

Department of Veterans Affairs

VistA Scheduling Enhancements (VSE)

Security Guide Update

Version 3.1



December 2016

Revision History

Date	Version	Description	Author
02/09/2017	3.1	Added Shareholder's Approval	VSE PMO
12/02/2016	3.1	Updated for Additional Enhancements work to add additional security key, section 2.5	D. Vick, PM; E. Phelps, Sr. TW
12/24/2015	3.0	Document Submission	D. Vick, PM; M. Woehrle, PM
12/23/2015	2.2	TW Review Performed	G. Scorca, Sr. TW
12/18/2015	2.1	Incorporated VAR, NSR002, OT3 and OT4. Removed Enh 1, Enh 2, and Enh 3 from document name.	D. Vick, PM
03/18/2015	2.0	Incorporated Enhancement 3	D. Vick, PM; B. Tomlin, Dev.; G. Scorca, TW
01/22/2015	1.0	Initial Version for Submission	E. Merica E. Crean, TW M. Colyvas, TW

Table of Contents

1. Introduction	1
2. Security Guide.....	1
2.1. Security/Identity Management	1
2.2. Continuity of Operations	1
2.3. Disaster Event Activities	1
2.4. Rules of Behavior	1
2.5. Security Keys	2
3. VSE User Guide.....	3
3.1. User Access Levels	3
4. Approval Signatures	4

1. Introduction

This document serves to assist Veterans Health Information Systems and Technology Architecture (VistA) Information Security and System Administration personnel by identifying potential security control implementation updates related to the VistA Scheduling Enhancements (VSE) project. Documentation support is provided for the System Security Plan (SSP) and Information System Contingency Plan (ISCP).

- Security control implementation evidence for the SSP is based on requirements in *VA Handbook 6500 Appendix D* and *NIST Special Publication 800-53 Revision 4*.
- ISCP items are based on requirements in *VA Handbook 6500.0, IT Contingency Planning*.

2. Security Guide

The sections below identify items as part of security control implementation evidence requirements of *VA Handbook 6500 Appendix D* and contingency planning items of *VA Handbook 6500.8*.

2.1. Security/Identity Management

Security/Identity management for VSE project is managed by current VistA Security/Identity management protocols and is not affected by the VSE enhancements.

2.2. Continuity of Operations

There is no additional information to add to Continuity of Operations documentation.

2.3. Disaster Event Activities

This document does not provide any additional detail for use in a facility-specific Disaster Recovery Plan (DRP), which is the first go-to plan for each facility.

2.4. Rules of Behavior

All VistA users are required to observe Health and Human Services (HHS) and Department of Veterans Affairs (VA) Rules of Behavior regarding patient privacy and the security of both patient information and VA computers and networks. Evidence of this control is documented as part of the Planning control PL-4, Rules of Behavior.

2.5. Security Keys

The database security keys that define access features for different application users are listed in the table below. This information can be applied to Access Controls AC-5, Separation of Duties, and AC-6, Least Privilege.

Table 1: Security Keys

Key Name	Description
SDECZMENU	All Vista Scheduling users must have this key to access to the following options Tasks Tab: <ul style="list-style-type: none">• Actions button• Arrangement button• Tools button• Clinic Schedules button• Provider Schedules button• Clinic Group button System Tab <ul style="list-style-type: none">• Availability button Reports tab: <ul style="list-style-type: none">• Audit Activity• EWL- Non Display Patients• Clinics• Managements Report (E3)
SDECZMGR	This key should be assigned to users who manage the overall Scheduling application. This key gives access to the Scheduling Management icon on the VSE applications System tab.
SDECZ REQUEST	Allows holder of key to access VAR mobile request icon and view mobile request list from the VAR application
SDOB	Authorized to overbook in the clinic to maximum allowed as defined in set up a clinic
SDMOB	Authorized to overbook in the clinic over the maximum allowed as defined in set up a clinic.
SDWL MENU	If user does not have this key assigned they cannot enter a new wait list request (right click option "Transfer to EWL" from an open APPT Request) or perform a disposition (which is the right click option for EWL Disposition) of a EWL request.
SDECVIEW	This key is assigned to users who need access to the Scheduling application but are not allowed to take action on any requests or schedules. This key gives access to the VistA Scheduling Graphical User Interface (VS GUI) application's Tasks tab view only. This key overrides any other scheduling key assigned to the user and restricts access to all adding and updating capabilities.

3. VSE User Guide

3.1. User Access Levels

Section 2.2: User Access Levels of the *VSE User Guide* describes the rights available through each of the user access levels. This information can be applied to Access Control AC-5, Separation of Duties, and AC-6, Least Privilege.

4. Approval Signatures



DM Approval Updated Security Guide.ms

Debbie Malkovich
Scheduling Systems Program Manager, OVAC
Business Sponsor

Date



RS Approval Updated Security Guide.ms

Robert Schmidt
Project Manager/COR

Date