|  |
| --- |
|  |
| **VA Enterprise Cloud (VAEC)**  **Amazon Web Services GovCloud High (AWS)**  And [Organization 2 name/acronym] [GRC Boundary Alignment] [Security Categorization: low/medium/high]  Disaster Recovery Plan |
| month yyyy |

OIT/OIS brand color cover art

Table of Contents

[Document Change Control Record 4](#_Toc528238417)

[Disaster Recovery Plan (DRP) Approval 5](#_Toc528238418)

[DRP Distribution 6](#_Toc528238419)

[1. INTRODUCTION 7](#_Toc528238420)

[1.1 Objective 8](#_Toc528238421)

[1.2 Scope 8](#_Toc528238422)

[1.3 DRP Assumptions and Constraints 10](#_Toc528238423)

[1.4 DRP Considerations 11](#_Toc528238424)

[1.5 DRP Roles and Responsibilities 11](#_Toc528238425)

[1.6 Threats and Vulnerabilities 13](#_Toc528238426)

[2. CONCEPT OF OPERATIONS 14](#_Toc528238427)

[2.1 Activation and Notification 14](#_Toc528238429)

[2.2 Recovery Site(s) 15](#_Toc528238430)

[3. RECOVERY 17](#_Toc528238431)

[3.1 Sequence of Recovery Activities 17](#_Toc528238433)

[3.2 Escalation Notices / Awareness 17](#_Toc528238434)

[4. RECONSTITUTION 18](#_Toc528238435)

[4.1 Concurrent Processing – IS Services 18](#_Toc528238437)

[4.2 Data Validation and Functionality Testing 18](#_Toc528238438)

[4.3 Reconstitution Declaration 18](#_Toc528238439)

[4.4 Notifications (Users) 18](#_Toc528238440)

[4.5 Cleanup 18](#_Toc528238441)

[4.6 Offsite Data Storage 18](#_Toc528238442)

[4.7 Data Backup 19](#_Toc528238443)

[4.8 Event Documentation 19](#_Toc528238444)

[4.9 Deactivation 19](#_Toc528238445)

[5. TEST, TRAINING AND EXERCISE 20](#_Toc528238446)

[6. DOCUMENT MANAGEMENT 22](#_Toc528238447)

[6.1 Document Ownership 22](#_Toc528238450)

[6.2 Plan Review and Maintenance 22](#_Toc528238451)

[6.3 Document Distribution 22](#_Toc528238452)

[Appendix A : DRP Personnel Contact Data - VA A-1](#_Toc528238453)

[Appendix B : Call Tree B-1](#_Toc528238454)

[Appendix C : Personnel Contact Data – Vendors C-1](#_Toc528238455)

[Appendix D : Alternate Storage Site D-1](#_Toc528238456)

[Appendix E : Telecommunications E-1](#_Toc528238457)

[Appendix F : Recovery Site F-1](#_Toc528238458)

[Appendix G : Associated Plans G-1](#_Toc528238459)

[Appendix H : DRP Glossary H-1](#_Toc528238460)

[Appendix I : DRP Acronym List I-1](#_Toc528238461)

# Table of Figures

Figure 1: VAEC AWS GovCloud High Architecture Diagram 10

Figure 2: DRP Call Tree B-1

# List of Tables

Table 1: Document Change Control 4

Table 2: DRP Distribution List 6

Table 3: IS Services/Applications/IS Support Services 10

Table 4: Roles and Responsibilities 13

Table 5: VAEC AWS Threat Assessment 13

Table 6: VAEC AWS Vulnerability Assessment 13

Table 7: TT&E Calendar 21

Table 8: DRP Personnel Contact Data – VA A-2

Table 9: Primary Site VAEC AWS Key Personnel Contact Data A-2

Table 10: Recovery Site VAEC AWS Key Personnel Contact Data A-2

Table 11: VAEC COMS Cyber Security Key Personnel Contact Data A-3

Table 12: Vendor Contact Data C-1

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

Entries in Green are instructions

Entries in RED are to be completed

Entries in BLACK are not to be changed, they are boiler plate

[Organization2] is the organization joining VAEC AZURE

All colored languages are to be removed

# Document Change Control Record

| Version | Release Date | Summary Of Changes | Author |
| --- | --- | --- | --- |
| **1.0** | 6/2/2017 | Initial Draft | Sathishbabu  Sandu/Ji Jung |
| **1.1** | 7/10/2017 | Review and update | Peter Davies,  MPG/CSRA |
| **1.2** | 11/14/2017 | Various Updates | Daniel Beaver/  Wilbert Francis,  MPG/CSRA |
| **1.3** | 11/14/2017 | Review and update | Peter Davies,  MPG/CSRA |
| **2.0** | 10/25/2018 | Updated to most recent template and added additional content | Kathleen Kerndt,VAEC Security Team/Cognosante  Organization 2 Author name - [System Acronym] |

Table 1: Document Change Control

Provide organization Author name and System Acronym in the document change control record table

# Disaster Recovery Plan (DRP) Approval

As the designated authority for VA Enterprise Cloud (VAEC) for Amazon Web Services GovCloud (AWS) High, hereafter known as VAEC AWS, I hereby certify that the VAEC AWS 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 VAEC, and that the recovery strategies identified will provide the ability to recover VAEC and each information system in the most expedient and cost-beneficial method in keeping with their individual level of criticality.

I further attest that this DRP for VAEC will be tested at least annually. This plan was last tested on August 27, 2018.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, and VA Handbook 6500.8 Information System Contingency Planning guidance.

