Z

VistA Adaptive Maintenance (VAM) INFORMATION System Contingency Plan

Security Categorization: High

GRC Boundary Alignment: Boundary Info

**September** 06, 2018

Table of Contents

[Actual Emergency Instruction Page 4](#_Toc523230991)

[Document Change Control Record 5](#_Toc523230992)

[Information System Contingency Plan (ISCP) Approval 6](#_Toc523230993)

[ISCP Distribution 7](#_Toc523230994)

[1. INTRODUCTION 8](#_Toc523230995)

[1.1 Background 8](#_Toc523230996)

[1.2 Critical Exposure Report of IS Services 9](#_Toc523230997)

[1.3 Scope 9](#_Toc523230998)

[1.4 Assumptions 10](#_Toc523230999)

[1.5 Threats and Vulnerabilities 11](#_Toc523231000)

[2. CONCEPT OF OPERATIONS 12](#_Toc523231001)

[2.1 System Description 12](#_Toc523231003)

[2.2 Overview of ISCP Phases 16](#_Toc523231004)

[2.3 Roles and Responsibilities 17](#_Toc523231005)

[3. ACTIVATION AND NOTIFICATION 19](#_Toc523231006)

[3.1 Activation Criteria and Procedures 19](#_Toc523231008)

[3.2 Notification Procedures 19](#_Toc523231009)

[3.3 Outage Assessment 19](#_Toc523231010)

[4. RECOVERY 21](#_Toc523231011)

[4.1 Sequence of Recovery Activities 21](#_Toc523231013)

[4.2 Escalation Notices / Awareness 21](#_Toc523231014)

[5. RECONSTITUTION 22](#_Toc523231015)

[5.1 Concurrent Processing 22](#_Toc523231017)

[5.2 Data Validation and Functionality Testing 22](#_Toc523231018)

[5.3 Reconstitution Declaration 22](#_Toc523231019)

[5.4 Notifications (Users) 22](#_Toc523231020)

[5.5 Cleanup 22](#_Toc523231021)

[5.6 Offsite Data Storage 22](#_Toc523231022)

[5.7 Data Backup 22](#_Toc523231023)

[5.8 Event Documentation 23](#_Toc523231024)

[5.9 Deactivation 23](#_Toc523231025)

[6. TEST, TRAINING AND EXERCISE 24](#_Toc523231026)

[7. DOCUMENT MANAGEMENT 26](#_Toc523231027)

[7.1 Document Ownership 26](#_Toc523231030)

[7.2 Plan Review and Maintenance 26](#_Toc523231031)

[7.3 Document Distribution 26](#_Toc523231032)

[Appendix A : Personnel Contact Data - VA A-1](#_Toc523231033)

[Appendix B : Call Tree B-1](#_Toc523231034)

[Appendix C : Personnel Contact Data – Vendors C-1](#_Toc523231035)

[Appendix D : Recovery Site D-1](#_Toc523231036)

[Appendix E : Alternate Storage Facility E-1](#_Toc523231037)

[Appendix F : Alternate Processing Procedures F-1](#_Toc523231038)

[Appendix G : Outage Assessment Checklist G-1](#_Toc523231039)

[Appendix H : Alternate Data / Voice Telecommunications H-1](#_Toc523231040)

[Appendix I : Data Backup I-1](#_Toc523231041)

[Appendix J : Detailed Recovery Procedures J-1](#_Toc523231042)

[Appendix K : Data and Functionality Validation Testing Procedures K-1](#_Toc523231043)

[Appendix L : Concurrent Processing L-1](#_Toc523231044)

[Appendix M : Cleanup M-1](#_Toc523231045)

[Appendix N : Business Impact Analysis (BIA) N-1](#_Toc523231046)

[Appendix O : ISCP Glossary O-1](#_Toc523231047)

[Appendix P : ISCP Acronym List P-1](#_Toc523231048)

Table of Figures

Figure 1: System Diagram 12

Figure 2: Call Tree B-1

List of Tables

Table 1: Critical Exposure Report for IS Service 9

Table 2: Contingency Planning Controls Addressed in this ISCP 10

Table 3: VAEC AWS IS Threat Assessment 11

Table 4: VAEC AWS IS Vulnerability Assessment 11

Table 5: IS System Components 14

Table 6: Associated Plans 15

Table 7: Information Systems That Connect with IS System name 15

Table 8: {site name} ISCP Roles and Responsibilities (Primary and Alternate) 18

Table 9: VAM TT&E Calendar 25

Table 10: ISCP Personnel Contact Data – VA A-1

Table 11: Outage Assessment Team Key Personnel Contact Data A-2

Table 12: {Team Name} Key Personnel Contact Data A-2

Table 13: ISCP Vendor Contact Data C-1

Table 14: Recovery Site Data D-1

Table 15: Alternate Storage Facility Data E-1

Table 16: Alternate Data/Voice Telecommunications Data H-1

Table 17: Detailed Recovery Priority Procedures J-1

Table 18: Critical Business Process Mapping / IS Services N-1

Table 19: Service / Business Line Maximum Tolerable Downtime (MTD) N-1

Table 20: IS Service Recovery Time Objective (RTO) N-2

Table 21: Service / Business Line MTD / RTO Gap Analysis N-2

Table 22: Acronym List P-1

# Actual Emergency Instruction Page

In the event of an actual emergency,

Go directly to:

