**Best Practice to Secure the SQL Server(s)**

Start with the physical server room where the Servers are kept

Insure that only selected IT staff has access (Network Admins, System Admins, and SQL DBAs)

Keep the backups not only on site, but keep a copy of backups off site

Install all service packs and critical fixes for Windows Operating System and SQL Server Service Packs

(Test on test server first before applying to production)

Disable the default admin the BUILTIN\Administrators group from the SQL Server (demo)

Use Windows Authentication mode as opposed to mixed Mode (demo)

Use service accounts for applications and create a different service account for each SQL Service

Create service accounts with the least privileges

Document all user permission with the script and keep track of which user has what permissions (demo)

Disable all features via the SQL Server Configuration Manager that are not in use (demo)

Install only required components when installing SQL Server (don’t install ssrs, ssis, ssas)

Disable the SA account and rename it (demo)

Remove the BUILTIN\Administrators Windows Group from a SQL (demo)

Use SQL Server Roles to limit logins accessing database (as shown in previous videos)

Use permission to give only that is needed to the SQL Login or User

Hide all databases from logins (demo)

Be proactive in securing the SQL Server and databases

--Drop the BUILTIN\administrators

EXEC master..xp\_logininfo

@acctname = 'Builtin\Administrators',

@option = 'members'

USE MASTER

IF EXISTS (SELECT \* FROM sys.server\_principals

WHERE name = N'BUILTIN\Administrators')

DROP LOGIN [BUILTIN\Administrators]

GO

--Verfiy the Builtin\Administrators group has been dropped

EXEC master..xp\_logininfo

@acctname = 'Builtin\Administrators',

@option = 'members'

--AddBuiltin\Administrators

EXEC sp\_grantlogin 'BUILTIN\Administrators'

EXEC sp\_addsrvrolemember 'BUILTIN\Administrators','sysadmin'

EXEC master..xp\_logininfo

@acctname = 'Builtin\Administrators',

@option = 'members'

--Enable Windows Authentication (requires a restart of services)

USE [master]

GO

EXEC xp\_instance\_regwrite N'HKEY\_LOCAL\_MACHINE',

N'Software\Microsoft\MSSQLServer\MSSQLServer', N'LoginMode',

REG\_DWORD, 1

GO

--Enable Mixed Mode Authentication (requires a restart of services)

USE [master]

GO

EXEC xp\_instance\_regwrite N'HKEY\_LOCAL\_MACHINE',

N'Software\Microsoft\MSSQLServer\MSSQLServer',

N'LoginMode', REG\_DWORD, 2

GO

--Get infor on all SQL Logins and Windows users

SELECT name AS Login\_Name,TYPE, type\_desc AS Account\_Type

FROM sys.server\_principals

WHERE TYPE IN ('U', 'S', 'G')

ORDER BY name, type\_desc

--make sure you have a login that is part of the sysadmin role before doing this!!!!

USE [master]

GO

ALTER LOGIN [sa] WITH PASSWORD=N'Password#12345'

GO

ALTER LOGIN [sa] DISABLE

GO

USE [master]

GO

ALTER LOGIN [sa] WITH PASSWORD=N'Password#12345'

GO

ALTER LOGIN [sa] ENABLE

GO

--Hide all databases

USE MASTER

GO

DENY VIEW ANY DATABASE TO PUBLIC

GO

--unhide all databases

USE MASTER

GO

GRANT VIEW ANY DATABASE TO PUBLIC;

GO