/ s /

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

David Catanoso

Director, Technical Lead

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

Joseph Stevenson

Manager, Cloud Infrastructure

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

Charles L Solomon-Jackson

Information Security Officer

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

Joseph Fourcade

Project Manager

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

Christopher Cardella

CIO

Organization 2 [System Acronym] signatory authorities

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

<Plan Approver Name>

<Job Title>

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

<Plan Approver Name>

<Job Title>

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

<Plan Approver Name>

<Job Title>

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

<Plan Approver Name>

<Job Title>

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.

**VAEC**

| Name | Title |
| --- | --- |
| Submitted via Risk Vision | VA AO via RiskVision |
| Joseph Stevenson | DRP Coordinator |
| Nagesh Gadamsetty | DRP Coordinator (Alternate) |
| David Catanoso | DRP Director |
| Joseph Stevenson | DRP Director (Alternate) |
| Christopher Cardella | Outage Assessment Team POC |
| Eugene Tai | Outage Assessment Team POC (Alternate) |
| David Catanoso | Business / Service Line POC |
| Joseph Stevenson | Business / Service Line POC (Alternate) |
| John Fisher | COMS Service Delivery Lead |
| Joseph Fourcade | Cyber Security |
| Ben Grafton | Director Technical Lead COMS |
| Matt Mullican | Director Technical Lead, AWS COMS |
| Charles L Solomon-Jackson | Information Security Officer (ISO) |
| Michael Lucas | Cybersecurity Team Lead COMS |
| Nick Hill | Infrastructure Manager COMS |
| Ruslan Best | Infrastructure Technical Lead COMS |
| William McDonough | Cloud System Architect |
| Lowell Wheeler | Cloud System Administrator COMS |
| Cheryl Owsley, COR and IT Project Manager  VA | VA POC |
| Lia Burrus, IT Project Manager  VA | VA POC |
| Eugene Tai, IT Project Manager VA | VA POC |
| All Disaster Recovery Activation Teams  Cognosante  Department of Veterans Affairs (VA)  Microsoft Azure Government (MAG)  Amazon Web Services (AWS) | Disaster Recovery Activation Team |

Enter your organization DRP distribution in the table below

[Organization 2 name/acronym]

| Name | Title |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Table 2: DRP Distribution List [Organization 2 name/acronym]

# INTRODUCTION

Information Systems (IS) are vital to the Department of Veterans Affairs (VA) business processes. This disaster recovery plan (DRP) for the VAEC Amazon Web Services GovCloud High establishes 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 are able to 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.

VAEC is a cloud-based GSS, hosted on Amazon Web Services GovCloud (AWS); FedRAMP package #: F1603047866. As per AWS’s FedRAMP authorization, AWS is responsible for all DRP activities within this environment. AWS’s DRP can be found in FedRAMP package #: F1603047866. The AWS is designed utilizing separate data centers (zones), and geographically separated regions. Currently AWS has two regions located in Iowa and Virginia. Based on the foregoing, the VAEC system DRP responsibilities are inherited from AWS FedRAMP package #: F1603047866.

All core services functions are replicated from AWS AZ 1 to AWS AZ 2. VAEC Information System Contingency

Plan (ISCP) documents the recovery and reconstitution procedures for the VAEC core services and hosted

applications within the VAEC system boundary.

This 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

## Objective

The purpose of the VAEC AWS and [Organization 2 name/acronym] DRP is to provide a documented plan to address 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. The DRP is supported by the Information System Contingency Plans (ISCP) for each critical IS Service at the affected facility and describes the coordination activities between the primary, and recovery site(s) that are required to recover and continue IS service operations.

## Scope

The VAEC AWS and [Organization 2 name/acronym] DRP has been developed for increasing the organizations’ resiliency posture in the face of an emergency that jeopardizes IS Services and operations in a specific facility. It was written in accordance with federal guidance NIST 800-34, Rev 1 and VA Handbook 6500.8. Specific IS Service procedures and instructions described within this DRP are for systems hosted within the VAEC AWS and [Organization 2 name/acronym]. The DRP does not address disruptions that can be resolved at the primary site either through the electronic transfer of data to an alternate location or through the acquisition and delivery of necessary backups to a different processing location. 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.

ISCPs for each IS Service are referenced in the DRP in order to assist in the restoration of critical systems or transfer of critical systems’ data to the recovery site after it has been appropriately configured.

### System Description

The VA Enterprise Cloud AWS GovCloud High (VAEC is a General Support System that provides a secure application and hosting environment for VA applications, content, and utilities.  These applications and services are used to deliver content to an audience made up of employees, veterans, contractors, partners across all VA medical centers and component facilities, Federal government, and the general public. Content

and applications are provided by Veterans Benefits Administration (VBA), Veterans Health Administration (VHA),

National Cemetery Administration (NCA) and Support Offices. VAEC provides the following services: Content

delivery, Application Hosting and Management Services.

The VAEC infrastructure is hosted by AWS GovCloud, a cloud service provider. The AWS GovCloud platform is

used to provide a variety of hosting environments to suit a variety of needs. AWS GovCloud can support

applications categorized up to High as rated in accordance with Federal Information Processing Standard (FIPS)

199. VA applications available to the public are hosted in AWS GovCloud.

A dedicated private data link (AWS Direct Connect) provides all connectivity for VA resources communicating to

the environment. Virtual Private Clouds (VPCs) wrap the applications within AWS GovCloud to encapsulate

network access. Access from the applications to VA internal resources such as Identity, Credential, and Access

Management (ICAM) and Active Directory (AD) Services are conducted over the encrypted private data link to

the VA Network.

VAEC is located in one region with two Availability Zones designed to allow U.S. government agencies,

contractors and customers to move sensitive workloads into the cloud for addressing specific regulatory and

compliance requirements. AWS GovCloud does not manage logical access controls within the VAEC system

boundary. VAEC offers the same level of security as other VA physical technology centers and supports existing

VA security controls and certification requirements such as FISMA, HIPAA, HITECH, SAS-70, ISO 27001, FIPS 140-

2 compliant end points, and PCI DSS.

