Vets.gov Disaster Recovery Plan
Version 1.2

DECEMBER 5,2019

Table of Contents

List of Tables

Document Change Control Record

Version	Release Date	Summary Of Changes	Author
1.0	August 21, 2017	Baseline	Brian Heckethorn
1.1	September 26,2018	Updated the DRP Distribution List, and made other minor changes and to standardize formatting.	Brian Gryth
1.2	January 3 2020	Updated IRP POCs and some minor updates	Faith Owusu-Sekyere

Table 1: Document Change Control

Disaster Recovery Plan (DRP) Approval

As the designated authority for Vets.gov, I hereby certify that the Vets.gov 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 Vets.gov, and that the recovery strategies identified will provide the ability to recover Vets.gov 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 Vets.gov will be tested at least annually. This plan was last tested on January 3, 2020. 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.

Christopher M. Johnston
1593443
2020.01.14 17:16:05
-05'00'

Christopher Johnston
System Owner

Griselda
Gallegos 204736

Digitally signed by Griselda Gallegos 204736
Date: 2020.01.15 14:09:41 -06'00'

Griselda Gallegos
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	Title
N/A	**On Duty Pager**
Patrick Bateman	**DSVA Lead**
Wyatt Walter	**DevOps Lead**
Rachel Rouche	**Product Manager**
Chris Johnston	**System Owner**
Rita Grewal	**Privacy Officer**
Griselda Gallegos	**ISSO**

Table 2: DRP Distribution List

1. INTRODUCTION

Information Systems (IS) are vital to the Department of Veterans Affairs (VA) business processes. This disaster recovery plan (DRP) for Vets.gov 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. 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, Federal Executive Branch National Continuity Program and Requirements, October 2012
- DHS, National Response Framework, May 2013
- DHS, Homeland Security Exercise and Evaluation Program (HSEEP), April 2013
- Homeland Security Council, National Continuity Policy Implementation Plan, August 2007
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, *Contingency Planning Guide for Information Technology Systems*, May 2010
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, January 2014
- NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, September 2006
- VA Handbook 6500.8, Information Technology Contingency Planning, April 2011
- OI&T Comprehensive Emergency Management Homeland Security Test, Training & Exercise Program Strategy (Draft), January 2010

1.1 Objective

The purpose of the Vets.gov 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.

1.2 Scope

The Vets.gov 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 at Amazon Web Services (AWS) GovCloud - Oregon. 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 level 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.

Vets.gov is maintained and operated in AWS GovCloud; an isolated AWS region designed to host sensitive data and regulated workloads in the cloud. AWS GovCloud supports their customers with U.S. government compliance requirements to include the Federal Risk and Authorization Management Program (FedRAMP).

AWS GovCloud (US) currently maintains the requirements necessary for the Federal Risk and Authorization Management Program (FedRAMP) Medium baseline applications hosted.

1.3 DRP Assumptions and Constraints

The following assumptions were used when developing this DRP:

- Vets.gov is hosted on Amazon Web Services (AWS) GovCloud and inherits features from this infrastructure. Please see VA AWS GovCloud ATO/FedRamp documentation for AWS.
- Vets.gov implements best practices described in the Amazon Web Services Well-Architected Framework Document (http://d0.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf).

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.

1.4 DRP Considerations

The Vets.gov DRP takes into consideration the existing capabilities of the recovery site location(s) and documents them along with any associated limitations or restrictions that would affect a data center, medical facility, benefits center, or national cemetery's data and access from being recovered as soon as possible after a major disruption. For "cold" or "warm" sites requiring setup of equipment or infrastructure to support operations, the DRP must include any activities necessary to prepare the continuity site to support the systems or data relocated or electronically transferred to it.

The expectation is that critical IS Services will continue by using previously demonstrated strategies for continuing operations, which include: coordinating with continuity site personnel; processing data from remote locations; using cached data; transferring of backups to another facility; and full service restoration after the disruption by utilizing the recovery teams identified in this plan.