**SECTION 3: Activation and Notification**

# Document Change Control Record

| **Version** | **Release Date** | **Summary Of Changes** | **Author** |
| --- | --- | --- | --- |
| **Version 1.0** | 08/08/2018 | Initial document | AbleVets |
| **Version 1.1** | 08/28/2018 | Updates from Internal Review | AbleVets |
| **Version 1.2** | 9/06/2018 | ISCP Approval Section Updates | AbleVets |
|  |  |  |  |

# Information System Contingency Plan (ISCP) Approval

As the designated authority for VistA Adaptive Maintenance (VAM), I hereby certify that the information system contingency plan (ISCP) is complete and that the information contained in this ISCP provides an accurate representation of the application, its hardware, software, and telecommunication components. I further certify that this document identifies the criticality of the system as it relates to the mission of the organization , and that the recovery strategies identified will provide the ability to recover the system functionality in the most expedient and cost-beneficial method in keeping with its level of criticality.

I further attest that this ISCP for VAM will be tested at least annually. This IS Service was last tested on <last date tested>.The test, training and exercise material associated with this plan are found in the VA plan repository. This document will be modified as changes occur and will remain under version control, in accordance with Federal regulations and guidance to include VA Handbook 6500.8 guidance.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<Dick Rickard> Date

<System Owner>

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<Bobbi Begay> Date

<System Information Security Officer>

# ISCP Distribution

Distribution of the ISCP should be restricted to personnel involved in the activities for the continued operations of systems and system owners. Update this table with key personnel required to receive and hold a copy of this plan, as well as plan updates when they are issued. The below members are from the VAEC AWS Team.

| Name | Title |
| --- | --- |
| **Chris Lopez** | **ISCP Coordinator** |
| **Ertha Patrick** | **ISCP Coordinator (Alternate)** |
| **Louis Lugo** | **ISCP Director** |
| **Chris Cockle** | **ISCP Director (Alternate)** |
| **Christopher Cardella** | **Outage Assessment Team POC** |
| **Brandon Petersen** | **Outage Assessment Team POC (Alternate)** |
| **Christopher Cardella** | **Business / Service Line POC** |
| **Ralph Parkison** | **Business / Service Line POC (Alternate** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# INTRODUCTION

Information Systems (IS) are vital to the Department of Veterans Affairs (VA) business processes; therefore, it is critical that services provided byVistA Adaptive Maintenance (VAM)operate effectively without excessive interruption. This Information System Contingency Plan (ISCP) establishes comprehensive procedures to recover VAM quickly and effectively following a service disruption.

VA requires a robust IS contingency planning process that includes both ISCPs and disaster recovery plans (DRP) that are fully compliant with:

* *E-Government Act, Title III, Federal Information Security Management Act (FISMA)*, December 2002
* Office of Management and Budget Circular A-130, *Management of Federal Information Resources, Appendix III*, November 2000
* Department of Homeland Security (DHS), National Security Presidential Directive 51 / Homeland Security Presidential Directive 20, *National Continuity Policy*, May 2007
* DHS, Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements*, October 2012
* DHS, *National Response Framework*, May 2013
* DHS, *Homeland Security Exercise and Evaluation Program (HSEEP),* April 2013
* Homeland Security Council, *National Continuity Policy Implementation Plan*, August 2007
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, *Contingency Planning Guide for Information Technology Systems*, May 2010
* NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, January 2014
* NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006
* VA Handbook 6500.8, *Information Technology Contingency Planning*, April 2011
* OI&T Comprehensive Emergency Management Homeland Security Test, Training & Exercise Program Strategy (Draft), January 2010

## Background

This VAM ISCP establishes procedures to recoverVAM following a disruption. The following recovery plan objectives have been established:

* Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
* Activation and notification phase to activate the plan and determine the extent of damage;
* Recovery phase to restore VAM operations; and
* Reconstitution phase to ensure that VAMis validated through testing and that normal operations are resumed.
* Identify the activities, resources, and procedures to carry outVAM processing requirements during prolonged interruptions to normal operations.
* Assign responsibilities to designated VAEC AWS personnel and provide guidance for recovering VAM during prolonged periods of interruption to normal operations. For a complete list of personnel, refer to Appendix A: Personnel Contact Data – VA and Appendix B Call Tree.
* Ensure coordination with other personnel responsible for VAEC AWS contingency planning strategies. Ensure coordination with external points of contact (POC) and vendors associated withVAM and execution of this plan. For a list of vendors associated with this ISCP, refer to Appendix C: Personnel Contact Data – Vendors.

## Critical Exposure Report of IS Services

This ISCP describes contingencies for circumstances, events, or acts that could cause harm to VAM by destroying, disclosing, modifying, or denying access toVAEC AWS ’s information resources. It provides flexible and scalable response and recovery strategies to accommodate a variety of disruptions.