*The VAEC AWS GovCloud High Architecture is provided in the Figure below:*

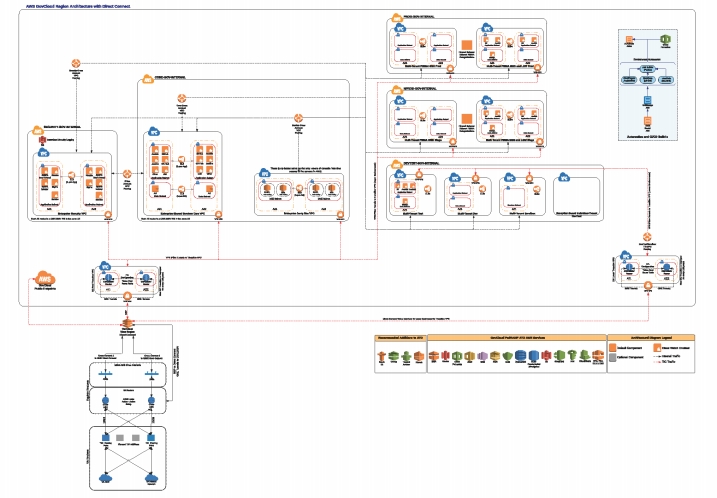


Figure 1: VAEC AWS GovCloud High Architecture Diagram

### Enter your organization System Description here

### VAEC Services

The information below documents Service Level Agreements (SLAs) provided by the VAEC.

|  |  |
| --- | --- |
| **Service / Business Line** | **MTD** |
| VAEC AWS GovCloud High | 6 hours |

|  |  |
| --- | --- |
| **Service / Business Line** | **MTD** |
| VAEC AWS GovCloud High | 6 hours |

Enter your organization Service / Business Line in the table below.

|  |  |
| --- | --- |
| **Service / Business Line** | **MTD** |
| VAEC AWS GovCloud High | 6 hours |

The information below documents Service Level Agreements (SLAs) provided by the [Organization2 name/acronym].

|  |  |
| --- | --- |
| **Service / Business Line** | **MTD** |
| [Organization 2 name/acronym] [GRC Boundary Alignment] [Security Categorization] |  |

|  |  |
| --- | --- |
| **Service / Business Line** | **MTD** |
| VAEC AWS GovCloud High | 6 hours |

|  |  |
| --- | --- |
| **Service / Business Line** | **MTD** |
| VAEC AWS GovCloud High | 6 hours |

|  |  |
| --- | --- |
| **Service / Business Line** | **MTD** |
| VAEC AWS GovCloud High | 6 hours |

The following IS Services are maintained at VAEC AWS:

| Service Line | IS Service [Applications/IS Support Services] | MTD | RTO |
| --- | --- | --- | --- |
|  | **Authentication Services** | 6 hours | 6 hours |
|  | **Server Configuration Management Service** | 6 hours | 6 hours |
|  | **Vulnerability Scanning Service** | **6 hours** | **6 hours** |
|  | **Monitoring Service** | **6 hours** | **6 hours** |
|  | **JumpBox Service** | **6 hours** | **6 hours** |
|  | **Auditing Service** | **6 hours** | **6 hours** |
|  | **Code Configuration and Release Management Services** | **6 hours** | **6 hours** |

Table 3: IS Services/Applications/IS Support Services

Enter your organization IS Service /applications is serviced  in the table below.

The following IS Services are maintained at [Organization 2 name/acronym].

| Service Line | IS Service [Applications/IS Support Services] | MTD | RTO |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 3: IS Services/Applications/IS Support Services

## DRP Assumptions and Constraints

The following assumptions were used when developing this DRP:

* The AWS GovCloud is responsible for maintaining the DR site.
* The AWS GovCloud is responsible for annual DR testing.
* 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.
* Management personnel with authority will be available to make decisions.
* System and supporting component restoration priorities have been documented within each IS Service’s ISCP.
* Alternate processing procedures (or workarounds) for critical business processes have been established by Service/Business lines and are listed in the ISCP for each system.
* Current backups of the system software and data are intact and available at the offsite data storage facility or facilities.
* The IS Service(s) at AWS are inoperable and cannot be recovered within the recovery time objective (RTO) required to allow the facility to continue to operate normally.

Additional assumptions:

* Applications can inherit the VAEC AWS DRP. An application level DRP is required for application-specific Disaster Recovery processes.

This 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.

## Enter your organization DRP Assumptions and Constraints here

## DRP Considerations

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

As depicted in Figure 1, “VAEC AWS GovCloud Architecture Diagram”, the VAEC AWS infrastructure is designed to be highly available, fault tolerant and scalable by using both AWS GovCloud AZ 1 and AZ 2. The components of the VAEC VPC are designed to be hosted in both AWS GovCloud Availability Zones.

The VAEC is designed with a comprehensive strategy to back up data, by first identifying the failure or disaster situation that can occur and the potential business impact. The VAEC leverages many built-in backup and recovery features of AWS GovCloud. The VAEC 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
  + Image-level recovery
  + Object-level recovery
  + Container-level recovery

The VAEC DRP takes into consideration the existing capabilities of the recovery site locations and documents them along with any associated limitations or restrictions that would hinder data and access for a data center, medical facility, benefits center, or national cemetery from being recovered as soon as possible after a major disruption.

The expectation is that critical IS services will continue by using strategies for continuing operations, including coordinating with continuity site personnel, processing data from remote locations, using cached data, transferring backups to another facility, and employing full-service restoration after the disruption by utilizing the recovery teams identified in this plan.

The DRP addresses all critical IS services as identified in the ISCPs. Facilities that are co-located or share infrastructure with other administrations should seek to ensure alignment with the continuity planning efforts developed for the other administrative or business units located in the facility.

