**SQL Server Security Standards and Guidelines**

This document list down the SQL security standards and guidelines which would help to manage the SQL server security and users more efficiently.

1. Create windows security groups for the group of employees who has same responsibilities. For examples, for all junior SQL database administrators or project DBA or a sql contractor create a group sql\_junioradmin. Similarly, you may have the sql\_biadmin, sql\_appsupport\_level1, sql\_appsupport\_level2, sql\_appsupport\_level3 security to groups. Or uses windows AD or security group naming conventions to create the SQL groups listed before.
2. Create the SQL login using the security group GLS\sql\_junioradmin instead of individual windows account.
3. Use the SQL group login names to assign members of a fixed Server Role and fixed database Role.
4. Create custom server roles and database roles. While adding members use the security group corresponding to a role.
5. Use following scripts or template to define the SQL Roles.
6. **Senior Database Administrator Role - Sysadmin**

User added to the sysadmin server role can perform an activity on the server.

**Script:** **[SITM-SQL-01] C:\DBA\SysAdmin.sql**

1. Creates a login for a give windows account.
2. Add the account to the sysadmin group.
3. **Junior Database Administrator Role – (svr\_juniorDBA and db\_juniorDBA)**

This user added to this group will have a limited database administrator privileges delegated by the senior database administrator. The user may be junior or beginner resource or a contractor or development team resource contributing to achieve project goals or department goals.

The best practice and recommended approach is to create a server role and database role and assign the user windows account or security Group account to both custom server role and database role. The server DBA role would be configured for set the **CONTROL** access, practically still the DBA account will have all the **sysadmin** rights until database role created is configured with the list of Deny rules. Refer the following script to create the Server Role and Database Roles.

**Script:** **[SITM-SQL-01] C:\DBA\Junior DBA.sql**

1. Creates Server Roles with Control Access
2. Create the Database Roles with Some Deny Rules
3. Create Or assign a user to the role.
4. **Infrastructure Support Level 1 Role - Infra\_Support\_l1**

User added to role will have Read-Only access to all databases on a server.

Recommendation is to use the fixed database role called db\_datareader. Use it to configure maintain and control the privileges for the group. This will require to add individual users accounts or windows security group to db\_datareader role at each database level.

**Script: [SITM-SQL-01] C:\DBA\Infra\_Support\_l1.sql**

1. Create a SQL login for the configured windows security group and the associated account.
2. Create database user account.
3. Add the windows account or security group as a member to each database fixed database role – db\_datareadonly.
4. **Application Support level 3 Role - App\_support\_l2**

User added to this role will have Read-Only, Write, Execute, SQL Agent Operator, SSIS DB operator access to msdb system database or the server.

The recommended approach is to create a database Role App\_Support\_l2 at msdb system database level and assign the execute permission. Add the user accounts to app\_Support\_l2 along with db\_datareader, db\_datawrite, SQLAgentOperatorRole, db\_ssisoperator

**Script:** **C:\DBA\app\_support\_l2.sql**

1. Create a SQL login for the configured Windows Account.
2. Create Database User Account for the msdb system database.
3. Add the Windows Account or Security group as a member to each of these database roles app\_support\_l2, db\_datareader, db\_datawrite, SQLAgentOperatorRole, and db\_ssisoperator.
4. **Application Support level 3 Role - App\_support\_l3**

User added to this role will have read and execute access all databases on a server.

The recommended approach is to create a database Role App\_Support\_l3 and assign the execute permission. Add the user accounts to app\_Support\_l2 and db\_datareadonly

**Script: C:\DBA\app\_support\_l3.sql**

1. Create a SQL login for the configured Windows Account.
2. Create Database User Account for all databases.
3. Add the Windows Account or Security group as a member to each of these database roles app\_support\_l3, db\_datareadonly.
4. **BI Administrator Role – bi\_admin**

User added to this role will have Read, Write and Execute access for databases on a server.

The recommended approach is to create a database Role **bi\_admin** and assign the execute permission. Add the user accounts to **bi\_admin**, db\_datareadonly and db\_datawrite roles

**Script: C:\DBA\bi\_admin.sql**

1. Create a SQL login for the configured Windows Account.
2. Create Database User Account for all databases.
3. Add the Windows Account or Security group as a member to each of this database to bi\_admin, db\_datareadonly and db\_datawrite roles.
4. **TEST Accounts**
5. GLS\bi\_admingroup

GLS\WindowsUser1 \ UJV"0^Td%J&E

GLS\WindowsUser2 \ JGVGq%4u:bNT

2. GLS\dba\_junioradmin

GLS\WindowsUser3 \ H2e.8yewV3zj

GLS\WindowsUser4 \ R~V5M\*!ad8uu

3. GLS\app\_support\_l2

GLS\WindowsUser5 \ L%7s%R6u$'EN

GLS\WindowsUser6 \ wXe.?Q3!SeHn

1. GLS\app\_support\_l3

GLS\WindowsUser7 \ @q`68gGB/Q8[

WindowsUser8 \ VGtrWAx~K(,q

5. GLS\Infra\_support

WindowsUser9 \ CYqdc-u#;fTH

WindowsUser10 \ jB64w]X5EST+