The Critical Exposure report, as shown in Table 1, is the culmination of the ISCPA process, in that it uses data and values gathered and assigned during the process to produce the IS exposure description for each IS service. This description is calculated by inserting threat, vulnerability, and business impact values into the following algorithm: **Threat x Vulnerability x Impact = Critical Exposure**. Table 1 below, shows a critical exposure report for the VAM IS Service.

| Threat | Threat Value | Vulnerability | Vulnerability Rating | Impact Value | **Exposure Value** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Table 1: Critical Exposure Report for IS Service

### GRC Boundary Alignment

Based on guidance from the Office of Cyber Security (OCS), this ISCP is aligned with the following GRC boundary (ies): <first boundary, second boundary, third boundary>.

## Scope

This ISCP has been developed for VAM, a High-impact system, in accordance with *FIPS 199,* and designed to assist in the recovery of VAM within RTO at both the primary and alternate sites. This plan does not address replacement or purchase of new equipment, short-term disruptions, and loss of data at the onsite facility or at the user-desktop levels.

With respect to facilities that are supported by a parent facility’s single IT Management staff, and located on the same campus or within a reasonable distance from one another, the {VAEC AWS } VAM ISCP may be utilized for all parent / child facility relationships. The following verifications of the relationship will be required: 1) the existence of an artifact demonstrating that the IT administration groups identified provide support across all parent / child facilities, and 2) an artifact demonstrating all administrators have logged into the facilities’ machines.

This ISCP addresses contingency planning (CP) controls contained within the family of contingency planning controls from NIST SP 800-34 Rev 1 and NIST SP 800-53 Rev 4. The controls for NIST 800-53 Rev 4 are matched with the sections of this plan, as shown in Table 2, providing a means of reference for documenting required elements within the control for systems with high critical exposures.

| Contingency Planning Controls | Relevant Section Of ISCP |
| --- | --- |
| CP-1 Policy & Procedures | Section 1, Section 1.1, Section 1.3, Section 3.1, Section 4.2 |
| CP-2 Contingency Plan | ISCP Approval, ISCP Distribution, Section 2.1.2, Section 2.3, Section 4.1, Section 7.3, Appendix A, Appendix B, Appendix C, Appendix D, Appendix F, Appendix H, Appendix J, Appendix N |
| CP-3 Contingency Training | ISCP Approval, Section 6 |
| CP-4 Testing & Exercises | Plan Approval, Section 6, Appendix D |
| CP-6 Alternate Storage Site | Section 1.4, Section 5.6, Section 5.7, Appendix E, Appendix I |
| CP-7 Alternate Processing Site | Section 1.4, Section 5.7, Appendix D |
| CP-8 Alternate Telecomm Services | Appendix H |
| CP-9 System Backup | Section 1.4, Section 2.1.1, Section 4.1, Section 5.7, Section 6, Appendix E, Appendix I |
| CP-10 Recovery and Reconstitution | Section 4, Section 5, Appendix J, Appendix K, Appendix L, Appendix M |
| CP-11 Alternate Communications Protocols | Not Applicable |
| CP-12 Safe Mode | Not Applicable |
| CP-13 Alternate Security Mechanisms | Not Applicable |

Table 2: Contingency Planning Controls Addressed in this ISCP

## Assumptions

The following assumptions were used when developing this ISCP:

* VAM has been established as a <High>impact system, in accordance with *FIPS 199.*
* Business Impact Analysis results developed for this plan have been incorporated in the development strategy of other organizational plans including, but not limited to, COOP, BCPs and DRP.
* Information System Owners have worked in coordination with service/business lines to identify essential mission, service and business functions;
* Recovery sites and offsite storage are required for High and Moderate systems, optional for Low systems, and have been established for this system as described in Appendices D and E.
* Alternate processing procedures have been established by business / service lines. Alternate processing procedures are manual procedures that can be initiated in lieu of the application to maintain business operations during an outage.
* Current backups of the system software and data are intact and available at the offsite storage facility or facilities
* The VAM at VAEC AWS is inoperable and cannot be recovered within the RTOrequired to operate normally.
* IS Service component restoration priorities have been established.
* Key VistA Adaptive Maintenance personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the VAM ISCP.

{Additional Assumptions}

This plan does not apply to the situations described below:

* Emergency evacuation of personnel addressed by the occupant evacuation plan.
* Overall recovery of business operations. Business / service line owners should address recovery of business operations in a separate business recovery plan.

## Threats and Vulnerabilities

The data gathered through the Information System Contingency Planning Assessment (ISCPA) process is used in the completion of a Business Impact Analysis (BIA), a Vulnerability assessment and a Threat assessment. The results of the Threat and Vulnerability assessments for VAEC AWS  **are inherited from FedRAMP package (F1603047866).** are shown in Tables 3 and 4.

| IS Threat | Likelihood | Capacity | Threat Rating |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

Table 3: VAEC AWS IS Threat Assessment

| IS Threat | Vulnerability | Exploit Potential | Mitigation Effectiveness | Mitigation Strength |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

Table 4: VAEC AWS IS Vulnerability Assessment

# CONCEPT OF OPERATIONS

The Concept of Operations section provides details about VAM, an overview of the three phases of the ISCP (Activation and Notification, Recovery, and Reconstitution), and a description of the roles and responsibilities forVAEC AWS ’s personnel during a contingency activation.