## Enter your organization DRP Considerations here.

## DRP Roles and Responsibilities

Roles and responsibilities are provided by AWS personnel and inherited from FedRAMP package #: F1603047866. The following table includes responsibilities that describe each role and identifies the individual or team responsible for executing or supporting system recovery.

| DRP Role | Job Title | Responsibilities |
| --- | --- | --- |
| **DRP Director** | **Director, Business Continuity Management** | * Overall responsibility for the development, execution, maintenance, activation, and deactivation of the DRP * Authorizes all changes to the DRP * Determines if manual or secondary processing should be initiated as a temporary method of maintaining business operations * Ensures that an alternate DRP Director is designated |
| **DRP Director (Alternate)** | **Business Continuity IT Specialist** | * Acts on behalf of the DRP Director should the need arise |
| **DRP Coordinator** | **Program Director** | * Monitors recovery team activities until the systems are recovered at the recovery site * Ensures that recovery operations are being performed consistent with service level agreements / service level requirements * Provides periodic status updates to the DRP Director * Files an after action report (AAR) upon resumption of normal operations |
| **DRP Coordinator (Alternate)** | **Deputy Project Manager** | * Acts on behalf of the DRP Coordinator should the need arise |
| Cybersecurity Engineering Team | Cybersecurity Team | * Provides cybersecurity oversight during DRP activities |
| **VA POC** | Infrastructure Manager | * Represents the recovery and restoration interests of the affected Service/Business line |
| **VA POC (Alternate)** | Technical Architect | * Represents the recovery and restoration interests of the affected Service/Business line |
| IS Services POC (Alternate) | Manager, Cloud  Infrastructure | * Represents the recovery and restoration interests of the affected service/business line |
| Disaster Recovery Activation Team | Disaster Recovery Activation Team includes the following groups:   * Cognosante * AWS * Other Affiliated and/or Personnel as needed * VA   MAG (TBD - if connected) | * Determines the expected duration of the failover to the recovery site * Prioritizes the sequence of resource recovery * Performs all system recovery and resumption activities * Powers on / off systems * May retrieve backup tapes * Configures systems * Ensures voice and data communications are functioning: activate pagers, sat phones * Provides IP numbers and network routing information * Includes validation testing teams or personnel * Responsible for coordinating recovery activities between each site’s teams |

Table 4: Roles and Responsibilities

## Enter your organization DRP Roles and Responsibilities in the table below.

Roles and responsibilities are provided by [Organization 2 name/acronym] personnel and inherited from FedRAMP package #: F1603047866. The following table includes responsibilities that describe each role and identifies the individual or team responsible for executing or supporting system recovery.

| DRP Role | Job Title | Responsibilities |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Table 4: Roles and Responsibilities [Organization 2 name/acronym]

## 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 AWSare shown in Tables 5 and 6.

| Threat | Likelihood | Capacity | Threat Rating |
| --- | --- | --- | --- |
| Unpatched operating systems create a potential threat to the system | Low | Low | Low |
| Network misconfigurations create a potential threat to the system | Low | Low | Low |

Table 5: VAEC AWS Threat Assessment

Enter your Organization Threat Assessment here

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

Table 5: [Organization 2 name/acronym] Threat Assessment

| IS Service | Threat | Vulnerability | Exploit Potential | Mitigation Effectiveness | Mitigation Strength |
| --- | --- | --- | --- | --- | --- |
| System Administration | Unpatched operating systems create a potential threat to the system | Operating Systems Required Patch Service Updates | Low | High | High |
| System Administration | Network misconfigurations create a potential threat to the system | Network daemons not managed by the package system | Low | High | High |

Table 6: VAEC AWS Vulnerability Assessment

Enter your Organization Vulnerability Assessment here

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

Table 6: [Organization 2 name/acronym] Vulnerability Assessment

# 2. CONCEPT OF OPERATIONS

The Concept of Operations section provides an overview of the VAEC AWS DRP activation and notification, recovery and, reconstitution phases, and supporting roles and responsibilities of VAEC AWS personnel during disaster activation.

The AWS is responsible for backup and recovery of data needed to restore operations to the requisite sites. VAEC inherits these responsibilities from AWS’s FedRAMP package #: F1603047866.

Disaster recovery (DR) is the function of 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 such as 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 with the program’s 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) 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.

# Enter your organization concept of operations here.



## 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 DRP Activation and Notification Phase defines the activities required to activate the DRP and notify supporting recovery personnel. These phases include preparing for deployment of support personnel to the specified recovery site or coordinating activities between the primary site and the site where data or operations will be temporarily processed. The following sub sections further describe the activation and notification activities for sites that will transfer data or processing to another facility or implement a full mobilization.

# Enter your organization activation and notification here.

### DRP Activation Criteria and Procedures

The VAEC AWS DRP may be activated if one or more of these criteria are met:

* The VAEC AWS facility is rendered unusable;
* Any or all of the critical IS Services residing within the facility will not be available within the accepted recovery time objective (RTO) set forth in the individual ISCPs.

Additionally, the decision to activate the VAEC AWS DRP may require the DRP director to consult with the service/business Line POC’s listed in Appendix A.

# Enter your organization DRP activation criteria and procedure here.

### Notification Procedures

The first step after activation of the VAEC AWS DRP is the notification of key personnel, stakeholders and IS Service(s) recovery support teams. This includes teams whose operations will be transferred to the recovery facility. However, this may be accomplished by notifying the Regional Operations Center who will coordinate and carry out notifications.

Notification procedures may include:

* Identification of who makes the initial notifications
* The sequence in which personnel are notified (e.g., system owner, technical POC, contingency plan coordinator, business/service line 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.

