

# AHS System Monitoring Standard

---

**Jack Green**

**10/14/2013**

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's security control requirements for the System Monitoring (SI-1, SI-3, SI-3(1), SI-3(2), SI-3(3), SI-4, SI-4(1), SI-4(2), SI-4(4), SI-4(5), SI-4(6), SI-5, SI-7, SI-7(1), SI-8, SI-8(1) ) Controls.

## Revision History

Date	Version	Description	Author
	.99	Draft received from HI and reviewed by Referentia	
	1.0	Created Document	AHS
8/16/2013	2.0	Document revised for VHC standards	Jack Green
10/14/2013	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 System Monitoring (SI-1, SI-3, SI-3(1), SI-3(2), SI-3(3), SI-4, SI-4(1), SI-4(2), SI-4(4), SI-4(5), SI-4(6), SI-5, SI-7, SI-7(1), SI-8, SI-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

#### **Malicious Code Protection**

1. Malicious code protection mechanisms must be employed at information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network.
2. Configures malicious code protection mechanisms to block at gateways and quarantine at host, validate quarantined code before releasing to user, clean quarantined malware as appropriate.
3. Standard malicious code protection software deployed on all workstations and servers must be configured to adhere to the following:
  - Servers must be scanned for malicious code on a continuous basis.
  - Workstations must be automatically scanned for malicious code on a daily basis.
  - Malicious code protection software must allow users to manually perform scans on their workstation and removable media.
  - Malicious code protection software must be updated concurrently with releases of updates provided by the vendor of the software. Updates should be tested and/or approved according to VHC requirements.

4. Malicious code protection mechanisms must be used to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) that is:
  - Transported by electronic mail, electronic mail attachments, web accesses, removable media (e.g., Universal Serial Bus [USB] devices, diskettes or compact disks), or other common means
  - Inserted through the exploitation of information system vulnerabilities
  - Encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file
5. Malicious code protection mechanisms (including signature definitions) must be updated whenever new releases are available and in accordance with organization-wide configuration management policy, procedures, and standards.
  - As applicable, the malicious code protection software must be supported under a vendor Service Level Agreement (SLA) or maintenance contract that provides frequent updates of malicious code signatures and profiles.
6. Malicious code protection mechanisms must be configured to:
  - Perform periodic scans of the information system daily and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with VHC security policy.
  - Block and quarantine malicious code and send alert to an administrator in response to malicious code detection.
7. The following elements must be addressed during vendor and product selection and when tuning the malicious code protection software:
  - The receipt of false positives during malicious code detection and eradication.
  - The resulting potential impact on the availability of the information.
8. In situations where traditional malicious code protection mechanisms are not capable of detecting malicious code in software (e.g., logic bombs, back doors), the organization must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended.
9. NIST SP 800-83 and current anti-malware vendor guidance must be used as guidance when implementing malicious code protection.
10. SSPs shall adopt a defense-in-depth strategy that integrates firewalls, screening, routers, wireless intrusion detection systems, antivirus software, encryption, strong authentication, and cryptographic key management to ensure information security solutions and secure connections to external interfaces are consistently enforced.

### **Information System Monitoring**

1. Events on the information systems must be monitored in accordance with defined monitoring objectives and information system attacks must be detected.

2. Unauthorized use of the system must be identified.
3. Must be monitored in accordance with Security Program Plan.
4. Monitoring devices must be strategically deployed within the information system to collect Organization-determined essential information.
  - These devices must be used to track the impact of security changes to the information system.
5. Monitoring devices must be deployed at ad hoc locations within the system to track the following:
  - Specific types of transactions of interest to the VHC.
  - The impact of security changes to the information system.
6. The granularity of information collected must be determined based upon organizational monitoring objectives and the capability of the information system to support such activities.
7. VHC shall obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.
8. VHC shall heighten the level of information system monitoring activity whenever there is an indication of increased risk to VHC operations, VHC assets, individuals, other organizations, or the nation based on law enforcement information, intelligence information, or other credible sources of information.
9. The information system must be configured to monitor inbound and outbound communications for unusual or unauthorized activities or conditions including, but not limited to:
  - Internal traffic that indicates the presence of malicious code within an information system or propagating among system components
  - The unauthorized export of information
  - Attack signatures
  - Signaling to an external information system
  - Localized, targeted, and network-wide events
10. Evidence of malicious code must be used to identify potentially compromised information systems or information system components.
11. Automated tools must be employed to support near real-time analysis of events.
12. The information system must be configured to provide a near real-time alert when indications of compromise or potential compromise occur from the following sources:
  - Audit records
  - Input from malicious code protection mechanisms
  - Intrusion detection and prevention mechanisms
  - Boundary protection devices, such as firewalls, gateways, and routers
13. The information system must be configured to prevent non-privileged users from circumventing intrusion detection and prevention capabilities.