## System Description

The purpose of the VistA Adaptive Maintenance (VAM) project is to establish a secure, sustainable, high-performing, cloud-based service to implement provider workflow logic back-end processing and storage. The VAM service will replicate the Remote Procedure Call (RPC) functionality currently provided via VistA in a modern, well-documented platform (i.e., Node.js and NoSQL database). VAM will enable the incremental transition of clinical workflow logic out of VistA into VAM services, while maintaining full compatibility with current VistA clients such as CPRS. VAM will be hosted in production within the VA’s Enterprise Cloud (VAEC) using the Amazon Web Services (AWS) service provider.

### System Architecture

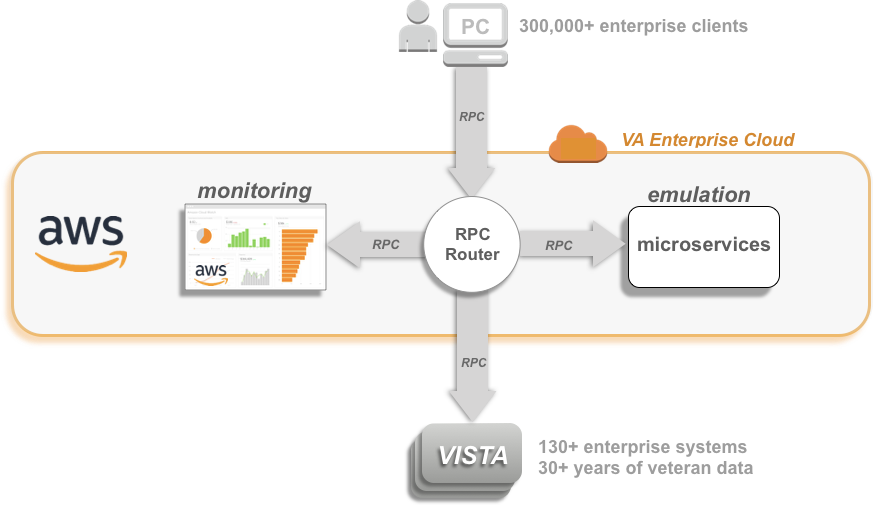


Figure 1: System Diagram

### The System’s Operating Environment

VAEC AWS West

### Physical Locations

No physical location, installation will be on VAEC

### General Location of Users

Existing CPRS Users in VA network; Refer to architectural diagram existing enterprise clients

### Partnerships with External Organizations / Systems

VAEC AWS

### Special Technical Considerations Important For Recovery Purposes

VAEC AWS connectivity to VISTA through IP address and port; Refer to EECCB ticket specific for opening those ports

### IS System Inventory of Components

| APPLICATION | Type | DATA STORAGE | NAME | Model | RPO (where applicable) | RTO |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Table 5: IS System Components

### 

### System Interconnections and Associated Plans

| ISCP or Other  (Full Name) | Version # | Location  (URL if Web-Based) | POC Title |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

Table 6: Associated Plans

\*Refer to Appendix A for POC contact information

| Information System | Information Transferred Or Support Provided | POC Title | POC’s Organization |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

Table 7: Information Systems That Connect with IS System name

\*Refer to Appendix A for POC contact information

## Overview of ISCP Phases

This ISCP has been developed to recover VistA Adaptive Maintenance using a three-phased approach. This approach ensures that system recovery efforts are performed in a methodical sequence to maximize the effectiveness of the recovery effort and minimize system outage time due to errors and omissions.

The three ISCP phases are:

1. **Activation and Notification Phase –** Activation of the ISCP occurs after a disruption or outage that may reasonably extend beyond the RTO established for a system. Once the ISCP is activated, system owners and users are notified of an outage and a thorough outage assessment is performed for the system. Information from the outage assessment is presented to system owners and may be used to modify recovery procedures specific to the cause of the outage.
2. **Recovery Phase –** The recovery phase details the activities and procedures for recovery of the affected system. Activities and procedures are written at a level that an appropriately skilled technician can recover the system without intimate system knowledge. This phase includes notification and awareness escalation procedures for communication of recovery status to system owners and users.
3. **Reconstitution Phase –** The reconstitution phase defines the actions taken to test and validate system capability and functionality. This phase consists of two major activities: validating successful recovery and deactivating the plan. During validation, the system is tested and validated as operational prior to returning operation to its normal state. Validation procedures may include functionality or regression testing, concurrent processing, and /or data validation. The system is declared recovered and operational by system owners upon successful completion of validation testing. Deactivation includes activities to notify users of system operational status. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, and readying resources for any future recovery events.

