

# AHS Data Validation and Error Handling Standard

---

Jack Green

10/13/2013

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's security control requirements for the Data Validation and Error Handling (SI-1, SI-9, SI-10, SI-11) 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
10/13/2013	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 Data Validation and Error Handling (SI-1, SI-9, SI-10, SI-11) 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

#### **Information Input Restrictions**

1. The capability to input information to the information system must be restricted to authorized personnel.

#### **Information Input Validation**

2. The information system must be configured to check the validity of information inputs.
  - The checks for input validation must be verified as part of system testing.
3. The information system must be configured to check all arguments or input data strings submitted by users, external processes, or untrusted internal processes.
  - The information system must validate all values that originate externally to the application program itself, including arguments, environment variables, and information system parameters.
  - Automated data entry transmittal from other servers must comply with requirements set forth in the procedures found in the Access Control Procedures.
  - The information system must trust only reliable external entities which have been identified by authorized VHC personnel.

4. Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) must be in place to verify that inputs match specified definitions for format and content.
5. The information system must be configured to perform the following input validations:
  - Type checks – Checks to ensure that the input is, in fact, a valid data string and not any other type of object.
    - i. Inputs passed to interpreters must be prescreened to prevent the content from being unintentionally interpreted as commands.
  - Format and syntax checks – Checks to verify that data strings conform to defined formatting and syntax requirements for that type of input.
  - Parameter and character validity checks – Checks to verify that any parameters or other characters entered, including format parameters for routines that have formatting capabilities, have recognized valid values.
    - i. Any parameters that have invalid values must be rejected and discarded.
    - ii. Web server applications must be configured to prohibit invalid data from web clients in order to mitigate web application vulnerabilities including, but not limited to, buffer overflow, cross-site scripting, null byte attacks, SQL injection attacks, and HTTP header manipulation.
6. Invalid inputs or error statements must not give the user sensitive data, storage locations, database names, or information about the application or information system's architecture.

## **Error Handling**

1. The information system must be configured to identify potentially security-relevant error conditions.
2. The structure and content of error messages must be carefully considered by information system personnel.
  - The criticality or severity level of error messages for the information system must be determined.
3. The information system must be configured to reveal error messages only authorized personnel.
  - System error messages must be revealed only to authorized personnel (e.g. systems administrators, maintenance personnel).
4. Error messages generated by the information system must provide information necessary for corrective actions without revealing sensitive information (e.g. account numbers, social security numbers, and credit card numbers) or potentially harmful information in error logs and administrative messages that could be exploited by adversaries.

- Error messages revealed to users must not include file pathnames or system architecture information.
  - Alert error messages revealed to the administrator must include file pathnames or system architecture information and must be written to the application's error log and audit trail.
5. The extent to which the information system is able to identify and handle error conditions must be guided by operational requirements.
  6. The information system's error-handling mechanisms must enable the administrator to configure the application to gracefully terminate processes, when appropriate in response to various errors and failures.

#### IMPORTANT INFORMATION

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