

AHS Account Management Standard

Jack Green

10/3/2013

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connector's security control requirements for the Account Management (AC-2, AC-2(2), AC-2(3), AC-2(4), AC-7) Controls.

Revision History

Date	Version	Description	Author
	1.0	Created Document	Department of Children and Family
8/16/2013	2.0	Document revised for VHC standards	Jack Green
10/4/2013	3.0	Procedures reviewed and adapted for VHC business processes and security requirements	Jack Green

PURPOSE/STANDARD STATEMENT:

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connector's security control requirements for the Account Management (AC-2, AC-2(2), AC-2(3), AC-2(4), AC-7) Controls.

The information systems covered in this procedure document contain but are not limited to the following:

- VHC website
- VHC Portal
- VHC workstations
- AHS Network Accounts
- AHS E-Mail accounts

SCOPE

The scope of this standard includes the VHC system and its constituent systems only

STANDARD

Establishing and activating accounts

1. Before the System Administrator can grant access to any VHC information systems, they require the following:
 - A valid access authorization.
 - i. If the request is for FTI Access, the business lead and supervisor must approve.
 - One valid role.
 - Other attributes as required by VHC or associated business functions.
2. Access requirements must be identified by the System/Business Owner for newly assigned personnel, personnel whom have a change of status or personnel whom are no longer with VHC. Additionally, required access levels (roles) must be defined by the System/Business Owner for each application and system they are responsible for prior to providing access to those personnel.
3. By default, each user must be assigned only the minimum access privileges he or she requires for any system in which they have been provisioned an account.
4. Normal system or application users **never** have access rights provided for any administration or security functions in any system.
5. Before an employee requests access to any information system account , they must adhere to the following requirements:

- Proper identification.
 - Completion of Security and Awareness Training.
 - Completion of HIPAA, PII Training.
 - Signed (handwritten or digital) access request forms indicating that the account recipient accepts of all compliance rules and regulations.
6. Before an employee requests access to an information system account with access to FTI data, they must adhere to the following requirements:
- Proper identification.
 - Completion of Security and Awareness Training.
 - Completion of HIPAA, PII Training.
 - Completion of FTI Training
 - If the request is for FTI Access, the business lead and supervisor must approve.
 - Signed (handwritten or digital) access request forms indicating that the account recipient accepts of all compliance rules and regulations.
7. Requests to establish any information system account such as email must adhere to the following:
- Approval of requests to establish information system accounts must be stored electronically.
8. In order to obtain access to the system, authorized users must be identified before the request and their access rights/privileges must be specified in the request. The system access request and account creation processes are below but not limited to the following:
- VHC Website:
 - i. No account is required to access publically available information.
 - VHC Customer Portal
 - i. Submit request for access from the portal by clicking “Organizations/Individuals Enter Here”.
 - ii. If not registered on the portal yet, click on the link “Please click here to apply.” If registered on the portal, input logon credentials.
 - iii. Access levels provided are standard across the VHC profiles.
 - VHC State Portal:
 - i. Access can only be granted by VHC’s Business Application Support Unit (BASU) and can only be done once the grant is awarded and approved.
 - ii. The BASU will create the account and grant access by providing the login information to the user of record.
 - iii. Access levels provided are standard across the State profiles.
 - VHC WAN Access:
 - i. Access can only be granted by BASU and can only be done once the grant is awarded and approved.

- ii. If FTI access is required, the BASU will verify that the individual has received appropriate training and **two** authorizations for FTI data.
 - iii. The MAO will create the account and grant access by providing the login information to the user of record.
 - iv. Access levels provided are standard across the State profiles.
 - Administration Portal:
 - i. Administrators must submit a request for access to the CGI customer support service.
 - ii. The CGI customer support service determines the appropriate access levels.
9. All access requests made via the user account request process are validated for the following by the System Administrator prior to processing:
 - System/Business administration must only process requests for access when they have been formally submitted and approved by the employee's management.
 - Requests must contain the employee's name and business justification for access.
 - All mandatory fields in the access request form must be completed prior to seeking management approval and account creation.
10. All provisioned user accounts remain active unless the employee is transferred and no longer requires access, or the employee is terminated.
11. Accounts created for emergency purposes are automatically disabled after 24 hours.
12. Temporary accounts will have a lifespan of less than 365 days.

