**SENSITIVE BUT UNCLASSIFIED**

OFFICE OF INFORMATION SECURITY

Vista Adaptive Maintenance (VAM)

Disaster Recovery Plan

8/30/2018

OIS INTERNAL DOCUMENT

NOT FOR EXTERNAL DISTRIBUTION



Table of Contents

Document Change Control Record ..................................................................................3

Disaster Recovery Plan (DRP) Approval ...........................................................................4

DRP Distribution...............................................................................................................5

1. INTRODUCTION...........................................................................................................6

1.1 Objective...........................................................................................................................7

1.2 Scope ................................................................................................................................7

1.3 DRP Assumptions and Constraints....................................................................................9

1.4 DRP Roles and Responsibilities .......................................................................................10

2. CONCEPT OF OPERATIONS........................................................................................11

2.1 Activation and Notification .............................................................................................12

2.2 Recovery Site(s) ..............................................................................................................12

3. RECOVERY .................................................................................................................13

4. RECONSTITUTION......................................................................................................14

5. TEST, TRAINING AND EXERCISE.................................................................................15

6. DOCUMENT MANAGEMENT .....................................................................................16

6.1 Document Ownership.....................................................................................................16

6.2 Plan Review and Maintenance .......................................................................................16

6.3 Document Distribution ...................................................................................................16

Appendix A : DRP Personnel Contact Data - VA........................................................... A-1

Appendix B : Call Tree .................................................................................................. B-1

Appendix C : Personnel Contact Data – Vendors......................................................... C-2

Appendix D : Alternate Storage Site ............................................................................D-1

Appendix E : Telecommunications................................................................................E-1

Appendix F : Recovery Site............................................................................................F-1

Appendix G : Associated Plans.....................................................................................G-1

Appendix H : DRP Glossary...........................................................................................H-1

Appendix I : DRP Acronym List...................................................................................... I-1

Table of Figures

Figure 1: VAM Architecture Diagram ..............................................................................8

**List of Tables**

Table 1: Document Change Control.................................................................................3

Table 2: DRP Distribution List...........................................................................................5

Table 3: VAM IS Services/Applications/IS Support Services............................................9

Table 3: VAM IS Services/Applications/IS Support Services..........................................12

Table 8: DRP Personnel Contact Data – VA.................................................................. A-1

Table 12: Vendor Contact Data.................................................................................... C-2

Table 13: Alternate Storage Site ..................................................................................D-1

Table 14: Telecommunications .....................................................................................E-1

Table 15: Recovery Site.................................................................................................F-1

Table 16: Associated Plans...........................................................................................G-1

Table 17: IS Services [Application/IS Support Services] Recovery Priority Ranking ....G-1

Table 18: Acronym List.................................................................................................. I-1

Document Change Control Record

**Version Release Date Summary Of Changes Author**

**1.0** 8/30/2018 Initial Draft AbleVets

*Table 1: Document Change Control*

Disaster Recovery Plan (DRP) Approval

As the designated authority for the Vista Adaptive Maintenance, hereafter known as (VAM), I hereby certify that the VAM Disaster Recovery Plan (DRP) is complete and that the information contained provides an accurate representation of the recovery requirements for this site / facility. I further certify that this document identifies the criticality of VAM, and that the recovery strategies identified will provide the ability to recover VAM and each information system in the most expedient and cost-beneficial method in keeping with their individual level of criticality.

Privacy Officer

Information Security Officer

DRP Distribution

Distribution of the DRP should be restricted to personnel involved in, or responsible for, the activities for the continued operations of the site/facility, the information 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.

**Name Role**

*Table 2: DRP Distribution List*

1. INTRODUCTION

Information Systems (IS) are vital to the Department of Veterans Affairs (VA) business processes. This DRP for VAM should establish comprehensive procedures to recover the site critical IS Services quickly and effectively following a disaster or extended critical disruption. It is important that IS Services can effectively operate at a recovery facility independent from the primary facility to ensure continued operations. The DRP is one plan within a suite of security and emergency management-related plans that provides guidance for fast recovery when a disaster impacts a VA facility.