## Roles and Responsibilities

The following table includes responsibilities that describe each role and identifies the individual or team responsible for executing or supporting system recovery.

| **ISCP Role** | **Job Title** | **Responsibilities** |
| --- | --- | --- |
| **ISCP Director** |  | * Overall responsibility for the development, execution, and maintenance of the ISCP * Ensures that the ISCP is developed with the cooperation of managers associated with the business processes supported by the system * Confirms expected duration of the system disruption with the ISCP Coordinator based on the outage assessment * Declares activation of the ISCP * Determines if interim / secondary processing procedures activities should be initiated to maintain current business operations or if operations should be suspended until the system has been recovered * Contacts organization officials if the situation needs to be escalated * Responsible for the testing, maintenance, and distribution of the ISCP, which may be delegated to other personnel * Authorizes all changes to the ISCP |
| **ISCP Director (Alternate)** |  | * Same responsibilities as ISCP director * Activated when the ISCP director is unavailable |
| **ISCP Coordinator** |  | * Monitors Recovery Team activities until the system is fully recovered * Ensures that recovery operations are being performed consistent with service level agreements / service level requirements * Provides periodic status updates to the ISCP director * Files an after action report (AAR) upon resumption of normal operations * Assists the ISCP director in testing, maintenance, and distribution of the ISCP |
| **ISCP Coordinator (Alternate)** |  | * Same responsibilities as ISCP coordinator * Activated when the ISCP coordinator is unavailable |
| **Business / Service Line POC** |  | * Represents the recovery and restoration interests of the affected business / service line |
| **Outage Assessment Team** |  | * Assesses the extent of damage to the facilities and the information systems * Estimates the time to recover operations * Determines accessibility to facility, building, offices, and work areas * Identifies salvageable hardware * Maintains a log / record of all salvageable equipment * Supports the cleanup of the data center following an incident * Develops and maintains a damage assessment plan * Estimates levels of outside assistance required * Reports updates, status, and recommendations to the ISCP coordinator |
| **{Team Name}** |  | * Determines the expected duration of the failover to the alternate site * Prioritizes the sequence of resource recovery * Performs all system recovery and resumption activities * Powers on / off systems * Retrieves backup tapes * Configures systems * Ensures voice and data communications are functioning: activate pagers, sat phones, etc. * Provides IP numbers and network routing information * Includes validation testing teams or personnel |

Table 8: {site name} ISCP Roles and Responsibilities (Primary and Alternate)

# ACTIVATION AND NOTIFICATION

The activation and notification phase defines initial actions taken once a VAM disruption has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the ISCP. At the completion of the activation and notification phase, VAM ISCP staff will be prepared to perform recovery measures to restore system functions.



## Activation Criteria and Procedures

The VistA Adaptive Maintenance ISCP may be activated when one or more of the following criteria are met:

1. The type of outage indicates VAM will be down for more than RTO.
2. The ISCP Director determines that VAM can be recovered on the primary site***.***
3. {Additional Notification Procedures}

Additionally, the decision to activate the VAMISCP may require the ISCP Director to consult with the facility leadership.

## Notification Procedures

The first step upon activation of the VAM ISCP is notification of appropriate business and system support personnel.

Notification procedures may include:

Identification of who makes the initial notifications;

The sequence in which personnel are notified (e.g., ISCP coordinator, business / service line POC, outage assessment team POC, and recovery team POC);

The method of internal and external notifications (e.g., email, mobile phone, automated notification system; etc.);

What to do if any single person in the notification sequence cannot be reached; and

Alert / notification messages.

{Additional Notification Procedures}

For a full list of all ISCP specific key personnel and contact information, refer to Appendix A.

For a list identifying leadership, recovery personnel and any facility POCs that are to be alerted of the ISCP activation, refer to Appendix A.

Call trees are an effective means of conveying the communication sequence in which leadership, recovery personnel, and facility POCs should be alerted. Refer to Appendix B.

## Outage Assessment

Following notification, a thorough outage assessment is necessary to determine the extent of the disruption, any damage, potential for further disruption or system damage, and an expected recovery time of VAM.

The outage assessment team conducts this outage assessment. Assessment results are provided to the ISCP coordinator to assist in the coordination of the recovery of VAM. The outage assessment process is located in Appendix G.

# RECOVERY

The recovery phase provides formal recovery operations that begin after the ISCP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery phase activities focus on implementing recovery **strategies** to restore system capabilities through the restoration of IS components, repair of damage, and resumption of operational capabilities at the original or new permanent location. At the completion of the recovery phase, VAM will be functional and capable of performing the functions identified in the plan.

**Note**: ***If the original facility is declared unusable, refer to the VAEC AWS*  *DRP for guidance on recovering data and system operations at the alternate site.***



## Sequence of Recovery Activities

The following high-level activities occur during the VAM recovery phase:

1. Identify recovery location (if not at original location);
2. Identify all required resources to perform recovery procedures;
3. Retrieve backup and system installation media;
4. Recover hardware and operating system (OS) (if required);
5. Recover system from backup and system installation media (refer to Appendix I);
6. Recover system from detailed recovery procedures (refer to Appendix J); and
7. Perform validation and functional system tests (refer to Appendix K).

{Additional Sequence of Recovery Activities}

## Escalation Notices / Awareness

Notifications include problem escalation to leadership and status awareness to system owners and users. Call Trees are an effective means of conveying the communication sequence in which leadership, recovery personnel and facility POC should be alerted.

# RECONSTITUTION

Reconstitution is the process by which a recovered system is tested to validate system capability and functionality. During reconstitution, recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. This phase consists of two major activities – validating successful recovery and deactivation of the plan*.*



## Concurrent Processing

If concurrent processing occurs for the system prior to making it operational, see Appendix L for the appropriate procedures.