Account Modifications

1. The following rules must be followed regarding account modification:
 - System/Business Owner must be notified by and approved by employee supervisor when their employee's access levels require a change.
 - Requests to modify information system accounts must be documented in writing by the submitter and stored electronically by the system administrator.

User activity logging and access review

1. The activities of all users must be supervised and reviewed by the System owner or administrator with respect to the enforcement and usage of information system access controls. If a user is found to be out of compliance per Access Control Policy, he/she will face disciplinary action including loss of account and access or additional penalties.

2. The information system owner shall ensure that all information system access is consistent with defined, documented, and approved user access requirements, roles and responsibilities, and account privileges.
3. System access must be reviewed by System/Business owner at least every 30 days to ensure that appropriate levels of access are permitted and provided only to authorized personnel.
4. Access controls must be reviewed every 30 days to ensure that access rights are removed for transferred or terminated employees, security controls are tested and cannot be bypassed, and employee access levels are setup appropriately per employee responsibilities.

Account deactivation

1. System Administrators managers shall review system accounts every 180 days to identify and deactivate accounts that have been inactive for 180 days or more.
2. When deactivating an account, the System Administrator must ensure that the activity is logged and management is notified of the deactivation.
3. When an employee transfers from his/her function with VHC, all roles associated with that user must be deactivated immediately (i.e. VHC Website, VHC State Portal, VHC Network Account, E-mail Account).
4. When an employee terminates his/her employment with VHC, all accounts associated with that user must be deactivated immediately i.e. VHC Website, VHC State Portal, VHC Network Account, E-mail Account).
5. When a contractor employee transfers from his/her function with VHC, all accounts associated with that user must be deactivated immediately (i.e. VHC Website, VHC State Portal, VHC Network Account, E-mail Account).
6. When a contractor employee terminates his/her employment with VHC, all accounts associated with that user must be deactivated immediately i.e. VHC Website, VHC State Portal, VHC Network Account, E-mail Account).
7. The System Administrator must disable any account which has been inactive in excess of 180 days and log all actions taken electronically.
8. The System Administrator will disable any account for an employee who is not in compliance with mandatory trainings per policy and compliance.

Account lockout

1. The information system enforce a limit of three (3) consecutive invalid login attempts by a user during a 15-minute time period.
2. For privileged and non-privileged accounts, the information system must automatically lock the account permanently, requiring a helpdesk call to reinstate the account, when the maximum number of unsuccessful login attempts is exceeded.

3. If the account has access to FTI data, the information system must automatically lock the account and suspend the account until an administrator reinstates the account when the maximum number of unsuccessful login attempts is exceeded.
4. Users should be permitted access to the help desk to release their account in the event it hinders productivity.

Password reset

1. VHC Website
2. VHC Customer Portal
 - Self-servicing Password Reset
 - i. From the login page, select the link “Password Retrieval” in the lower right corner. They then will be prompted to input the organization E-mail address to have the password reset details sent.
 - Administrative Password Reset
 - i. A Password Reset requires is sent to the MOU, and upon verification of user, the MOU will reset the password.
 - ii. A notification will be sent to the user confirming that the password has been reset.
3. VHC State Portal
 - Self-servicing Password Reset
 - i. From the login page, select the link “Password Retrieval” in the lower right corner. They then will be prompted to input the organization E-mail address to have the password reset details sent.
 - Administrative Password Reset
 - i. A Password Reset requires is sent to the MOU, and upon verification of user, the MOU will reset the password.
 - ii. A notification will be sent to the user confirming that the password has been reset.
4. VHC WAN
 - Administrative Password Reset
 - i. A Password Reset is sent to the MOU, and upon verification of user, the MOU will reset the password.
 - ii. A notification will be sent to the user confirming that the password has been reset.

IMPORTANT INFORMATION

These procedures can be found at <http://dvha-intra.ahs.state.vt.us/policies-protocols/InfoSec>