SALT LAKE COUNTY
COUNTYWIDE INFORMATION TECHNOLOGY STANDARD
ON
SECURE MS SQL DATABASE CONFIGURATION

Purpose –

The purpose of this standard is to provide guidance and consistency in the configuration of Microsoft SQL servers.

Employees of Salt Lake County are expected to follow the *Secure Database Configuration Standard* established by the Information Technology Division. The Information Technology Division will monitor and enforce compliance with this standard.

Reference –

The standards set forth herein are provided in accordance with Countywide Policy 1400, which directs Salt Lake County Information Technology to provide information technology standards.
Also referencing the following:
All Countywide Information Technology Security Policies in the 1400 series
All Countywide Human Resource Policies
Salt Lake County Ordinance - Chapter 2.81 – Security of Personal Identifiers

1.0 Scope

All Salt Lake County employees shall adhere to this Countywide information technology standard whenever they access County information technology resources and systems, any device that connects to any Salt Lake County network, or any device that resides at a Salt Lake County facility.

2.0 Definitions

Information Technology Resource(s) and/or System(s)
Computers, hardware, software, data, storage media, electronic communications (including, but not limited to, email, fax, phones, phone systems, and voice mail), networks, operational procedures and processes used in the collection, processing, storage, sharing or distribution of information within, or with any access beyond ordinary public access to, the County's shared computing and network infrastructure.

Electronic Database
An electronic database is any collection of data or information specially organized for rapid search and retrieval by a computer. Databases are structured to facilitate the storage, retrieval, modification, and deletion of data in conjunction with various data-processing operations.

Structured Query Language (SQL)
Structured Query Language is a domain-specific language used in programming and designed to manage data held in a relational database management system (RDBMS) or stream processing in a relational data stream management system (RDSMS). It is advantageous in handling structured data, i.e., data incorporating relations among entities and variables.

Database Management System (DBMS)
A database management system extracts information from the database in response to queries.

Relational Database Management System (RDBMS)
An RDBMS is a DBMS designed specifically for relational databases. A relational database refers to a database that stores data in a structured format, using rows and columns. This makes it easy to locate and access specific values within the database.

3.0 Standard Guidance

3.1 All County users will follow the secure MS SQL database configuration standard as defined in appendix A.

4.0 Exceptions

Any exceptions to this standard must be explicitly approved in writing by the Salt Lake County Chief Information Officer or their designee.

5.0 Enforcement

Anyone found to have knowingly violated this standard shall be subject to disciplinary action by County disciplinary policies.

Appendix A
Secure Database Configuration Standard – MS SQL

Installation, Updates, and Patches

1.1 - Ensure Latest SQL Server Cumulative and Security Updates are Installed
- Automated control
- CIS Control 2.2 - Ensure Vendor supports software

1.2 - Ensure Single-Function Member Servers are Used
- Manual control
- CIS Control 2.10 - Physically or Logically Segregate High-Risk Applications

Surface Area Reduction

2.1 - Ensure the' Ad Hoc Distributed Queries' Server Configuration Option is set to '0.'
- Automated control
- CIS Control 9.2 - Ensure Only Approved Ports, Protocols and Services Are Running

2.2 - Ensure 'CLR Enabled' Server Configuration Option is set to '0'
- Automated control
- CIS Control 18.11 - Use Standard Hardening Configuration Templates for Databases

2.3 - Ensure 'Cross DB Ownership Chaining' Server Configuration Option is set to '0.'
- Automated control
- CIS Control 14.6 - Protect Information through Access Control Lists

2.4 - Ensure the' Database Mail XPs' Server Configuration Option is set to '0.'
- Automated control
- 9.2 Ensure Only Approved Ports, Protocols, and Services Are Running

2.5 - Ensure the 'Ole Automation Procedures' Server Configuration Option is set to '0.'
- Automated controls
- CIS Control 5.1 - Establish Secure Configurations

2.6 - Ensure the 'Remote Access' Server Configuration Option is set to '0.'
- Automated control
- CIS Control 9.2 - Ensure Only Approved Ports, Protocols and Services Are Running

2.7 - Ensure 'Remote Admin Connections' Server Configuration Option is set to '0.'
- Automated control
- CIS Control 9.2 - Ensure Only Approved Ports, Protocols and Services Are Running

2.8 - Ensure the' Scan For Startup Procs' Server Configuration Option is set to '0.'
- Automated Control
- CIS Control 5.1 - Establish Secure Configurations

2.9 - Ensure 'Trustworthy' Database Property is set to 'Off.'
- Automated Control
- CIS Control 14.6 - Protect Information through Access Control Lists

2.10 Ensure Unnecessary SQL Server Protocols are set to 'Disabled.'
- Manual control
- CIS Control 9.2 - Ensure Only Approved Ports, Protocols and Services Are Running

2.11 Ensure SQL Server is configured to use non-standard ports
- Automated Control
- CIS Control 9.2 Ensure Only Approved Ports, Protocols, and Services Are Running

