**Revision Details**

|  |  |  |
| --- | --- | --- |
| Date | Author | Version Description |
|  |  |  |
|  |  |  |
|  |  |  |

**Reviewers**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Position | Date | Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Approving Authority**

Delete this text once the following steps are done:

1. Got to the Insert Tab and click on ‘Signature Line’.
2. Click ‘Ok’.
3. Enter Approving Personnel’s Information and click ‘Ok’.
4. Have Approving Authority revise the document and sign it.

**Points of Contact**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Position | Extension | E-mail |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Introduction 2](#_Toc437327721)

[Purpose 2](#_Toc437327722)

[Scope 2](#_Toc437327723)

[SQL 2012 STIG Related Settings and Configurations 2](#_Toc437327724)

[Backup and Recovery Procedures 2](#_Toc437327725)

[Disaster Recovery Procedures 2](#_Toc437327726)

[Data at Rest 2](#_Toc437327727)

[SQL Audits 2](#_Toc437327728)

[File Permissions 2](#_Toc437327729)

[Installation Account 3](#_Toc437327730)

[DBA 3](#_Toc437327731)

[Ports and Protocols 3](#_Toc437327732)

[V-40934 Programmability 3](#_Toc437327733)

[V-40907 4](#_Toc437327734)

[V-40917 4](#_Toc437327735)

[V-40932 4](#_Toc437327736)

[V-40941 4](#_Toc437327737)

[V-40945 4](#_Toc437327738)

[V-41044 4](#_Toc437327739)

[V-41047 4](#_Toc437327740)

[V-41307 5](#_Toc437327741)

[Login List 5](#_Toc437327742)

[Direct Permissions Assignment to Logins 5](#_Toc437327743)

[Server Role Permissions Assignment 5](#_Toc437327744)

[Server Role Membership 5](#_Toc437327745)

[Database-Level Documentation 5](#_Toc437327746)

[Appendix 5](#_Toc437327747)

[TDE 5](#_Toc437327748)

[SQL Server Audits 6](#_Toc437327749)

# Introduction

# Purpose

The SQL Server STIG System Security Plan Addendum will document all settings and configurations related to a specific-instance’s SQL STIG settings and policy compliance. This document will explain and detail the pre-defined posture of a SQL Server 2012 Server or cluster.

# Scope

The SQL Server STIG System Security Plan Addendum will be generated for each SQL Server system in the enclave. There is one document per instance, including multiple nodes per instance.

# SQL 2012 STIG Related Settings and Configurations

## Backup and Recovery Procedures

The system will be backed-up in accordance with the Enclave’s backup and recovery requirements defined in the document here <link document or paste copy here>

## Disaster Recovery Procedures

Disaster Recovery procedures for restoring this server and databases in our DR site can be found at:

<link document or paste copy here>

## Data at Rest

The system will have data-at-rest protected by Microsoft SQL Server Transparent Database Encryption (TDE). Please see the addendum for more information and a description of the configuration and test plan.

Only DBAs and Auditors will have access to the encryption keys and online databases.

## SQL Audits

The system will use SQL Server Auditing to support the SQL auditing requirements of the instance. Please see the addendum for more information on SQL Server Audits and the configuration (as well as, mapping from the SQL STIG event IDs to SQL Audit criteria).

Audit data will be retained on the system for less than XX days and data will be backed up and archive for an extended period of time.

Only DBA and auditors will have access to the audit data.

**File Permissions**

SQL Server 2012 File Permissions changes are unsupported by Microsoft. The Engineers tested the SQL Server 2012 STIG permissions changes in a lab; it caused unrepairable damage to the Instance. Until the changes can be successfully tested, the organization has chosen not to alter this setting due to their un supported nature and the additional risk they present to the services availability. The below SQL 2012 STIG items will not be altered.

Microsoft Premier Services has advised this customer that any SQL STIG related changes to the baseline ACL of the SQL server directories and logs may result in ability to patch or update the instance. The customer would then have to re-install and restore the databases to recover and patch the service.

V-40944 (the baseline file or log directory ACL)

V-41016

V-41017

V-41040

V-54859

V-54879

V-54881

**Installation Account**

This is the account used to install SQL server and the designated owner of all the binaries and files.

<InstallAccount>

Use of Installation account is logged monitored by Quest. The account is disabled when not in use. The account is only to be used to install and patch the instance.

**DBA**

Below is the list of the approved DBA group and members.

List Groups

List Users

**Ports and Protocols**

##### TCP Port is used by default for all 2012 Instances.

**V-40934 Programmability**

The attached file list all custom code on the instance. See SSP-A Results.xlsx

<paste results or embed results file here>

**V-40907**

SSL encryption is enabled on the instance.

<paste output from query or notes>

**V-40917**

All databases on the instance are encrypted.

<paste output from query or notes>

**V-40932**

See SSP-A Results.xlsx

**V-40941**

Paste into PowerShell. This checks for SQL Server Data Tools (no output is idea).

$servers = @("server","server1")

$cmd = { Write-Host $env:COMPUTERNAME; Get-ChildItem HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall | % { Get-ItemProperty $\_.PSPath } | ? { $\_.DisplayName -match "SQL Server Data Tools" } }

$servers | % { Invoke-Command -ComputerName $\_ -ScriptBlock $cmd }

**V-40945**

product\_version product\_level

<paste output from query or notes>

**V-41044**

See SSP-A Results.xlsx

**V-41047**

<paste output from query or notes>

**V-41307**

The sa account is listed below. The account is also disabled and password is set to a random value.

<sa account name here>

**Login List**

See SSP-A Results.xlsx

**Direct Permissions Assignment to Logins**

See SSP-A Results.xlsx

**Server Role Permissions Assignment**

See SSP-A Results.xlsx

**Server Role Membership**

Role Login

<paste output from query or notes>

# Database-Level Documentation

**Encrypted data and Symmetric Keys**

# Appendix

**TDE**

Below is the data-at-rest encryption information and process for Microsoft SQL Server TDE



**SQL Server Audits**

Below is the information and process for SQL Server Audits

