

AHS Configuration and Change Control 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 Configuration and Change Control (CM-1, CM-2, CM-2(1), CM-2(3), CM-2(4), CM-3, CM-3(2), CM-4, CM-4(1), CM-4(2), CM-5, CM-6, CM-6(3), CM-7, CM-7(1), CM-8, CM-8(1)) Controls.

Revision History

Date	Version	Description	Author
	.99	Procedures received from HI and reviewed by Referentia	
8/21/2013	1.0	Created Document	Jack Green
10/10/2013	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 Configuration and Change Control (CM-1, CM-2, CM-2(1), CM-2(3), CM-2(4), CM-3, CM-3(2), CM-4, CM-4(1), CM-4(2), CM-5, CM-6, CM-6(3), CM-7, CM-7(1), CM-8, CM-8(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

Baseline Configuration

The Agency of Human Services Information System Director (AHS ISD) issues VHC wide information security policy, guidance, and architecture requirements for all VHC information systems.

- A current baseline configuration will be developed, documented, and maintained under configuration control for the information system by System/Business Owner.
- The baseline configuration documents and provides information about the components of an information system including:
 - i. Standard operating system/installed applications with current version numbers
 - ii. Standard software load for workstations, servers, network components, and mobile devices and laptops
 - iii. Up-to-date patch level information
 - iv. Network topology
 - v. Logical placement of the component within the system and enterprise architecture

vi. Technology platform

- Each time changes are made to an information system, new baselines will be created prior to change implementation. Changes to the information system must be analyzed to determine potential security impacts.
- The baseline configuration of the information system must be consistent with VHC enterprise architecture.
- The baseline configuration must be reviewed and updated at least annually.
- The baseline configuration is archived in order to support rolling back the configuration.

Configuration Change Control

1. All changes to the information system that are determined to be configuration controlled must be approved and documented by the System/Business Owner.
2. The approvals to implement a configuration-controlled change to the information system must include a security impact analysis.
3. Records of configuration-controlled changes to the system must be retained and reviewed by the System/Business Owner.
4. Oversight for configuration change control activities must be provided and coordinated through VHC Change Advisory Board (CAB) that convenes at least once per month.
5. The configuration change control process for the information system must include a systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications.
6. All changes made to the information system are tested, validated, and documented before the changes are implemented on the information system.
7. All information system changes are audited.
8. Security functionality related to changes made to the information system are check to verify that the functionality is implemented and operating correctly after changes have been made to the information system.

Security Impact Analysis

1. Before change implementation, any changes to the information system are analyzed to determine potential security impacts by the Security and Privacy Manager or other trained staff.
2. The security impact analysis activity must include:
 - Reviewing information system documentation to understand how specific security controls are implemented within the system and how changes might affect the controls.

- Assessing risk to understand the impact of the changes and to determine if additional security controls are required.
 - Testing the changes looking for security impacts due to flaws, weakness, incompatibility, and/or intentional malice.
3. The AHS ISD will maintain a list of software that is not authorized to be executed on any of the VHC information system.

Access restrictions for change

1. The System/Business Owner shall define, document, approve, and enforce physical and logical access restrictions associated with changes (e.g., upgrades, modifications) to the information system.
 - Individuals authorized to perform configuration changes must be documented in the configuration management plan.
 - Logical and physical access control lists that authorize qualified individuals to make changes to an information system or component must be created and maintained.
 - Access is restricted to only qualified and authorized individuals for purposes of initiating changes including upgrades, and modifications.
2. Access records are then maintained to ensure that configuration change control is being implemented as intended.
 - All information system changes associated with access privileges for such changes must be reviewed.
 - The System/Business owner reviews and verifies access lists quarterly and documents any variances that are found.

Configuration Settings

1. A standard set of mandatory configuration settings must be established and documented for information technology products employed within the information system. The System/Business Owner is responsible for the creation and ongoing maintenance of this documentation.
2. The selected configuration settings, whether agency standards or designed specifically for the information system, will also reflect the most restrictive mode consistent with operational requirements and must be derived from the following sources, listed in order of precedence:
 - NIST recommended configurations and checklists found at <http://checklists.nist.gov/>
 - National Security Agency (NSA) configuration guides found at http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml
 - Internal Revenue Service's Safeguards Computer Security Evaluation Matrices (SCSEMs) found at <http://www.irs.gov/uac/Safeguards-Program>

- Any others as listed by NIST
3. The source of the configuration standard employed must be documented in the Configuration Management Plan and System Security Plan (SSP).
 4. Configuration settings must be implemented and exceptions from the mandatory configuration settings must be identified, documented, and approved for individual components within the information system based on explicit operational requirements.
 5. Changes to the configuration settings are then monitored and controlled in accordance with VHC policies and procedures.
 - The individuals on the Sev 1 notification list is notified immediately upon the detection of an unauthorized, security relevant change to the information system.

Information System Component Inventory

1. The System/Business Owner develops, documents, and maintains an inventory of information system components or CIs that accurately reflects the current information.
2. The information system's identification number is then assigned to each item in the inventory.
3. The inventory of information system components must be updated as an integral part of the component installations, removals, and information system updates.
4. The following inventory of information system components include any information determined to be necessary by the organization to achieve effective property accountability including:
 - Manufacturer
 - Type
 - Model
 - Serial number
 - Physical location
 - Software license information
 - Information system/component owner
 - Associated component configuration standard
 - Software/firmware version information
 - Networked component/device machine name or network address

Least Functionality

1. The information system must be configured to provide only essential capabilities.
2. The use of the following functions, ports, protocols, and/or services, at a minimum, must be specifically prohibited or restricted:
 - Domain Name System (DNS)

- i. Port 53 / Transmission Control Protocol (TCP), User Datagram Protocol (UDP)
 - File Transfer Protocol (FTP)
 - i. Ports 20, 21 / TCP
 - Hypertext Transfer Protocol (HTTP)
 - i. Port 80 / TCP
 - Internet Message Access Protocol (IMAP)
 - i. Port 143 / TCP, UDP
 - Internet Relay Chat (IRC)
 - i. Port 194 / UDP
 - Network Basic Input Output System (NetBIOS)
 - i. Port 137 / TCP, UDP
 - Post Office Protocol 3 (POP3)
 - i. Port 110 / TCP
 - Session Initiation Protocol (SIP)
 - i. Port 5060 / TCP, UDP
 - Simple Mail Transfer Protocol (SMTP)
 - i. Port 25 / TCP
 - Simple Network Management Protocol (SNMP)
 - i. Port 161 / TCP, UDP
 - Structured Query Language (SQL)
 - i. Port 118 / TCP, UDP
 - ii. Port 156 / TCP, UDP
 - Telnet
 - i. Port 23 / TCP
3. Any ports that are left open must be documented in a list and maintained.
 4. Any port that is required must be accompanied by a business justification by the requestor.
 5. Any risk identified from using multiple services must be documented and brought to the attention of the Authorizing Official (AO). Prior to moving forward, the AO must accept the risks and provide authorization.
 6. Functions and services provided by organizational information systems, or individual components of information systems, must be carefully reviewed by the operations and security teams in order to determine which functions and services are candidates for elimination. Examples of such functions and services are:
 - Voice over Internet Protocol (VoIP)
 - Instant Messaging
 - Auto-execute
 - File sharing
 7. Any unused and unnecessary physical and logical ports and protocols on information system components must be considered for disabling to prevent

unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. This can be overseen by the Security and Privacy Manager in coordination with the System/Business Owner.

8. The information system is reviewed at least annually to identify and eliminate any unnecessary function, ports, protocols, and/or services.

IMPORTANT INFORMATION

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