## Data Validation and Functionality Testing

Data validation and functionality testing is the process of testing and validating recovered data, data files or databases and functionality after the IS Service has been completely recovered , before granting user access. See Appendix K for the data validation and functionality testing procedures.

## Reconstitution Declaration

Upon successfully completing testing and validation, the ISCP Director will formally declare recovery efforts complete. Facility leadership, business / service line and technical POCs will be notified of the declaration by the ISCP Director.

## Notifications (Users)

Upon return to normal system operations, VAM users will be notified by the ISCP director or designee using predetermined notification procedures (e.g., VA-PAS, email, broadcast message, phone calls; etc.).

## Cleanup

Cleanup is the process of restocking supplies used, returning manuals or other documentation to their original locations, and readying the system for a possible future contingency event. See Appendix M for the cleanup procedures.

## Offsite Data Storage

It is important that all backup and installation media used during recovery be returned to the offsite data storage location (as applicable). See Appendix E for alternate storage site details.

## Data Backup

As soon as reasonable following recovery, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup is then kept with other system backups. See Appendix I for detailed backup procedures.

## Event Documentation

It is important that all recovery events be well documented. It is the responsibility of each recovery team or person to document their actions during the recovery effort, and to provide that documentation to the ISCP Coordinator. Alternatively, one of the recovery teams may be appointed the task of tracking the events. Event documentation should include:

* Activity logs (including recovery steps performed and by whom, the time the steps were initiated and completed, and any problems or concerns encountered while executing activities);
* Functionality and data testing results;
* Lessons learned documentation; and
* After Action Report (AAR).

## Deactivation

Once all activities have been completed and documentation has been updated, the ISCP Director will formally deactivate the ISCP recovery efforts. Notification of this declaration will be provided to all business and technical POCs.

# 

# TEST, TRAINING AND EXERCISE

All ISCPs should be reviewed and tested at least yearly or whenever there is a significant change to the system.

* For low-impact systems, a yearly tabletop exercise is sufficient. The tabletop exercise should include all ISCP POC, and be conducted by an outside or impartial observer.
* For moderate-impact systems, a yearly functional test is required. The functional test should include all ISCP POC and be facilitated by an outside or impartial observer.
* For high-impact systems, a yearly full functional test is required.

The full functional test should include all ISCP POC and be facilitated by an outside or impartial observer. A formal test plan is developed prior to the tabletop or functional test and exercise. Tabletop questions or functional test procedures are developed to include key sections of the ISCP, including a walk-through of the following:

* Notification procedures;
* System recovery on an alternate platform from backup media;
* Internal and external connectivity; and
* Reconstitution procedures.

Results of the test are documented in an after action report, and Lessons Learned are developed for updating information in the ISCP.

Persons or teams with assigned ISCP roles must be trained to respond to a contingency event affecting the VAM efficiently and correctly. VA OIT has developed a test, training and exercise (TT&E) program compliant with the Homeland Security Exercise and Evaluation Program (HSEEP) and supports the following objectives:

* Ensure that organization’s personnel are familiar with the ISCP and its associated activation, recovery, and reconstitution procedures;
* Validate ISCP policies and procedures;
* Exercise procedures through the use of tabletop and functional exercises, as appropriate; and
* Ensure that hardware, software, backup data, and records required to support recovery are available.

**NOTE**: Full functional tests of systems normally are failover tests to the alternate locations, and may be very disruptive to system operations if not planned well. Other systems located in the same physical location may be affected by or included in the full functional test. It is highly recommended that several functional tests be conducted and evaluated prior to conducting a full functional (failover) test.

| **Activities | Tests | Training** | **Frequency** |
| --- | --- |
| DHS test reporting of the formal reporting processes of test results as directed by the Department of Homeland Security (DHS) / Federal Emergency Management Agency (FEMA). This report is prepared by the Office of Operations, Security and Preparedness (OSP) with input from the Administrations and Staff Offices to include OIT. | Annually |
| Alert, Notification, and Activation Procedures Testing for mission critical/emergency personnel. | Annually |
| Continuity Facility Logistics Testing and exercising of required physical security capabilities at the identified continuity facility(s). | Annually |
| Continuity communications testing of communications equipment (both secure and non-secure) to ensure the internal and external interoperability and viability of continuity communications systems and capabilities. | Annually |
| Test ISCP communications. | Annually |
| Test recovery of vital classified and unclassified records, critical information systems, services, and data. | Annually |
| Test ISCP notification/activation procedures. | Annually |
| Internal and External Interdependency Testing of internal and external interdependencies identified in the OI&T CEMP plans, with respect to performance of, and other agencies’ MEFs. | Annually |
| Test primary and backup infrastructure systems and services at alternate operating facilities, (e.g., power, water, fuel). | Annually |
| Documenting and reporting testing of the internal processes for formally documenting and reporting tests and their results. | Annually |
| CEMP Awareness/Orientation training: a high-level overview presentation of CEMP concepts for all OIT staff (both mission critical/emergency personnel and non-mission critical/emergency personnel, to include contractors). | Annually |

Table 9: VAM TT&E Calendar

# DOCUMENT MANAGEMENT



## Document Ownership

The contents of this document are the responsibility ofVAEC AWS , which has assigned the ISCP director with responsibility for its content, modifications, currency, distribution to stakeholders, and its presence in the VA plan repository.