2.12 Ensure the 'Hide Instance' option is set to 'Yes' for Production SQL Server instances
- Automated Control

Revision History
AUGUST 2021 - MLE

- 9.2 - Ensure Only Approved Ports, Protocols and Services Are Running

2.13 Ensure the 'sa' Login Account is set to 'Disabled.'
- Automated control
- CIS Control 16.8 - Disable Any Unassociated Accounts

2.14 Ensure the 'sa' Login Account has been renamed
- Automated control
- CIS Control 5.1 - Establish Secure Configurations

2.15 Ensure 'AUTO_CLOSE' is set to 'OFF' on contained databases
- Automated Control
- CIS Control 5.1 - Establish Secure Configurations

2.16 Ensure no login exists with the name 'sa'
- Automated control
- CIS Control 5.1 - Establish Secure Configurations

Authentication and Authorization

3.1 Ensure 'Server Authentication' Property is set to 'Windows Authentication Mode.'
- Automated control
- CIS Control 16.2 - Configure Centralized Point of Authentication

3.2 Ensure CONNECT permissions on the 'guest' user is Revoked within all SQL Server databases, excluding the master, msdb, and tempdb
- Automated control
- CIS Control 14.6 - Protect Information through Access Control Lists

3.3 Ensure 'Orphaned Users' are Dropped from SQL Server Databases
- Automated control
- CIS Control 16.8 - Disable Any Unassociated Accounts

3.4 Ensure SQL Authentication is not used in contained databases
- Automated control
- CIS Control 16.2 - Configure Centralized Point of Authentication

3.5 Ensure the SQL Server's MSSQL Service Account is Not an Administrator
- Manual control
- CIS Control 4.3 - Ensure the Use of Dedicated Administrative Accounts

3.6 Ensure the SQL Server's SQLAgent Service Account is Not an Administrator
- Manual control
- 4.3 Ensure the Use of Dedicated Administrative Accounts

3.7 Ensure the SQL Server's Full-Text Service Account is Not an Administrator
- Manual control
- CIS Control 4.3 - Ensure the Use of Dedicated Administrative Accounts

3.8 Ensure only the default permissions specified by Microsoft are granted to the public server role
- Automated control
- CIS Control 14.6 - Protect Information through Access Control Lists

3.9 Ensure Windows BUILTIN groups are not SQL Logins
- Automated control
- CIS Control 14.6 - Protect Information through Access Control Lists

3.10 Ensure Windows local groups are not SQL Logins
- Automated control
- CIS Control 14.6 - Protect Information through Access Control Lists

3.11 Ensure the public role in the msdb database is not granted access to SQL Agent proxies
- Automated control

Revision History
AUGUST 2021 - MLE

- CIS Control 14.6 - Protect Information through Access Control Lists

Password Policies

4.1 Ensure 'MUST_CHANGE' Option is set to 'ON' for All SQL Authenticated Logins
- Manual control
- CIS Control 4.2 - Change Default Passwords

4.2 Ensure 'CHECK_EXPIRATION' Option is set to 'ON' for All SQL Authenticated Logins Within the Sysadmin Role
- Automated control
- CIS Control 16.10 - Ensure All Accounts Have An Expiration Date

4.3 Ensure 'CHECK_POLICY' Option is set to 'ON' for All SQL Authenticated Logins
- Automated control
- Cis Control 4.4 - Use Unique Passwords

Auditing and Logging

5.1 Ensure 'Maximum number of error log files is set to greater than or equal to '12.'
- Automated control
- CIS Control 6.4 - Ensure adequate storage for logs

5.2 Ensure the 'Default Trace Enabled' Server Configuration Option is set to '1.'
- Automated control
- CIS Control 6.3 - Enable Detailed Logging

5.3 Ensure 'Login Auditing' is set to 'failed logins'
- Automated controls
- CIS Control 16.13 - Alert on Account Login Behavior Deviation

5.4 Ensure 'SQL Server Audit' is set to capture both 'failed' and 'successful logins'
- Automated controls
- CIS Control 4.9 - Log and Alert on Unsuccessful Administrative Account Login

Application Development

6.1 Ensure Database and Application User Input is Sanitized
- Manual control
- CIS Control 18.2 - Ensure Explicit Error Checking is Performed for All In-house Developed Software

6.2 Ensure 'CLR Assembly Permission Set' is set to 'SAFE_ACCESS' for All CLR Assemblies
- Automated control
- CIS Control 5.1 - Establish Secure Configurations

Encryption

7.1 Ensure 'Symmetric Key encryption algorithm' is set to 'AES_128' or higher in non-system databases
- Automated control
- CIS Control 14.4 - Encrypt All Sensitive Information in Transit

7.2 Ensure Asymmetric Key Size is set to 'greater than or equal to 2048' in non-system databases
- Automated control
- CIS Control 14.4 - Encrypt All Sensitive Information in Transit

Additional Considerations

8.1 Ensure 'SQL Server Browser Service' is configured correctly
- Manual control
- CIS Control 9.2 - Ensure Only Approved Ports, Protocols and Services Are Running

