

# AHS Security Assessment and Plan of Actions and Milestones Standard

---

Jack Green

10/9/2013

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's security control requirements for the Security Assessment Plan and Plan of Actions ( CA-1, CA-2, CA-2(1), CA-5, CA-5(1)) Controls.

## Revision History

Date	Version	Description	Author
	.99	Procedures received from HI and reviewed by Referentia	
10/9/2013	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 Connect's (VHC) security control requirements for the Security Assessment Plan and Plan of Actions (CA-1, CA-2, CA-2(1), CA-5, CA-5(1)) Controls.

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

- VHC website
- VHC Portal
- VHC workstations and mobile phones
- Network Accounts
- E-Mail accounts

### SCOPE

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

### STANDARD

#### **Security Assessments**

1. The Security and Privacy Managers must create a security assessment plan defining the scope of the assessment that includes the following :
  - i. Security controls and control enhancements being assessed
  - ii. Procedures for performing assessments on the security control effectiveness
  - iii. Overview of the assessment environment, team, and roles and responsibilities
2. The Security and Privacy Managers is responsible for performing an annual security assessment on all VHC Information Systems.
  - i. The assessment includes a review to ensure all security controls are implemented correctly, working as intended, and meeting defined security requirements.
  - ii. An assessment of each security control will be performed as part of:
    1. Continuous monitoring
    2. Testing/evaluation of VHC Information Systems as part of the developmental life cycle processes
    3. Security authorization
  - iii. The Security and/or Privacy Managers may employ an independent assessor of assessment team to conduct the assessment of the security controls.

3. During an assessment the Security and/or Privacy Manager performs the following steps:
  - i. Validate the Information System boundaries.
  - ii. Determine the security control inheritance in the information system being assessed.
  - iii. Gather all system related documentation.
  - iv. Assess all security controls by reviewing all documentation and interviewing System Administrators.
  - v. All assessments that are performed must ensure coordination between information systems with security control inheritance or other dependencies.
4. Upon completion of a security assessment, the Security and/or Privacy Manager will provide a Security Assessment Report (SAR) which documents any findings or results of the assessment.
5. The SAR is used by Security and/or Privacy Manager to determine whether controls are implementing correctly and operating as expected. The SAR must state whether or not the VHC Information System in the assessment is meeting the security requirements.
6. The Security and Privacy Manager must update the SAR when changes are made in the information system pertaining to security controls.
7. The Security and Privacy Manager must then make the SAR available to the System Administrator of the information system in the assessment.
8. All security controls in each VHC Information System will be assessed by the Security and/or Privacy Manager at least once every three years.
9. All security controls that receive, store, process, or transmit FTI data must be assessed by the Security and/or Privacy Manager at least annually.

### **Plan of Action / Milestones**

1. In the event a weakness or deficiency is identified in security controls, a plan of action must be developed by the System Administrator or application owner to reduce or eliminate the identified vulnerability.
2. The plan of action is to then be maintained and any additional findings, recommendations, and source are to be notated and tracked.
3. Each finding must be classified by the plan owner and assigned a risk category (high, medium, low).
4. Every finding must have an associated determination for action to mitigate based on risk level.
5. All findings must also then be entered and tracked in the VHC Federal Information Security Management Act (FISMA) reporting and tracking tool by the plan owner.
6. Findings stored in the FISMA reporting and tracking tool will continually be used to meet any federal or state reporting requirements.

7. Once the task has been reported, but will not be completed, it must then be closed by a System Administrator and contain a justification reason and documentation.
8. All Plan of Action / Milestone data must then be continually reviewed and updated at least once per month to ensure its accuracy of planned, implemented, and evaluated actions to correct or reduce identified deficiencies.
9. The ownership of the Plan of Action will then remain with the Security and/or Privacy Manager.

IMPORTANT INFORMATION

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