# Enter your organization notification procedure here

For a full list of all DRP 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 DRP activation, refer to Appendix B.

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.

### Accountability of OIT Recovery Personnel

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

In the event of a natural or man-made disaster, DoD directives stipulate that all agencies achieve 100% personnel accountability. Normally, personnel accountability begins with the activation of your Directorate phone trees/recall roster. Additionally, the Veterans Administration has employed a mass notification system referred to as the VA-Personnel Accountability System (VA-PAS). VA-PAS is a bidirectional mass alert system that provides proactive assessment of personnel status and safety following any emergency, and maintaining communications while incidents are resolved.

# Enter your organization accountability of OIT recovery personnel here.

## Recovery Site(s)

The AWS is responsible for recovery of data needed to restore operations to the requisite sites. VAEC inherits recovery from AWS Package #: F1603047866. VAEC documents recovery and reconstitution procedures for IS services in the VAEC ISCP. This information is in Appendix F.

# Enter your organization recovery site(s) here.

3. RECOVERY

The recovery phase provides formal recovery operations that begin after the DRP has been activated, outage assessments have been completed (if possible), personnel have been notified, and in some situations, appropriate teams have been mobilized.

Recovery Phase activities focus on implementing recovery strategies to restore the site / facilities IS Services and data capabilities at a recovery facility. At the completion of the recovery phase, VAEC AWS and [Organization 2 name/acronym] IS Services and data capabilities will be operational at the recovery site and capable of performing the functions identified in the plan. These functions will continue until IS Services and components are restored, repair of damage is completed, and the operational capabilities at the original or new permanent location are resumed.



## Sequence of Recovery Activities

High-level activities that occur during the recovery of VAEC AWS’s and [Organization 2 name/acronym] ‘s systems, data and operations are identified in their associated ISCPs listed in Appendix G.

## 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 points of contact should be alerted.

# 4. RECONSTITUTION.

Reconstitution is the process by which a facility is tested to validate that all its system capabilities and functionalities are fully restored and operational. During the Reconstitution phase, recovery activities are completed and normal systems operations are resumed, and operations are transitioned back to the primary site (if needed). If the original facility is “unrecoverable”, the activities in this phase can be applied to preparing the recovery site as a new permanent location to support system processing requirements.

The AWS is responsible for reconstitution of data needed to restore operations to the requisite sites. VAEC inherits recovery from AWS Package #: F1603047866. VAEC documents recovery and reconstitution procedures for IS services in the VAEC ISCP.

Enter your Organization reconstitution here.



## Concurrent Processing – IS Services

In concurrent processing, an IS Service operates at two separate locations concurrently until there is a level of assurance that the recovered system is operating correctly. Please refer to the individual ISCPs for details regarding concurrent processing strategies for each IS Service resident within VAEC AWS. For a list of associated plans, see Appendix G.

Enter your Organization concurrent processing IS services here.

## Data Validation and Functionality Testing

Data validation and functionality testing is the process of validating recovered data, data files or databases and testing to confirm that functionality have been recovered completely. Please refer to the individual ISCPs for details for each IS Service resident within VAEC AWS.

Enter your Organization data validation and functionality testing here.

For a list of associated plans, see Appendix G.

## Reconstitution Declaration

Upon successfully completing testing and validation, the DRP director will formally declare recovery efforts complete. The DRP director will notify facility leadership, business / service line and technical POCs of the declaration.

## Notifications (Users)

Upon return to normal system operations, VAEC AWS users will be notified by DRP Director using predetermined notification procedures (e.g., VA-PAS, email, broadcast message, phone calls, etc.).

Enter your Organization notifications(Users) here.

## 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. Please refer to the individual ISCPs for details for each IS Service resident within VAEC AWS.

Enter your Organization cleanup here

For a list of associated plans, see Appendix G.

## 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). The offsite data storage procedures should be followed to return backup and installation media. Refer to Appendix D.

## 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.

## Event Documentation

It is important that all recovery events throughout the transition of operations to the continuity site and back to the primary site, be well documented and lessons learned for inclusion and update to the DRP. 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 DRP 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 DRP director or designee will formally deactivate the DRP recovery efforts. Notification of this declaration will be provided to all business and technical POCs.

# 5. TEST, TRAINING AND EXERCISE

The AWS is responsible for reconstitution of data needed to restore operations to the requisite sites. VAEC inherits recovery from AWS Package #: F1603047866. VAEC documents recovery and reconstitution procedures for IS services in the VAEC ISCP.

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

NOTE: Full functional tests of systems are normally 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.

A formal test plan is developed prior to the tabletop or functional test and exercise. Functional test procedures are developed to include key sections of the DRP, 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 AAR, and lessons learned are developed for updating information in the DRP.

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

* Ensure that VAEC AWS’s personnel are familiar with the DRP and its associated activation, recovery and reconstitution procedures.
* Validate DRP policies and procedures.
* Exercise procedures through the use of table top and functional exercises, as appropriate.
* Ensure that hardware, software, backup data, and records required to support recovery at a continuity site are available.
* Exercises should be designed for the complete loss of a facility. The exercise should be a functionality test of application and infrastructure to ensure ability to continue critical business processes meeting mission essential functions of the VA enterprise performed by the primary site.

| Activities | Tests | Training | Exercises | Frequency |
| --- | --- |
| 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 DRP’s communications. | 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 primary and backup infrastructure systems and services at alternate operating facilities, (e.g., power, water, fuel). | Annually |
| Alert, Notification, and Activation Procedures Testing for mission critical/emergency personnel. | Annually |
| 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 |
| Alternate Facility Logistics Testing and exercising of required physical security capabilities at the identified alternate facility(ies). | Annually |
| Test recovery of vital classified and unclassified records, critical information systems, services, and data. | Annually |
| Documenting and reporting testing of the internal processes for formally documenting and reporting tests and their results. | Annually |
| Test DRP’s notification/activation procedures. | 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 |
| Relocation exercise to the recovery site. | Annually |

Table 7: TT&E Calendar

Enter your Organization deactivation here

Enter test, training, and exercise (TT&E) results in the table below

| Activities | Tests | Training | Exercises | Frequency |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Table 7: TT&E Calendar [Organization 2 name/acronym]

# 6. DOCUMENT MANAGEMENT



## Document Ownership

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

Enter your Organization document ownership here

## Plan Review and Maintenance

To ensure currency, this document will be reviewed annually in conjunction with the annual DRP test / exercise and when systems at this facility incur significant modifications.

