

AHS Contingency Planning 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 Contingency Planning (CP-1, CP-2, CP-2(1), CP-2(2), CP-3, CP-4, CP-4(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 Contingency Planning (CP-1, CP-2, CP-2(1), CP-2(2), CP-3, CP-4, CP-4(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

Contingency Plan Development

1. A contingency plan must be developed as follows:
 - i. Develop a contingency plan template.
 - This template must be used when developing the information system's contingency plan.
 - This template must address the following:
 - a. The procedures in this document must be addressed.
 - b. Contingency activity roles and responsibilities must be identified.
 - c. Individuals must be assigned to appropriate roles and responsibilities.
 - d. Responsibilities may be identified by teams.
 - e. Contact information (e.g., home number, mobile number) for the identified individuals must be included.
 - f. Maintaining essential missions and business functions despite an information system disruption, compromise, or failure must be addressed.
 - g. Activities that must be documented include:
 - i. Plan activation

- ii. Notification
 - iii. Outage assessment
 - iv. Recovery
 - v. Reconstitution
 - vi. Return to normal operations
 - vii. Plan deactivation
 - h. Procedures for restoration/reconstitution of normal operations by transitioning from the alternate processing site to the original or new primary processing facility must be included.
 - i. Procedures for testing security both during recovery at the alternate processing site and during restoration/reconstitution at the original or new primary processing facility must be included.
- ii. Assign a resource and designate in writing the Contingency Planning Coordinator.
 - The Contingency Coordinator is someone who has extensive knowledge about the system at hand and can act as an appropriate resource and perform tasks around system criticality, assignment of resources, and distribution of those resources.
- iii. Conduct Business Impact Analysis (BIA) define the scope of the contingency plan.
 - Generally, the BIA will be included in the appendix of the Contingency Plan itself.
 - Full information system restoration must be addressed and in conjunction to the adherence of all security measures planned and implemented for the system.
 - Identify preventative controls, both in place and planned.
 - Design and develop recovery strategies, both in place and planned and assign associated costs.
 - The BIA must incorporate the following:
 - a. Identify essential missions and business functions and associated contingency requirements.
 - b. Identify critical resources for each business process.
 - c. Determine the impacts of disruptions, damages to resources, and the maximum tolerable downtime (MTD) for each resource in each business process, should an adverse event occur.
 - d. Develop recovery priorities for each resource, considering criticality and dependencies or interdependencies of resources.
 - The BIA must be reviewed at least annually and updated with new information, as applicable, to identify new contingency planning requirements, recovery objectives, restoration priorities, and metrics.

- a. The BIA findings, particularly the down times and disruption impacts, must serve as inputs to develop and maintain the Contingency Plan's recovery time and recovery point objective requirements.
 - b. Application recovery requirements must be shared and coordinated with associated System Owners.
 - c. System Owners shall consider the application recovery requirements and incorporate these requirements into their continuity of support considerations of their contingency planning program.
- iv. Develop the contingency plan document.
- v. Create plans for training, testing, and exercising the contingency plans.
- vi. Plan for maintenance of all elements of the contingency planning program.
2. Reviews of the Contingency Plan should be conducted annually or when a major system change occurs.
3. The Contingency Plan must be reviewed and approved by designated officials within the organization.
4. Copies of the Contingency Plan shall be distributed to at minimum individuals with any contingency planning responsibilities based on the information system.
5. Weaknesses found in the Contingency Plan during development, testing, or implementation must be listed and tracked using the Plan of Action and Milestones (POA&M) for the information system.

Contingency Training

1. All personnel must be trained in their contingency roles and responsibilities with respect to the information system and attend annual refresher training.
2. A comprehensive log of all Contingency Plan related training is maintained and monitored by the System Owner.
3. The log must include participant, information system name(s), type of training, date of completion, and whether the training was initial training or refresher training.
4. Contingency training plans must be developed and maintained for all information systems.
5. The training plan must meet the following criteria:
 - Training objectives and requirements must be identified and documented.
 - All personnel with Contingency Plan responsibilities must be identified and included in the contingency training plan.
 - The training plan must identify the mandatory training activities for personnel with contingency roles and responsibilities.

- The training plan must identify the types of training to be provided, such as classroom training, table top exercises, or full test simulations. However, actual plan testing may serve as a training activity.
 - The training plan may include both team-specific and cross-team training exercises, spanning orientation, drills, tabletop, functional, and full-scale methods.
6. Contingency Plan training must be provided by a qualified and certified commercial or internal source.

Contingency Plan Testing and Exercises

1. The Contingency Plan must be tested on an annual basis to determine the plan's effectiveness and the VHC's readiness to execute the plan.
2. The Contingency Plan is tested before the system goes into production.
3. Results of the contingency plan test are reviewed and necessary corrective actions initiated. Significant deficiencies must be remediated prior to production deployment.
4. Costs of testing must be budgeted and accounted for.
5. An exercise plan for each scheduled test or exercise may include the following:
 - Objectives of the test or exercise
 - The type of test or exercise (e.g., checklist, walk-through/table-top, simulation: parallel, full interrupt).
 - The scenario(s) for the test or exercise
 - Participants
 - Logistics for the test or exercise
 - Documentation for implementing the test or exercise
 - Development of an After Action Report and any improvement plan to correct weaknesses uncovered by the test or exercise
6. Test or exercise scenarios must include, but are not limited to, one or more of the following:
 - Equipment damage/failure.
 - COOP emergency relocation, when applicable.
 - Data loss/corruption.
 - Network outage.
 - Staff shortage due to pandemic influenza.
 - Localized or larger scale natural or man-made disaster scenarios relevant to potential or expected occurrences of the locality (e.g., earthquakes, floods, hazardous materials releases, etc.).
 - Restoration of user-level and system-level files from backup media.
7. The results of the Contingency Plan testing must be reviewed by the System Owner.

8. The results of Contingency Plan testing must be used to identify and remediate weaknesses within the Contingency Plan. All weaknesses found must also be documented and corrected per process and procedures.

IMPORTANT INFORMATION

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