server 2008 is out of scope.

## Patches & Updates

* Apply the latest service packs, hot fixes and patches in accordance with ACME Security Patch Management Process.
  + Apply patches and service packs to development instances prior to applying them to production.
  + Refer to the appropriate Windows Policy for hardening and patch information.
  + All new SQL Server installations should include the latest approved Service Pack and Cumulative Update for the selected version.

## Services

* Disable the Distributed Transaction Coordinator if not in use. (MS DTC should be configured properly if we are using it)
  + For MS SQL Server 2000, disable the following services from starting up:
    - MSSQLSERVER service for any instances that are not currently in use.
    - MSSQLServerADHelper if not in use.
  + For MS SQL Server 2005, disable the following services from starting up:
    - SQL Server and SQL Server Agent service for any instances that are not currently in use.
    - SQL Server Analysis Services, SQL Server FullText Search, SQL Server Reporting Services if not in use.

## Protocols

* Restrict SQL Server to TCP/IP and Named Pipes.

## Account Security

* Windows authentication is required. If an application cannot use Windows authentication for technical reasons, SQL authentication may be used.  In those cases, SQL authentication should be considered only for application userids and not for end user accounts.
* SQL Server Service account (svcMsSqlServ), SQL Server Agent Service account (svcMsSqlAgent), SQL Server Full text Service Account (svcMsSqlFullText) and SQL Server Analysis Services account (svcMSSqlAnSrvc), if they exist, should be normal domain users with no domain admin rights;
* Remove Built-in\Administrators Login from System Administrator role;
* Do not grant permissions to the public role;
* Create custom database roles if required, for finer control over permissions. Database Roles to be assigned to Users or User Groups and privileges to be assigned to the roles;
* sa account should not be used for administrative tasks and should not be used at all by applications. An exception can be made for the duration of an application/database install process if deemed the best option by the DBA. In this case the sa password should be changed for the duration of the installation process and changed back afterward.;
* Scan for NULL passwords for SQL Logins;
* Use strong password for sa account and for all SQL Server users. Password policy must follow the Access Control Policy;
* Access to a group of users to SQL Server should be enabled only using Windows Domain Groups

### For MS SQL Server 2005 only:

* Do not directly grant access to various SQL Server service accounts (such as MsSqlAgentService-ls) unless the service account needs to be changed post installation.  Instead, allow the SQL Server installation process to grant least privileges as designed;
* Grant sysadm role to ACME01\MsSqlAgentService-ls and ACME01\MsSqlService-ls but not to MsSqlAnalysisService-ls and MsSqlFullTextService-ls;
* For application users no Server level roles or DB Owner is given unless mandatory for the application and then will be limited to least required privilege;
* Access to a group of users to SQL Server should be enabled only using Windows Domain Groups;
* The Security Model in SQL Server 2005 can be designed more strictly as needed using the following features:
  + User Schema Separation
  + Credentials
  + Proxy Accounts
  + Impersonation
  + Encryption
  + TRUSTWORTHY Database Property

## Filesystem Security

* **Everyone** group should not have permissions on SQL Server install directories (by default, \Program Files\Microsoft SQL Server\MSSQL);
* **Everyone** group should not have permissions to SQL Server data/log files. Refer Server Hardening checklist;
* Delete setup log files.

## Ports

* Do not use default TCP port 1433 for SQL Server;
* Configure instances to listen on the following ports:
  + 52065 internal instances
  + 52062 public facing instances
  + 52072 store instances
  + For multiple instances in the same server/cluster, use increasing sequential numbers.

## Registry Security

* Make sure the *Everyone* group does not have permissions for the SQL Server registry keys;
* For MS SQL Server 2000:
  + HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Microsoft SQL Server\80\Tools\SQLEW\Registered Servers.

## Auditing & Logging

* Log all SQL Server authentication attempts (success and failure);
* *For SQL 2000: C2 Level Auditing can be enabled on a case by case basis.*

## Server Security

* Physical Security: Ensure server is located in the secured location (Data Center or Store Server Room);
* Install SQL Server on a partition formatted with NTFS;
* Do not install SQL server on a domain controller;
* SDKs and resource kits should not be installed on production database servers;
* Disable the guest user account in the msdb database to prevent unauthorized users from creating DTS packages or SQL Agent jobs;
* Windows authentication is required. If Windows authentication is not available, SQL authentication may be used.
* Application clients should have no rights to system databases and should default to an appropriate application database.
* An Application ID associated with a proxy can be granted specific and minimal rights in the msdb database to provide necessary functionality.
* For MS SQL Server 2005:
  + Encrypt sensitive data stored in the database.
* For MS SQL Server 2005:
  + After installation of SQL Server, remove the following default local windows groups:

servername\SQLServer2005SQLAgentUser$servername$Instancename

servername\SQLServer2005MSSQLUser$servername$Instancename

servername\SQLServer2005MSFTEUser$servername$Instancename

servername\SQLServer2005FTS$servername$Instancename

servername\SQLServer2005MSSQLServerOLAPservice$servername$Instancename

servername\SQLServer2005ReportServerUser$servername$Instancename

servername\SQLServer2005ReportingServicesWebServiceUser$servername$Instancename

servername\SQLServer2005Notificationservices$servername$Instancename

servername\SQLServer2005SQLServerBrowser$servername$Instancename

servername\SQLServer2005MSADHekper$servername$Instancename

servername\SQLServer2005SQLWriter$servername$Instancename

servername\SQLServer2005User$servername$Instancename

## Database Objects

* Delete (or do not install) sample databases pubs, Northwind and AdventureWorks in QA/PROD;
* Restrict XP\_CMDSHELL access to only users that have a specific requirement. In SQL2005 use Proxy and Credentials to manage this access;
* Provide only Exec rights on procedures;
* No select access to be provided to developers in QA or Prod for sensitive data.
* *For MS SQL 2000:* 
  + Deny execute permissions to the msdb..sp\_add\_dtspackage stored procedure.
* MS DTC Security
  + Set the log on account for the “DTC (Distributed Transaction Coordinator)” service to “NT AUTHORITY\NETWORK SERVICES.”
  + For COM Security, grant the group “Everyone” the “Allow” permission
  + In network DTC access, enable “Allow Remote Clients” and “Allow Remote Administration.”
  + In transaction manager communications enable “Allow Inbound and Allow Outbound.”
  + Enable “XA Transactions.”

## Review & Revision

This policy will be reviewed and revised annually.

## Enforcement

Strict compliance with this policy is essential for the effective protection of ACME. Any violation will be forwarded to the appropriate manager, Information Security, and HR representative for appropriate action up to and including termination of employment.

## Exceptions

ACME Information Security must approve any exceptions to this policy. You can initiate the security exception process by sending a detailed email to the following email address: security@acme.com.