The DRP is a component of the overall VAEC Management Plan. This plan, and all related project management plans, can be found in RiskVision.

The Project Management Team will review the DRP every 365 days and as necessary to address project conditions, client input, or contract changes.

This document will be subject to formal change control after approval by the VA contracting officer. Subsequent changes to this document will be requested, approved, and implemented in accordance with the change management processes defined in the Change Management Plan. Changes to this document will be recorded in the revision history table.

The most current version of the Privacy and Security Management Plan will be posted to the VAEC instance in RiskVision.

Enter your Organization plan review and maintenance here.

## Document Distribution

A copy of the AWS DRP is in the AWS FedRAMP package #: F1603047866. A copy of the VAEC AWS 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

Enter your Organization document distribution here.

: DRP Personnel Contact Data - VA

**DRP Leadership**

| Key Personnel | Contact Information |
| --- | --- |
| **DRP Director** | Work #: 732-440-9583 |
| Name: David Catanoso | VA Cellular #: 732-440-9583 |
| Title: Director, Enterprise Cloud Solutions Office (ECSO) | VA E-mail: david.catanoso@va.gov |
| **DRP Director (Alternate)** | Work #: (202) 461-0447 |
| Name: Joseph Stevenson | VA Cellular #: |
| Title: VAEC Implementation Team Leader & COMS PM | VA E-mail: [Joseph.Stevenson@va.gov](mailto:Joseph.Stevenson@va.gov) |
| **Cybersecurity Engineering Team** | Work #: (561)291-2175 |
| Name: Joseph Fourcade | VA Cellular #: (561)291-2175 |
| Title: Cyber Security Analyst | VA E-mail: Joseph.Fourcade@va.gov |
| **Cybersecurity Engineering Team (Alternate)** | Work #: 202-491-4248 |
| Name: Michael Lucas | VA Cellular #: 202-491-4248 |
| Title: Security Manager/Information Assurance Lead | VA E-mail: michael.lucas@va.gov |
| **Cognosante Leadership** | Work #: (801) 921-3760 |
| Name: John Fisher | VA Cellular #:(801) 921-3760 |
| Title: COMS Service Delivery Lead | VA E-mail: john.fisher3@va.gov |
| **Cognosante Leadership** | Work #: 571-606-0859 |
| Name: Lee Johnson | VA Cellular #:571-606-0859 |
| Title: COMS Program Manager | VA E-mail: billy.johnson2@va.gov |
| **DRP Coordinator** | Work #: (202) 461-0447 |
| Name: Joseph Stevenson | VA Cellular #: |
| Title: VAEC Implementation Team Leader & COMS PM | VA E-mail: [Joseph.Stevenson@va.gov](mailto:Joseph.Stevenson@va.gov) |
| **DRP Coordinator (Alternate)** | Work #: 703-867-1200 |
| Name: Nagesh Gadamsetty | VA Cellular #: |
| Title: AWS Program Manager Lead | VA E-mail: Nagesh.Gadamsetty@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](mailto:Christopher.Cardella@va.gov) |
| **Alternate Outage Assessment Team POC** | Work #: (512) 326-6737 |
| Name: Eugene Tai | VA Cellular #: (512) 569-2989 |
| Title: Implementation Manager, Service Management and Planning | VA E-mail: [Eugene.Tai@va.gov](mailto:Eugene.Tai@va.gov) |

Table 8: DRP Personnel Contact Data – VA

Enter your Organization DRP Personnel Contact data here

[Organization 2 name/acronym] **DRP Leadership**

| Key Personnel | Contact Information |
| --- | --- |
| **DRP Director** | Work #: |
| Name: | VA Cellular #: |
| Title | VA E-mail: |
| **DRP Director (Alternate)** | Work #: |
| Name: | VA Cellular #: |
| Title: | VA E-mail: |
| **Cybersecurity Engineering Team** | Work #: |
| Name: | VA Cellular #: |
| Title: | VA E-mail: |
| **Cybersecurity Engineering Team (Alternate)** | Work #: |
| Name: | VA Cellular #: |
| Title: | VA E-mail: |
| Title: | VA E-mail: |
| **DRP Coordinator** | Work #: |
| Name: | VA Cellular #: |
| Title: | VA E-mail: |
| **DRP Coordinator (Alternate)** | Work #: |
| Name: | VA Cellular #: |
| Title: | VA E-mail: |
| **Outage Assessment Team POC** | Work #: |
| Name: | VA Cellular #: |
| Title: | VA E-mail: |
| **Alternate Outage Assessment Team POC** | Work #: |
| Name: | VA Cellular #: |
| Title: Implementation Manager, Service Management and Planning | VA E-mail: |

Table 8: DRP Personnel Contact Data – [Organization 2 name/acronym]

**Primary Site VAEC AWS 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 9: Primary Site VAEC AWS Key Personnel Contact Data

Enter your Organization primary site key personnel in the table below

**Primary Site** [Organization 2 name/acronym] **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 9: Primary Site [Organization 2 name/acronym] Key Personnel Contact Data

