

AGENCY OF HUMAN SERVICES

# AHS Security Authorizations Standard

---

Jack Green

10/3/2013

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's security control requirements for the Security Authorizations (CA-1, CA-3, CA-6) Controls.

## Revision History

Date	Version	Description	Author
	.99	Procedures received from HI and reviewed by Referentia	
8/16/2013	2.0	Document revised for VHC standards	Jack Green
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 Authorizations (CA-1, CA-3, CA-6) 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 systems only

### STANDARD

#### **Security Authorization**

1. Prior to commencing any operations, all VHC information systems must receive an authorization to operate (ATO).
2. The information system owner must ensure that every 3 years, the security authorization is updated. Additionally, the security authorization must also be updated in the event there is a major system change.
3. All information systems at the VHC must be assigned an Authorizing Official (AO).
  - i. The security The System Security Plan (SSP) will identify the AO and provide full information including contact name and information.
4. The authorization process is as follows:
  - i. A security authorization package will be delivered to the AO which consists of the SSP, Security Assessment Report, and Plan of Action.
  - ii. The AO will review the security authorization package information and must then make a risk-based decision on whether or not to allow the system to operate.
  - iii. If risks are deemed acceptable, the AO will provide a signed ATO, otherwise a denial of authorization will be provided.
  - iv. The Executive Director must all sign off on the authorization of a new connection in addition to the AO.

- v. The AO's decision must then be documented. If the decision results in an authorization, then the associated risks must also be documented and the AO must provide a signature accepting accountability for the authorization decision.
  - vi. The AO may be permitted to add any additional requirements necessary to ensure security.
  - vii. If the system is permitted to authorize, then, the final authorization package, including the decision for authorization and any additional security requirements determined by the AO will then be sent to the Security and Privacy Manager.
    - The Security and Privacy Manager must enter all documents and information into the VHC FISMA reporting and tracking tool.
  - viii. The decision to deny an ATO must be documented in the authorization decision document and based on the following:
    - Rationale for not accepting the risks
    - Required corrective actions, if applicable
5. If a short-term authorization is required, then the following process must be followed:
- i. Notification of short-term authorization must be provided to the AHS CIO and the Security and Privacy Manager with any applicable terms or conditions that place limitations or restrictions on the operations of the information system.
  - ii. Additionally, the following items must be addressed in the short-term authorization:
    - A defined, short period of time for testing or operations
      1. The duration established for an ATO must be commensurate with the risk to VHC operations, VHC assets, or individuals associated with the operation of the information system not to exceed one year.
      2. The information system must be authorized to operate, testing completed or halted, or taken out of operations by the end of the one year period.
    - Tasks in the plan of action to address identified weakness in the information system resulting from deficiencies in the planned or implemented security controls.
    - The specific terms and conditions established by the AO that convey limitations on the information system's use and acknowledge greater risk to the VHC for a specified period of time.

### **Security reauthorization**

1. Security reauthorization must occur in accordance with federal, the state of Vermont, and VHC policies or at the discretion of the AO.

- iii. To reduce the administrative cost of security reauthorization, the AO shall use the results of the continuous monitoring process to the maximum extent possible as the basis for rendering a reauthorization decision.
- iv. The following questions must be answered when reinitiating the security authorization process:
  - Have any changes to the information system affected the security controls in the system or introduced new vulnerabilities into the system?
  - If so, has the VHC-level risk (i.e., the risk to VHC operations, VHC assets, or individuals) been affected?
  - Has a specified time period passed requiring the information system to be reauthorized in accordance with federal or VHC security policy?
- v. Security controls assessment and reauthorization are required when there is a significant change in risk or risk exposure.
- vi. Security controls assessment and reauthorization must be completed prior to the expiration of the existing ATO.
- vii. The time period for reauthorization must be calculated from the date the information system receives its ATO.

### **Connections to/from VHC Information Systems**

1. All connections from external systems that reside outside of the VHC networks approved boundaries to VHC internal information systems must be authorized through the use of Interconnection Security Agreements (ISA) by the Security and Privacy Manager.
2. All connections from VHC information systems to external systems outside the approved boundaries will require an Interagency Agreement in addition to the ISA.
3. Connection requests that reside within the approved boundaries will not require an ISA or any other agreements.
4. Connections between VHC and non-VHC information systems
5. Connection requests for systems within the VHC Information System network will only require an ISA if the Security and Privacy Manager deems necessary.
6. To establish connectivity from or to an HCC Information System, the requestor must perform the following:
  - Provide a business case.
  - Ensure all technical, security, and administrative issues are vetted and addressed.
    - a. Identify any risks that may be introduced when the systems are connected.
  - Design a plan for cancelling the connection when no longer necessary.
  - Document all technical requirements for the system including:

- a. Security Requirements
  - b. Interface characteristics
  - c. Roles and responsibilities of the users
- Obtain authorization from the approvers.
  - Update System Security Plan (SSP) to ensure any major changes to the system or risks are documented.
  - Ensure an annual review occurs to reaffirm that system security requirements are being met.

IMPORTANT INFORMATION

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