Revision History
AUGUST 2021 - MLE

Appendix B
Secure Configuration Check List

Secure Database Configuration Check List – MS SQL			
Control Description		Set Correctly	
		Yes	No
1	**Installation, Updates, and Patches**		
1.1	Ensure Latest SQL Server Cumulative and Security Updates are Installed (Automated)	☐	☐
1.2	Ensure Single-Function Member Servers are Used (Manual)	☐	☐
2	**Surface Area Reduction**		
2.1	Ensure 'Ad Hoc Distributed Queries' Server Configuration Option is set to '0' (Automated)	☐	☐
2.2	Ensure 'CLR Enabled' Server Configuration Option is set to '0' (Automated)	☐	☐
2.3	Ensure 'Cross DB Ownership Chaining' Server Configuration Option is set to '0' (Automated)	☐	☐
2.4	Ensure 'Database Mail XPs' Server Configuration Option is set to '0' (Automated)	☐	☐
2.5	Ensure 'Ole Automation Procedures' Server Configuration Option is set to '0' (Automated)	☐	☐
2.6	Ensure 'Remote Access' Server Configuration Option is set to '0' (Automated)	☐	☐
2.7	Ensure 'Remote Admin Connections' Server Configuration Option is set to '0' (Automated)	☐	☐
2.8	Ensure 'Scan For Startup Procs' Server Configuration Option is set to '0' (Automated)	☐	☐
2.9	Ensure 'Trustworthy' Database Property is set to 'Off' (Automated)	☐	☐
2.10	Ensure Unnecessary SQL Server Protocols are set to 'Disabled' (Manual)	☐	☐
2.11	Ensure SQL Server is configured to use non-standard ports (Automated)	☐	☐
2.12	Ensure the 'Hide Instance' option is set to 'Yes' for Production SQL Server instances (Automated)	☐	☐
2.13	Ensure the 'sa' Login Account is set to 'Disabled' (Automated)	☐	☐
2.14	Ensure the 'sa' Login Account has been renamed (Automated)	☐	☐
2.15	Ensure 'AUTO_CLOSE' is set to 'OFF' on contained databases (Automated)	☐	☐
2.16	Ensure no login exists with the name 'sa' (Automated)	☐	☐
3	**Authentication and Authorization**		
3.1	Ensure 'Server Authentication' Property is set to 'Windows Authentication Mode' (Automated)	☐	☐
3.2	Ensure CONNECT permissions on the 'guest' user is Revoked within all SQL Server databases, excluding the master, msdb, and tempdb (Automated)	☐	☐
3.3	Ensure 'Orphaned Users' are Dropped From SQL Server Databases (Automated)	☐	☐
3.4	Ensure SQL Authentication is not used in contained databases (Automated)	☐	☐
3.5	Ensure the SQL Server's MSSQL Service Account is Not an Administrator (Manual)	☐	☐
3.6	Ensure the SQL Server's SQLAgent Service Account is Not an Administrator (Manual)	☐	☐
3.7	Ensure the SQL Server's Full-Text Service Account is Not an Administrator (Manual)	☐	☐
3.8	Ensure only the default permissions specified by Microsoft are granted to the public server role (Automated)	☐	☐
3.9	Ensure Windows BUILTIN groups are not SQL Logins (Automated)	☐	☐
3.10	Ensure Windows local groups are not SQL Logins (Automated)	☐	☐

Revision History
AUGUST 2021 - MLE

3.11	Ensure the public role in the msdb database is not granted access to SQL Agent proxies (Automated)	☐	☐
4	**Password Policies**		
4.1	Ensure the 'MUST_CHANGE' Option is set to 'ON' for All SQL Authenticated Logins (Manual)	☐	☐
4.2	Ensure the 'CHECK_EXPIRATION' Option is set to 'ON' for All SQL Authenticated Logins Within the Sysadmin Role (Automated)	☐	☐
4.3	Ensure the 'CHECK_POLICY' Option is set to 'ON' for All SQL Authenticated Logins (Automated)	☐	☐
5	**Auditing and Logging**		
5.1	Ensure 'Maximum number of error log files is set to greater than or equal to '12' (Automated)	☐	☐
5.2	Ensure 'Default Trace Enabled' Server Configuration Option is set to '1' (Automated)	☐	☐
5.3	Ensure 'Login Auditing' is set to 'failed logins' (Automated)	☐	☐
5.4	Ensure 'SQL Server Audit' is set to capture both 'failed' and 'successful logins' (Automated)	☐	☐
6	**Application Development**		
6.1	Ensure Database and Application User Input is Sanitized (Manual)	☐	☐
6.2	Ensure 'CLR Assembly Permission Set' is set to 'SAFE_ACCESS' for All CLR Assemblies (Automated)	☐	☐
7	**Encryption**		
7.1	Ensure 'Symmetric Key encryption algorithm' is set to 'AES_128' or higher in non-system databases (Automated)	☐	☐
7.2	Ensure Asymmetric Key Size is set to 'greater than or equal to 2048' in non-system databases **(Automated)**	☐	☐
8	**Appendix: Additional Considerations**		
8.1	Ensure 'SQL Server Browser Service' is configured correctly (Manual)	☐	☐

Revision History
AUGUST 2021 - MLE