As per NIST SP 800-34, the DRP applies to a major, usually physical disruption to service that deny access to the primary facility infrastructure for an extended period. A DRP is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency. The DRP may be supported by multiple information system contingency plans to address recovery of impacted individual systems once the alternate facility has been established.

VAM’s DRP is, in applicable parts, compliant with the following guidance and directives:

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, Fed*eral 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

1.1 Objective

The purpose of VAM DRP is to provide a documented plan that addresses the restoration of mission critical IS Services and operations from a recovery site following an event that prevents the normal continuation of those services from the organization’s primary site.

1.2 Scope

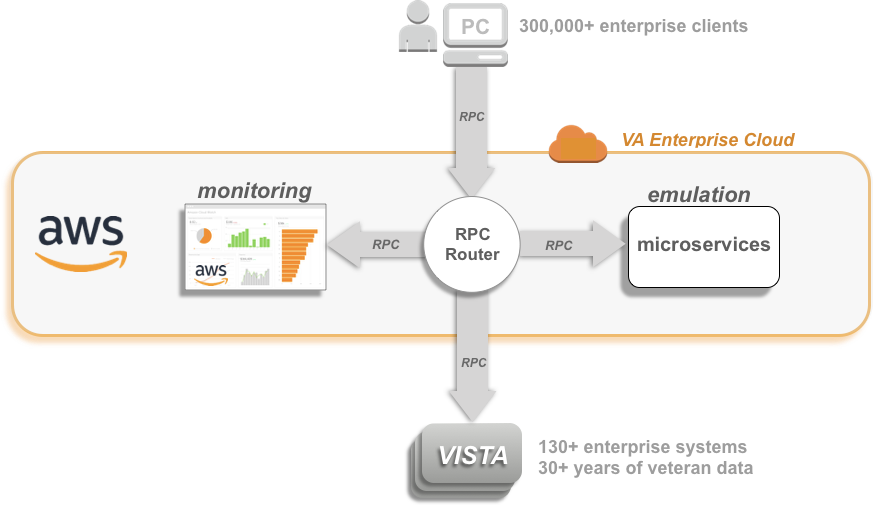
VAM’s DRP has been developed in accordance with federal guidance NIST 800-34, Rev 1 and Federal Risk and Authorization Management Program (FedRAMP) standards. Specific VAM Services procedures and instructions are described within the DRP.

*1.2.1 System Description*

VISTA Adaptive Maintenance (VAM) provides a cloud-based roadmap and software for maintaining continuity of the Veterans Information Systems Technology Architecture (VISTA) and the VA workflows it supports using straightforward off-the-shelf commercial cloud services and microservices during the multi-year EHR modernization (EHRM) program. VAM will be deployed within the VA’s Enterprise Cloud using Amazon Web Services (AWS) and Amazon CloudWatch.

The VAM Project will provide adaptive sustainment services to enable VA to migrate Veterans Information Systems and Technology Architecture (VistA) off of its Massachusetts General Hospital Utility Multi-Programming System (MUMPS) infrastructure to provide backwards and forwards compatibility for VistA domains and use cases including Patient Data Entry and Pharmacy Computerized Physician Order Entry (CPOE).

*The VAM Architecture is provided in the Figure below:*



*Figure 1: VAM Architecture Diagram*

*1.2.2 System Testing*

Annual DRP testing is the responsibility of the VAM. VAM Services are tested annually by the VAM team and documented in the VAM ISCP. The information below documents Service Level Agreements (SLAs) provided by the VAM.

**Service / Business Line MTD**

VAM 12 hours

**Service / Business Line MTD RTO RPO**

Server Configuration Management Service Code Configuration and Release Management Services

6 hours 6 hours 6 hours

6 hours 6 hours 6 Hours

*Table 3: VAM IS Services/Applications/IS Support Services*

1.3 DRP Assumptions and Constraints

The following assumptions were used when developing this DRP:

The VAM is responsible for maintaining the DR site.

