OFFICE OF INFORMATION AND TECHNOLOGY
IT Operations and Services

Standard Operating Procedure VistA Service Accounts

May 29, 2019| VAD, Applications/Kernel Infrastructure

Revision History

Date	Version	Description	Author
05/29/2019	1.0	Initial SOP creation	Rhoda M. Tyson

Table of Contents VistA Service Accounts

OFFICE OF INFORMATION AND TECHNOLOGY
IT Operations and Services

VistA Service Accounts Standard Operating Procedure

1 Purpose

To establish procedures and responsibilities for VistA Service Accounts creation, review, password changes.

2 Definitions

VistA Service Accounts are used by a service, program, application, or other process that require authentication. VistA Service Accounts are identified by User Class (Connector Proxy or Application Proxy). Verify code for VistA Service Accounts will be set to Never Expire equals Yes and are not assigned Elevated Privileges.

VistA Service Accounts shall be set with complex passwords, they must be12-20 characters mixed alphanumeric and punctuation (except '^', ';', ':'). VistA Service Accounts shall be reviewed each semi-annual to ensure they are still required, and that the Termination Reason field within Vista under New Person File (File 200) continues to accurately reflect the Account Information Owner for the account.

VistA Service Accounts should have the password changed at least every 3 years, except for National Service Accounts (Appendix A). This shall be documented in the Termination Reason Field of the New Person File (File 200) with the statement "National Do Not Change". Care should be taken when changing the password of a Service Account, as the change must be coordinated with the Account Information Owner and on the remote system manager, which use the account to authenticate services.

For Internal Use Only

R2PBC GUI reports shall be used to create a report identifying VistA Service Accounts which will require a password change in the upcoming 6 Months.

3 Roles

Vista Application Division Kernel Section will conduct a Semi-Annual Service Account Review by running a report from the R2PBC GUI of the Service Accounts.

VAD Kernel Section will enter a ServiceNow ticket documenting the review was completed. Accounts that require attention will have a child ticket generated to the appropriate Account Information Owner for password change coordination with identified site to minimize system interruptions.

4 Responsibility

4.1 Account Information Owners

Account Information Owners can be any of the following VistA Application Division(s): Admin/Finance, BSSL Business Critical, Clinical, COTS or Kernel/Infrastructure.

4.1.1 Account Information Owners are responsible for the creation of VistA Service Accounts.

4.1.2 Account Information Owners are responsible for the change of Verify Codes.

4.1.3 Account Information Owners are responsible for the support of the VistA Service Accounts that fall under their section.

5 Process Overview

5.1 Account Creation Procedures:

1. Log-in to Vista

2. Access the Menu Option: FOUNDATIONS MANAGEMENT (XOBU SITE SETUP MENU)

3. Choose CP: **Enter/Edit Connector Proxy User**

4. At the Enter NPF CONNECTOR PROXY NAME: prompt they will enter the appropriate name

For Internal Use Only

5. Are you adding 'XXXXXX,XXXXXXXX' as a NEW PERSON (the XXXXXXTH)? No// Answer: **Yes**

6. At the Want to edit ACCESS CODE (Y/N): <enter> **Y**

7. Copy the Auto Generated Access Code. If one is not Autogenerated you will be able to create your own.

8. At the Do you want to keep this one? YES// <enter> **Y**es

9. At the Please re-type the new code to show that I have it right: Type in the new Access Code that was given.

10. At the Want to edit VERIFY CODE (Y/N): <enter> **Y**

11. Type in a new Verify Code which must be12-20 characters mixed alphanumeric and punctuation (except do not enter: '^’, ‘;' , ':').

12. At the Please re-type the new code to show that I have it right: prompt Please Type in the new Verify Code that you created.