## Plan Review and Maintenance

To ensure currency, this document will be reviewed annually in conjunction with the annual test / exercise and if system modifications occur.

## Document Distribution

A copy of this ISCP will be:

* Provided to system stakeholders who have an interest or responsibility for the development or testing of this plan;
* Held electronically or in hard copy or both by every member of the Outage Assessment and Recovery Teams where it is easily accessible in an emergency;
* Entered in the VA plan repository.
* Stored in an off-site location in both soft and hard copy format for ease of use under a wide range of circumstances.

: Personnel Contact Data - VA

**ISCP Leadership**

| **Key Personnel** | **Contact Information** |
| --- | --- |
| **ISCP Director** | Work #: |
| Name: | VA Cellular #: |
| Title: | VA E-mail: |
| **Alternate ISCP Director** | Work #: |
| Name: | VA Cellular #: |
| Title: | VA E-mail: |
| **ISCP Coordinator** | Work #: |
| Name: | VA Cellular #: |
| Title: | VA E-mail: |
| **Alternate ISCP Coordinator** | Work #: |
| Name: | VA Cellular #: |
| Title: | VA E-mail: |
| **Business / Service Line POC** | Work #: |
| Name: | VA Cellular #: |
| Title: | VA E-mail: |

Table 10: ISCP Personnel Contact Data – VA

**Outage Assessment Team Key Personnel**

| **Key Personnel** | **Contact Information** |
| --- | --- |
| **Team Lead** | Work #: |
| Name: | VA Cellular #: |
| Title: | E-mail: |
| **Team Member** | Work #: |
| Name: | VA Cellular #: |
| Title: | E-mail: |

Table 11: Outage Assessment Team Key Personnel Contact Data

**{Team Name}** **Key Personnel**

| **Key Personnel** | **Contact Information** |
| --- | --- |
| **Team Lead** | Work #: |
| Name: | VA Cellular #: |
| Title: | VA E-mail: |
| **Team Member** | Work #: |
| Name: | VA Cellular #: |
| Title: | VA E-mail: |

Table 12: {Team Name} Key Personnel Contact Data

: Call Tree



Figure 2: Call Tree

: Personnel Contact Data – Vendors

| Vendor Contact Data | Details |
| --- | --- |
| Vendor Name |  |
| Vendor Type |  |
| Address |  |
| City, State, and ZIP Code |  |
| Primary Contact Name |  |
| Office Phone Number |  |
| Emergency Phone Number |  |
| Email Address |  |
| Secondary Contact Name |  |
| Office Phone Number |  |
| Email Address |  |
| SLA/MOU |  |
| Special Instructions |  |

Table 13: ISCP Vendor Contact Data

: Recovery Site

These are the procedures for processing data at the recovery site location when the means to operate at the primary facility is disrupted for a period longer than the RTO.

| Recovery Site | Details |
| --- | --- |
| City |  |
| State |  |
| Distance from Primary Facility |  |
| Is VA Owned |  |
| POC Name |  |
| Procedures for accessing and using the recovery site (Including Security Features) |  |
| Names and contact information for those authorized to go to the recovery site |  |
| Type of Recovery Site, and Equipment Available At Site |  |
| Recovery Site configuration information |  |
| Potential Accessibility problems to the recovery site |  |
| Mitigation steps to access recovery site |  |
| SLAs or other agreements of use of recovery site |  |

Table 14: Recovery Site Data

: Alternate Storage Facility

| Alternate Storage Site | Details |
| --- | --- |
| City |  |
| State |  |
| Names and contact information of persons authorized to retrieve media |  |
| Procedures for retrieving media |  |
| POC Name |  |
| Types of data located at alternate storage site |  |
| Alternate storage configuration features (Including Security Features) |  |
| Is VA Owned? |  |
| Distance from primary facility |  |
| Potential accessibility problems to the alternate storage site |  |
| Mitigation steps to access alternate storage site |  |
| Delivery schedule and procedures for packing media |  |
| SLAs or other agreements of use of alternate storage site |  |

Table 15: Alternate Storage Facility Data

: Alternate Processing Procedures

Substitute, business related, manual processing procedures available that allow the business unit to continue some processing of information that would normally be done by the affected site / facility are listed below.

: Outage Assessment Checklist

List applicable procedures and methodology to determine the scope and impact of a disruption or outage affecting this IS Service.

: Alternate Data / Voice Telecommunications

| Type of Information Needed | Alternate Data/Voice Telecommunications Details |
| --- | --- |
| Name and contact information of carrier |  |
| Geographic locations of vendor facilities |  |
| Contracted Data/Voice Capacity |  |
| SLAs or other agreements for implementation |  |
| Information on Vendor Contingency Plans |  |
| Names and contact information for those authorized to implement/use Capacity |  |

Table 16: Alternate Data/Voice Telecommunications Data

: Data Backup

: Detailed Recovery Procedures

| Recovery Priority | Procedure Name | POC Title |
| --- | --- | --- |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

Table 17: Detailed Recovery Priority Procedures

**Recovery Priority 1 Detailed Procedures:**

**Recovery Priority 2 Detailed Procedures:**

**Recovery Priority 3 Detailed Procedures:**

: Data and Functionality Validation Testing Procedures

Data Validation Testing Procedures

Users can type their Data Validation Testing Procedures here or remove the text box and upload an document.