The VAM is responsible for annual DR testing.

The VAM Personnel well versed in the day-to-day IS service operating procedures are available to operate at the recovery site.

Relocated IS Service recovery teams are prepared to deal with emergency procedures without the need to reference detailed written steps.

The VAM management personnel with authority will be available to make decisions.

Alternate processing procedures (or workarounds) for critical business processes have been established by

Service/Business lines and are listed in the VAM ISCP for each system.

VAM’s DRP plan does not apply to the situations described below:

Disruptions deemed recoverable at the primary site.

Emergency evacuation of personnel, addressed by the occupant evacuation plan.

Overall recovery of business operations. Service/Business line owners should address recovery of business operations in a separate business recovery plan.

*1.3.1 Backup and Recovery Solution Design in VAM*

The VAM is responsible for backup and recovery of data needed to restore operations to the requisite sites.

As depicted in Figure 1, “VAM Architecture Diagram”, the VAM Infrastructure is designed to be highly available, fault tolerant and scalable.

The VAM also implements backup processes that offer the appropriate level of granularity to meet pre-defined RTO and RPO (listed in Table 3) that includes:

File-level recovery

Volume-level recovery

Container-level recovery

1.4 DRP Roles and Responsibilities

Roles and responsibilities are provided by VAM personnel and inherited from VAEC AWS GovCloud High.

2. CONCEPT OF OPERATIONS

The VAM is responsible for backup and recovery of data needed to restore operations to the requisite sites.

Disaster recovery (DR) is about preparing for and recovering from a disaster, that is, any event having a negative impact on your business continuity or security. This could include hardware or software failure, a network outage, a power outage, physical damage to a building like fire or flooding, human error, malicious occurrence,

or some other significant disaster. Several Federal Information Processing Standards (FIPS) and National Institute of Standards and Technology (NIST) policies are relevant to VA in this context: FIPS 199, FIPS 200, NIST SP 800-

34, and NIST SP 800-53. Additionally, VA Handbooks 6500, 6500.5, and 6500.8 address how the 800- 53 controls

are applied and implemented for systems and applications developed for, or used by, VA. Regular testing of DR plans is critical to train staff and to assess and validate DR components. Without regular, rigorous, and realistic testing, DR plans and solutions are almost certain to fail in the event of a disaster. A key concept is the difference between high availability (HA) and DR. As a practical matter, HA addresses routine component, sub-

system or system failures, while DR addresses catastrophic failures or events that could take down an entire site. Proper DR planning requires understanding of the following industry terms:

• Recovery Time Objective (RTO) – The time it takes after a disruption to restore a business process to its service level, as defined by the DR plan within the programs accreditation package.

• Recovery Point Objective (RPO) – The acceptable amount of data loss measured in time. In addition to these industry standards, VA also uses and requires the following:

• Business Impact Analysis (BIA) – a BIA, as defined by NIST Special Publication (SP) 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems, is an analysis of an information system’s requirements, functions, and interdependencies, and must correlate information systems with critical mission/business processes (e.g., VA’s Mission Essential Functions (MEFs)) and respective services.

• Maximum Tolerable Downtime (MTD) – total amount of time that is acceptable for a mission/business process outage or disruption, determined by utilizing BIA constructs.

VAM Services are tested annually by the VAM team and documented in the VAM ISCP. The information below documents Service Level Agreements (SLAs) provided by the VAM.

**Service / Business Line MTD**

VAM 12 hours

**Service / Business Line MTD RTO RPO**

Server Configuration Management Service Code Configuration and Release Management Services

6 hours 6 hours 6 hours

6 hours 6 hours 6 hours

*Table 3: VAM IS Services/Applications/IS Support Services*

2.1 Activation and Notification

The Activation and Notification Phase defines initial actions taken once a disruption has been detected and recovery activities appear to be imminent. The ISCP Activation and Notification Phase define the activities required to activate the ISCP and notify supporting recovery personnel. Notification and activation criteria and procedures are documented in the VAM ISCP.