**Recovery Site VAEC AWS 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 10: Recovery Site VAEC AWS Key Personnel Contact Data

Enter your Organization recovery site key personnel in the table below

**Recovery Site** [Organization 2 name/acronym] **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 10: Recovery Site [Organization 2 name/acronym] Key Personnel Contact Data

**VAEC COMS Cyber Security** **Key Personnel**

| Key Personnel | Contact Information |
| --- | --- |
| **Team Lead** | Work #: 202-491-4248 |
| Name: Michael Lucas | VA Cellular #: 202-491-4248 |
| Title: Security Manager/Information Assurance Lead | VA E-mail: michael.lucas@va.gov |
| **Team Member** | Work #: (619) 248-1655 |
| Name: Edward Teeple | VA Cellular #: (619) 248-1655 |
| Title: Security Analyst | VA E-mail: James.Teeple@va.gov |
| **Team Member** | Work #: 703-623-2175 |
| Name: Kathleen Kerndt | VA Cellular #: 703-623-2175 |
| Title: Security Analyst | VA E-mail: ellen.kerndt@va.gov |
| **Team Member** | Work #: 443-739-3249 |
| Name: Steven Quach | VA Cellular #: 443-739-3249 |
| Title: Security Analyst | VA E-mail: steven.quach@va.gov |
| **Team Member** | Work #: 703-206-6198 |
| Name: Kristen Hill | VA Cellular #: 703-206-6198 |
| Title: Security Analyst | VA E-mail: kristen.hill3@va.gov |

Table 11: VAEC COMS Cyber Security Key Personnel Contact Data

: Call Tree



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Role** | **Telephone** | **Email** | **Priority** |
| David Catanoso | DRP Director | Work #: 732-440-9583Cell #: 732-440-9583 | [David.Catanoso @va.gov](mailto:louis.lugo@va.gov) | 1 |
| Joseph Stevenson | DRP Director (Alternate) | Work #: (202) 461-0447 Cell #: | [Joseph.Stevenson @va.gov](mailto:Chris.Cockle@va.gov) | 2 |
| Joseph Stevenson | DRP Coordinator | Work #: (202) 461-0447 Cell #: | [Joseph.Stevenson @va.gov](mailto:Chris.Cockle@va.gov) | 3 |
| Nagesh Gadamsetty | DRP Coordinator (Alternate) | Work #: 703-867-1200  Cellular #: | [Nagesh.Gadamsetty@va.gov](mailto:Nagesh.Gadamsetty@va.gov) | 4 |

Figure 2: DRP Call Tree

*1. The help desk team calls the DRP Director (or alternate), opens a communications bridge over Skype, and distributes a meeting invitation to all participants*

*2. The DRP Director calls the Program Director (or Deputy Project Manager)*

*3. The Program Director calls the ISO, the Cybersecurity Engineer, the Deputy Project Manager, the Project Coordinator, and the DRP Coordinator*

*4. The DRP Coordinator notifies all infrastructure team members as necessary*

*5. The ISO notifies the VA security team as necessary*

*6. The Program Director notifies VA program management in accordance with notification protocols and requirements*

Enter your Organization call tree in the table below

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  | 1 |
|  |  |  |  | 2 |
|  |  |  |  | 3 |
|  |  |  |  | 4 |

Figure 2: DRP Call Tree [Organization 2 name/acronym]

*1. The help desk team calls the DRP Director (or alternate), opens a communications bridge over Skype, and distributes a meeting invitation to all participants*

*2. The DRP Director calls the Program Director (or Deputy Project Manager)*

*3. The Program Director calls the ISO, the Cybersecurity Engineer, the Deputy Project Manager, the Project Coordinator, and the DRP Coordinator*

*4. The DRP Coordinator notifies all infrastructure team members as necessary*

*5. The ISO notifies the VA security team as necessary*

*6. The Program Director notifies VA program management in accordance with notification protocols and requirements*

: Personnel Contact Data – Vendors

| Vendor Contact Data | Details |
| --- | --- |
| Vendor Name | AWS GovCloud |
| Vendor Type | Cloud Service Provider |
| Address | 1915 Terry Ave. |
| City, State, and ZIP Code | Seattle, WA 98101 |
| Primary Contact Name | Jason Nixdorf |
| Office Phone Number | 704-453-6466 (mobile) |
| Emergency Phone Number | 704-453-6466 |
| Email Address | [nixdorf@amazon.com](mailto:nixdorf@amazon.com) |
| Secondary Contact Name | Jim Jennis |
| Office Phone Number | 540-247-4820 (mobile) |
| Email Address | [jhjennis@amazon.com](mailto:jhjennis@amazon.com) |
| SLA/MOU | NA |
| Special Instructions |  |

Table 12: Vendor Contact Data

Enter your organization personnel contact data in the table below

| 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 12: [Organization 2 name/acronym] Contact Data

: Alternate Storage Site

VAEC is a highly available system that automatically fails over to AWS Region 2. Addresses for these sites are not published.

| Alternate Storage Site | Details |
| --- | --- |
| City |  |
| State |  |
| Distance from Primary Facility |  |
| Is VA Owned? | No |
| POC Name |  |
| Delivery Schedule and procedures for packaging media |  |
| Procedures for retrieving media |  |
| Names and contact information of persons authorized to retrieve media |  |
| Alternate storage configuration details |  |
| Potential accessibility problems to the alternate storage site |  |
| Mitigation steps to access alternate storage site |  |
| Types of data located at alternate storage site | All - replicated |

Table 13: Alternate Storage Site

Enter your organization Alternate Storage Site in the table below

[Organization 2 name/acronym] is a highly available system that automatically fails over to alternate site. Addresses for these sites are not published.