`

Functionality Validation Testing Procedures

Users can type their Data Validation Testing Procedures here or remove the text box and upload an document.

: Concurrent Processing

: Cleanup

: Business Impact Analysis (BIA)

This business impact analysis (BIA) was developed as a part of the contingency planning process for the VistA Adaptive Maintenance (VAM)**.**

The purpose of the BIA is to identify and prioritize system components by correlating them to the mission / business process(es) the system supports, and using this information to characterize the impact on the process(es) if the system were unavailable.

The BIA is composed of the following three steps:

1. **Determine the mission / business processes and recovery criticality.** Mission / business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum that an organization can tolerate while still maintaining the mission.
2. **Identify resource requirements**. Realistic recovery efforts require a thorough evaluation of the resources required to resume mission / business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.
3. **Identify recovery priorities for system resources**. Based upon the results from the previous activities, system resources can more clearly be linked to critical mission / business processes. Priority levels can be established for sequencing recovery activities and resources.

The following reports are derived from the BIA:

| Business Processes Dependent On This Service |
| --- |
|  |

Table 18: Critical Business Process Mapping / IS Services

| Service / Business Line | MTD |
| --- | --- |
|  |  |

Table 19: Service / Business Line Maximum Tolerable Downtime (MTD)

| IS Service | RTO |
| --- | --- |
|  |  |

Table 20: IS Service Recovery Time Objective (RTO)

| Service / Business Line | MTD | RTO | GAP |
| --- | --- | --- | --- |
|  |  |  |  |

Table 21: Service / Business Line MTD / RTO Gap Analysis

: ISCP Glossary

**Alternate Processing Procedures**—Procedures that can be initiated in lieu of the application to maintain business operations during an outage.

**Alternate Site**—A location, other than the systems primary location, used to continue operational capabilities during a significant system disruption.

**Business Impact Analysis (BIA)**—An analysis of an information system’s requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

**Critical Business Process (CBP)**—the operational and / or business support functions that could not be interrupted or unavailable for more than a mandated or predetermined timeframe without significantly jeopardizing the organization.

**Data**—A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means.

**Disruption**—An unplanned event that causes an information system to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

**Disaster Recovery Plan (DRP**)—A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.

**Hardware**—The mechanical, magnetic, electrical, and electronic devices or components of an information system.

**Information System (IS)**—An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, and control data or information. An information system will consist of automated data processing system hardware, operating system and application software, peripheral devices, and associated data communications equipment.

**IS Contingency Plan (ISCP)** — Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters.

**Information System Contingency Planning**—Information system contingency planning refers to the dynamic development of a coordinated recovery strategy for information systems, operations, and data after a disruption.

**Information System Contingency Plan Assessment (ISCPA) Process**—The nine-step process for contingency planning within VA.

**Maximum Tolerable Downtime (MTD)** — The amount of time mission/business process can be disrupted without causing significant harm to the organization’s mission.

**Operating System (OS)**—An organized collection of techniques, procedures, programs, or routines for operating an information system, usually supplied by the system hardware vendor.

**Recovery Time Objective (RTO)** — The overall length of time an information system’s components can be in the recovery phase before negatively impacting the organization’s mission or mission/business processes.

**System**—A generic term used for briefness to mean either a major application or a general support system.

**Test**—An evaluation tool that uses quantifiable metrics to validate the operability of a system or system component in an operational environment specified in an ISCP.

**Test Plan**—A document that outlines the specific steps that will be performed for a particular test, including the required logistical items and expected outcome or response for each step.

**User**—A person who accesses information systems to use programs or applications in order to perform an organizational task.

: ISCP Acronym List

| Term / Abbreviation | Description |
| --- | --- |
| AAR | After Action Report |
| BIA | Business Impact Assessment |
| CBP | Critical Business Process |
| CP | Contingency Planning |
| DHS | Department of Homeland Security |
| DRP | Disaster Recovery Plan |
| FEMA | Federal Emergency Management Administration |
| GRC | Governance, Risk Management, and Compliance |
| HSEEP | Homeland Security Exercise and Evaluation Program |
| ID | Identification |
| IP | Internet Protocol |
| IS | Information System |
| ISA | Interconnected System Agreement |
| ISCP | Information System Contingency Plan |
| ISCPA | Information System Contingency Planning Assessment |
| IT | Information Technology |
| LAN | Local Area Network |
| MOU / A | Memorandum of Understanding / Agreement |
| MTD | Maximum Tolerable Downtime |
| NIST | National Institute of Standards and Technology |
| OCS | Office of Cyber Security |
| OIT | Office of Information Technology |
| OS | Operating System |
| PBX | Private Branch Exchange |
| POC | Point of Contact |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| SLA | Service Level Agreement |
| SN | Serial Number |
| SOP | Standard Operating Procedure |
| SP | Special Publication |
| SSP | System Security Plan |
| TT&E | Test, Training, and Exercise |
| VA | Department of Veterans Affairs |

Table 22: Acronym List

**This Page Intentionally Left Blank**