*2.1.1 Accountability of OIT Recovery Personnel*

In the event of a natural or man-made disaster, VAM Package #: F1603047866 states that all requisite infrastructure and services required to restore site operations are replicated across VAM data centers (zones).

2.2 Recovery Site(s)

A recovery site/facility provides a location where the systems and operations and hosted in the original facility can be resumed or recovered in the event of a catastrophic event that disables or destroys the primary facility. This information is located in Section 3.

3. RECOVERY

The VAM is responsible for recovery of data needed to restore operations to the requisite sites. VAM inherits recovery from VAEC AWS GovCloud High. VAM documents recovery and reconstitution procedures for IS services in the VAM ISCP.

4. RECONSTITUTION

The VAM is responsible for reconstitution of data needed to restore operations to the requisite sites. VAM inherits recovery from VAEC AWS GovCloud High. VAM documents recovery and reconstitution procedures for IS services in the VAM ISCP.

5. TEST, TRAINING AND EXERCISE

The VAM is responsible for TTE with respect to restoration of operations to the requisite sites. VAM inherits TTE from VAEC AWS GovCloud High. VAM conducts annual ISCP TTE for IS services in accordance with VA Handbook 6500.

6. DOCUMENT MANAGEMENT

6.1 Document Ownership

The contents of this document are the responsibility of the VAM, which has assigned the ISCP coordinator responsibility for its content, modifications, currency, distribution to stakeholders, and its presence in the VA document repository.

6.2 Plan Review and Maintenance

To ensure currency, this document will be reviewed annually in conjunction with the annual ISCP TTE and when systems within the VAM boundary incur significant modifications.

6.3 Document Distribution

A copy of the VAM DRP is in the Risk Vision instance of VAM. Additionally, a copy the VAM DRP will be:

Provided to facility stakeholders (listed in Plan Distribution table at the front of this document) 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 recovery teams where it is easily accessible in an emergency.

Stored in the VA document repository.

Stored in an off-site location in both soft and hard copy format for ease of use under a wide range of circumstances

Appendix A: DRP Personnel Contact Data - VA

**DRP Leadership**

**Key Personnel Contact Information**

ISCP Director Work #: (512) 326-6269

Name: Louis Lugo VA Cellular #: (512) 663-1395

Title: Director, Business Continuity Management VA E-mail: louis.lugo@va.gov

Alternate ISCP Director Work #: (512) 820-7329

Name: Christopher Cockle VA Cellular #: (512) 820-7329

Title: Business Continuity IT Specialist VA E-mail: Chris.Cockle@va.gov

ISCP Coordinator Work #: 512-663-1630

Name: Chris Lopez VA Cellular #: 512-663-1630

Title: Chris Lopez VA E-mail: Chris.Lopez@va.gov

Alternate ISCP Coordinator Work #: 512-745-5795

Name: Ertha Patrick VA Cellular #: 512-745-5795

Title: Business Continuity Program Manager VA E-mail: Ertha.Patrick@va.gov

Outage Assessment Team POC Work #: 512-326-6180

Name: Christopher Cardella VA Cellular #: 512-590-9414

Title: Manager, Cloud Infrastructure VA E-mail: Christopher.Cardella@va.gov

Alternate Outage Assessment Team POC Work #: (512) 850-9341

Name: Brandon Petersen VA Cellular #: (512) 850-9341

Title: IT Specialist, Core Systems Engineering VA E-mail: Brandon.Petersen@va.gov

Business / Service Line POC Work #: 512-326-6180

Name: Christopher Cardella VA Cellular #: 512-590-9414

Title: Manager, Cloud Infrastructure VA E-mail: Christopher.Cardella@va.gov

Business / Service Line POC (Alternate) Work #: (512) 326-6114

Name: Ralph Parkison VA Cellular #: (512) 820-7325

Title: Information Technology Specialist, System

Analyst, Cloud Archite, IT Operations and Services

*Table 8: DRP Personnel Contact Data – VA*

VA E-mail: Ralph.Parkison@va.gov

Appendix B: Call Tree

**Orders of Succession**

The line of succession lists personnel responsible to assume authority for executing this plan in the event the designated person (Team Leader) is unavailable, unable, or chooses to delegate the responsibility to a successor.