13. Type **Q**uit

14. Go into VA Fileman

15. Choose Enter Or Edit File Entries

16. At the Input to what File: OPTION// Prompt Type New Person

17. At the EDIT WHICH FIELD: ALL// Prompt Type VERIFY CODE NEVER EXPIRES

18. At the THEN EDIT FIELD: Prompt Type 9.4

19. At the next THEN EDIT FIELD: Prompt just hit enter

20. At the Select NEW PERSON NAME: Type in the VistA Service Account Name you created

21. At the VERIFY CODE never expires: **Y**es// Prompt make sure it is set to Yes.

22. At the Termination Reason: Prompt Put in the Account Information Owner.

23. At the next Select NEW PERSON NAME: Prompt just hit enter and close Fileman

5.2 Review Procedures:

1. Vista Applications Division Kernel Section will Initiates a Semi-Annual Review using the R2PBC GUI.

For Internal Use Only

2. Vista Applications Division Kernel Section will create a Parent ServiceNow Incident.

3. Enter “FYXX Mid-Year Review” or “FYXX End of Year Review,” site name (station number), and “VistA Service Account Review Completed” in the short description field (where XX is the current Fiscal Year).

4. Enter “see child ticket(s)” or “no deficiencies found” in the description field.

5. Vista Applications Division Kernel Section will create a child incident for every VistA Service Account to meet 3- Year Verify Code Compliance requirement.

6. Enter the site name, and the VistA Service Account name, Review for Compliance in the short description field

7. Enter either “Admin/Finance,” “Clinical,” “Infrastructure,” “COTS,” or “Business Critical” and the VistA Service Account name, codes are older than 3 years or within 180 days from expiring in the description Field.

8. Vista Applications Division Kernel Section will assign ServiceNow Incident to the appropriate Account Information Owners.

9. Enter the assignment group for the team responsible for completing the review:

    Admin/Finance: IO.HBMC.FO.APP.VADADMIN.Triage

    Clinical: IO.HBMC.FO.APP.VADCLIN.Triage

    Infrastructure: IO.HBMC.FO.APP.VADKERNEL.TRIAGE

    COTS: IO.HBMC.FO.APP.COTSTriage

    Business Critical: IO.HBMC.FO.HEALTHSYSTEMS.TRIAGE

10. Account Information Owners will work with the remote vendor or system to coordinate the Verify Code Change.

11. If a Verify Code Change must be completed the Account Information Owner will complete the change.

12. If VistA Service Account is no longer in use, Service Information Owner will need to Terminate/DISUSER the account.

13. Account Information Owners will close out the Child Incident in ServiceNow

14. Vista Applications Division will monitor the Parent ServiceNow Incident and close it out when all Child Incidents are closed.

6 References

6.1 VA Handbook 6500

6.2 VA Handbook 6500 Appendix F

For Internal Use Only

7 Rescissions

8 Review

SOP will be reviewed no later than 05/29/2021.

9 Concurrence

Approved/~~Disapproved~~

Stefan G. Test 122392 Digitally signed by Stefan G. Test 122392
Date: 2020.02.04 07:55:43 -06'00'

Signed: Stefan Test Date:

Applications Manager, Infrastructure Operations (IO)

Approved/~~Disapproved~~

Michael J. Giurbino 172493 Digitally signed by Michael J. Giurbino 172493
Date: 2020.02.04 08:57:14 -05'00'

Signed: Michael Giurbino Date:

Director, Health, Benefits, Memorial and Corporate (HBMC)

For Internal Use Only

Appendix A:

Exempted VistA Service Accounts

1. All Application Proxy Service Accounts are exempted from 3 year Verify Code Change.

2. National Service Accounts and Verify Codes cannot be changed without breaking functionality:

    1. VISTALINK, EMC
    2. VISTALINK, EDIS
    3. VISTALINK, HINES

Service Account Listings per sites are located:
https://vaww.esl.portal.va.gov/applications/vistaapps/vista_infra/Pages/SvcAccntAudit.aspx

R2PBC User Guide

R2PBC GUI USER GUIDE.docx

For Internal Use Only