14. NIST SP 800-61, Revision 1 must be used as guidance on responding to attacks through various types of security technologies.
15. NIST SP 800-83 must be used as guidance on responding to detecting malware based attacks.
16. NIST SP 800-92 must be used as guidance on monitoring and analyzing computer security event logs.
17. NIST SP 800-94 must be used as guidance on intrusion detection and prevention.

### **Security Alerts, Advisories, and Directives**

1. VHC shall receive information system security alerts, advisories, and directives from designated external organizations on an ongoing basis.
2. Internal security alerts, advisories, and directives must be generated, as deemed necessary.
3. Security alerts, advisories, and directives must be disseminated to VHC personnel
  - Information system and security personnel shall check for security alerts, advisories, and directives on an ongoing basis.
  - All security alerts, advisories, and directives must be from reputable sources (i.e., vendors, manufacturers, government agencies, CSIRC).
4. Security directives must be implemented in accordance with established time frames, or the issuing organization must be notified of the degree of noncompliance.
5. The types of actions to be taken in response to security alerts/advisories must be documented.
6. Information system personnel shall take appropriate actions in response to security alerts/advisories.
  - Any updates or notices from CSIRC must be implemented per CSIRC instructions.
  - CSIRC must be contacted with any security alert/advisory concerns or questions.
  - CSIRC must be notified when the actions are completed.
7. The coordinator for CSIRC shall maintain a repository of the alerts and advisories, including related communications (i.e., responses, questions, concerns) from other VHC personnel.
8. VHC shall maintain contact with special interest groups (e.g., information security forums) that:
  - Facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies).
  - Provide access to advice from security professionals.
  - Improve knowledge of security best practices.
9. NIST SP 800-40, Version 2.0 must be used as guidance on monitoring and distributing security alerts and advisories.

## **Security Functionality Verification**

1. The information system must verify the correct operation of security functions at one of the following intervals:
  - At defined system transitional states (e.g., startup, restart, shutdown, abort).
  - Upon command by a user with appropriate privilege.
  - At least every 30 days.
2. The information system must implement one of the following actions when anomalies are discovered:
  - Notify system administrator.
  - Notify ISO.
3. For those security functions that are not able to execute automated self-tests, compensating security controls must be implemented or the risk of not performing the verification as required must be explicitly accepted.
  - The System Security Plan must reflect whether or not compensating security controls have been implemented or the risk has been accepted.
4. The appropriate VHC personnel must be trained and made aware of proper procedures to shut down or restart the information system.

## **Software and Information Integrity**

1. The information system must be configured to detect unauthorized changes to software and information.
2. Integrity verification applications must be employed on the information system to look for evidence of information tampering, errors, and omissions.
3. Good software engineering practices must be employed on the information system with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and tools must be used to automatically monitor the integrity of the information system and the applications it hosts.
  - The mechanism should be able to provide a means to determine the date and time a resource was last modified or accessed depending on sensitivity.
4. VHC shall reassess the integrity of software and information by performing quarterly integrity scans of the information system.

## **Spam Protection**

1. Spam protection mechanisms must be employed at information systems entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network.
2. The VHC shall centrally manage spam protection mechanisms.

3. Spam protection mechanisms must be used to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means.
4. Spam protection mechanisms (including signature definitions) must be updated when new releases are available.
  - Updates are implemented in accordance with VHC configuration management policy and procedures.
5. Spam protection mechanisms must be configured to perform the following:
  - Maintain a list of authorized Internet Protocol (IP) addresses or ensure authorized sources will always be allowed.
  - Block a list of senders that have been verified as sending spam.
  - Allow users to tag or block suspected spam messages that were not detected by the spam mechanism.
6. VHC shall give consideration to using spam protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations).
7. NIST SP 800-45, Version 2, must be used as guidance on electronic mail security.

#### IMPORTANT INFORMATION

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