**Name Role Telephone Email Priority**

Louis Lugo ISCP Director Work #: (512) 326-

6269

Cell #: (512) 663-1395

louis.lugo@va.gov 1

Christopher Cockle ISCP Director

(Alternate)

Work #: (512) 820-

7329

Cell #: (512) 820-7329

Chris.Cockle@va.gov 2

Chris Lopez ISCP Coordinator Work #: 512-663-1630

Cell #: 512-663-1630

Chris.Lopez@va.gov 3

Ertha Patrick ISCP Coordinator

(Alternate)

Work #: 512-745-5795

Cellular #: 512-745-

5795

Ertha.Patrick@va.gov 4

Appendix C: Personnel Contact Data – Vendors

**Vendor Contact Data Details**

Vendor Name VAM

Vendor Type Contractor

Address 15049 Conference center

City, State, and ZIP Code Chantilly, VA, 20151

Primary Contact Name Dr. Wyatt Smith

Office Phone Number 571.379.2745

Email Address [wyatt.smith@ablevets.com](mailto:wyatt.smith@ablevets.com)

Secondary Contact Name Jeff Miller

Email Address Jeff.Miller@ablevets.com

SLA/MOU NA

URLs NA

*Table 12: Vendor Contact Data*

Appendix D: Alternate Storage Site

These site recovery services are inherited from the VAM VAEC AWS Gov Cloud High.

Appendix E: Telecommunications

These site recovery services are inherited from the VAM VAEC AWS Gov Cloud High.

Appendix F: Recovery Site

These site recovery services are inherited from the VAM VAEC AWS Gov Cloud High.

Appendix G: Associated Plans

|  |  |  |  |
| --- | --- | --- | --- |
| **ISCP or other (Full Name)** | **Version #** | **Location (URL if web based)** | **POC Title** |
| VAM ISCP | 1.2 | Risk Vision | Bobby Begay (ISO) |

*Table 16: Associated Plans*

|  |  |
| --- | --- |
| **IS Services [Application/IS Support Services]** | **Recovery Priority** |
| Authentication Services | 1 |
| Server Configuration Management Service | 2 |

*Table 17: IS Services [Application/IS Support Services] Recovery Priority Ranking*

Appendix H: DRP Glossary

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

**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. The ISCP provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system. The ISCP differs from a DRP primarily in that the information system contingency plan procedures are developed for recovery of the system regardless of site or location.

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

**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.

Appendix I: DRP Acronym List

**Term / Abbreviation**

DRP Disaster Recovery Plan

IS Information Systems

VA Department of Veterans Affairs

ISCP Information System Contingency Plan

**Description**

FISMA Federal Information Security Management Act

DHS Department of Homeland Security

HSEEP Homeland Security Exercise and Evaluation Program (NIST) SP Special Publication

FedRAMP Federal Risk and Authorization Management Program

VBA Veterans Benefits Administration VHA Veterans Health Administration NCA National Cemetery Administration

FIPS Federal Information Processing Standard

VPC Virtual Private Cloud

ICAM Identity, Credential, and Access Management

AD Active Directory

SLAs Service Level Agreements

DR Disaster recovery

HA high availability

RTO Recovery Time Objective RPO Recovery Point Objective BIA Business Impact Analysis MEFs Mission Essential Functions

MTD Maximum Tolerable Downtime

ISCPA Information System Contingency Plan Assessment

OS Operating System

*Table 18: Acronym List*

**This Page Intentionally Left Blank**