| Alternate Storage Site | Details |
| --- | --- |
| City |  |
| State |  |
| Distance from Primary Facility |  |
| Is VA Owned? |  |
| POC Name |  |
| Delivery Schedule and procedures for packaging media |  |
| Procedures for retrieving media |  |
| Names and contact information of persons authorized to retrieve media |  |
| Alternate storage configuration details |  |
| Potential accessibility problems to the alternate storage site |  |
| Mitigation steps to access alternate storage site |  |
| Types of data located at alternate storage site |  |

Table 13: Alternate Storage Site [Organization 2 name/acronym]

: Telecommunications

| Type of Information Needed | Telecommunications Details |
| --- | --- |
| Name and contact information of carrier |  |
| Geographic locations of vendor facilities |  |
| Contracted capacity |  |
| SLA or other agreements for implementation |  |
| Information on vendor contingency plans |  |
| Names and contact information for those authorized to implement/use capacity |  |

Table 14: Telecommunications

Data telecommunication services are inherited from the AWS GovCloud FedRAMP Package #: F1603047866.

Enter your Organization telecommunication details below

| Type of Information Needed | Telecommunications Details |
| --- | --- |
| Name and contact information of carrier |  |
| Geographic locations of vendor facilities |  |
| Contracted capacity |  |
| SLA or other agreements for implementation |  |
| Information on vendor contingency plans |  |
| Names and contact information for those authorized to implement/use capacity |  |

Table 14: Telecommunications [Organization 2 name/acronym]

: 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. These site recovery services are inherited from the AWS GovCloud FedRAMP Package #: F1603047866.

| Recovery Site | Details |
| --- | --- |
| City | AWS GovCloud |
| State |  |
| Distance from primary facility |  |
| Is VA Owned? | No |
| POC Name |  |
| Procedures for accessing and using the recovery site |  |
| Names and contact information for those authorized to go to recovery site |  |
| Type of recovery site, and equipment available at site | Hot 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 | Refer to the AWS FedRAMP Package #: F1603047866 |

Table 15: Recovery Site

Enter your Organization recovery site in the table below

| Recovery Site | Details |
| --- | --- |
| City |  |
| State |  |
| Distance from primary facility |  |
| Is VA Owned? |  |
| POC Name |  |
| Procedures for accessing and using the recovery site |  |
| Names and contact information for those authorized to go to 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 15: Recovery Site [Organization 2 name/acronym]

: Associated Plans

| ISCP or Other  (Full Name) | Version # | Location  (URL if Web-Based) | POC Title |
| --- | --- | --- | --- |
| AWS FedRAMP Package #: F1603047866 |  |  |  |
| VAEC AWS GovCloud High ISCP | 1.2 | RiskVision | Charles Solomon-Jackson (ISO) |
| System Security Plan |  | RiskVision | ISO |
| Risk Assessment |  | RiskVision | ISO |
| Configuration Management Plan |  | RiskVision | ISO |
| Incident Response Plan |  | RiskVision | ISO |
| Information Security Contingency Plan |  | RiskVision | ISO |
| Disaster Recovery Plan |  | RiskVision | ISO |
| Privacy Impact Assessment |  | RiskVision | ISO |

Table 16: Associated Plans

Enter your Organization associated plans in the table below

| ISCP or Other  (Full Name) | Version # | Location  (URL if Web-Based) | POC Title |
| --- | --- | --- | --- |
|  |  |  |  |
| [Organization 2 name/acronym] [GRC Boundary Alignment] [Security Categorization] ISCP |  |  |  |
| System Security Plan |  |  |  |
| Risk Assessment |  |  |  |
| Configuration Management Plan |  |  |  |
| Incident Response Plan |  |  |  |
| Information Security Contingency Plan |  |  |  |
| Disaster Recovery Plan |  |  |  |
| Privacy Impact Assessment |  |  |  |

Table 16: Associated Plans [Organization 2 name/acronym]

| IS Services [Application/IS Support Services] | Recovery Priority |
| --- | --- |
| Authentication Services | 1 |
| Server Configuration Management Service | 2 |
| Vulnerability Scanning Service | 3 |
| Monitoring Service | 4 |
| JumpBox Service | 5 |
| Auditing Service | 6 |
| Code Configuration and Release Management Services | 7 |

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

All hardware, network, and physical infrastructure are the responsibility of AWS and are outside of the scope of this document. Recovery priorities are determined based on the criticality to the solution, as well as the number of users impacted and risk for interruption to normal business processes. Detailed processes are provided in the VAEC System High Availability and Recovery Plan.

Enter your Organization IS Services [Application/IS Support Services] Recovery Priority Ranking in the table below

| IS Services [Application/IS Support Services] | Recovery Priority |
| --- | --- |
| Authentication Services | 1 |
| Server Configuration Management Service | 2 |
| Vulnerability Scanning Service | 3 |
| Monitoring Service | 4 |
| JumpBox Service | 5 |
| Auditing Service | 6 |
| Code Configuration and Release Management Services | 7 |

Table 17: IS Services [Application/IS Support Services] Recovery Priority Ranking [Organization 2 name/acronym]

: 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 daAWSe 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.

: DRP Acronym List

Enter additional acronym used

| Term / Abbreviation | Description |
| --- | --- |
| AAR | After Action Report |
| BIA | Business Impact Assessment |
| CBP | Critical Business Process |
| DHS | Department of Homeland Security |
| DRP | Disaster Recovery Plan |
| FEMA | Federal Emergency Management Administration |
| HSEEP | Homeland Security Exercise and Evaluation Program |
| 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 |
| POC | Point of Contact |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| SLA | Service Level Agreement |
| SOP | Standard Operating Procedure |
| SP | Special Publication |
| SSP | System Security Plan |
| TT&E | Test, Training, and Exercise |
| VA | Department of Veterans Affairs |

Table 18: Acronym List

**This Page Intentionally Left Blank**