The DRP will address 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.

2. ALTERNATIVE STORAGE SITE

2.1 Alternate Storage Site

- Vets.gov utilizes cloud computing infrastructure capabilities to leverage established redundant storage sites within Amazon Web Services (AWS) GovCloud for the storage and recovery of information.

- System data backups are made daily and are stored in multiple AWS GovCloud availability zones (AZ), which are distinct locations that are engineered to be insulated from failures in other availability zones.

- Each AWS GovCloud AZ maintains the same security safeguards, ensuring they are equivalent across sites.

    - The Vets.gov team does NOT interact with any physical infrastructure.

- Application code and deployment setup scripts are stored in the Vets.gov GitHub repository which also provides redundant storage.

2.2 Separate Alternate Storage Sites

- All Vets.gov production services are always running in multiple AWS GovCloud AZ's, which are distinct locations that are engineered to be insulated from failures in other AZ's.

- AWS GovCloud AZ's are physically distinct data centers serviced by different electrical and cooling suppliers to reduce susceptibility to the same threats.

2.3 Accessibility to Alternate Storage Sites

- Vets.gov utilizes AWS GovCloud infrastructure capabilities to leverage established redundant storage sites.

- The Vets.gov team does not interact with any physical infrastructure.

3. Alternate Processing Site

3.1 Alternate Processing Site

- Vets.gov utilizes cloud computing infrastructure capabilities to leverage established redundant storage sites within AWS GovCloud for the storage and recovery of information.

- System processing is executed in multiple AWS GovCloud AZ's, which are distinct locations that are engineered to be insulated from failures in other AZ's.

- Each AWS GovCloud availability zone maintains the same security safeguards, ensuring they are equivalent across sites.

    - The Vets.gov team does not interact with any physical infrastructure.

- Application code and deployment setup scrips are stored in GitHub which also provides redundant storage.

3.2 Separate Alternate Processing Site

- All Vets.gov production services are always running in multiple AWS GovCloud availability zones, which are distinct locations that are engineered to be insulated from failures in other availability zones.

- AWS GovCloud availability zones are physically distinct data centers serviced by different electrical and cooling suppliers to reduce susceptibility to the same threats.

3.3 Accessibility to Alternate Processing Site

- Vets.gov utilizes AWS GovCloud infrastructure capabilities to leverage established redundant processing sites.
- As a cloud service provider, AWS entirely virtualizes the region.
    - The Vets.gov team does not interact with any physical infrastructure

3.4 Priority-of-Service Provisions

- Vets.gov utilizes AWS GovCloud, which is a commercial cloud service provider that provides unlimited scalability across multiple availability zones.
- The AWS GovCloud SLA specifies a 99.95% availability guarantee, which is equivalent to the Vets.gov availability requirements.

.

4. INFORMATION SYSTEM BACKUP

4.1 Information System Backup

- Backups of system-level information stored in databases are taken every night from Amazon Relational Database Service (RDS) instances and are stored across multiple data centers to ensure redundancy.
- System-level information is maintained in CloudFormation and Ansible scripts which are stored in the Vets.gov DevOps GitHub repository.
- Information system documentation, including security documentation, are stored in the Vets.gov DevOps GitHub repository.
- Backup information maintained in AWS is not publicly hosted and only available to Vets.gov team members. All users are required to have multi-factor authentication on their accounts.
- Backup information maintained in GitHub is in private repositories only available to approved members of the Vets.gov team. All users are required to have multi-factor authentication on their accounts.

4.2 Backup Integrity

- Vets.gov will test information backups on an annual basis to verify the process of restoring data to Vets.gov.
- As a cloud service provider, AWS entirely virtualizes the region.
    - The Vets.gov team does not interact with any physical infrastructure. Media reliability, therefore, is abstracted by AWS.

5. INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

- Vets.gov will provide, through the utilization of fault-tolerant systems architecture via AWS, for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.
- AWS employs the concept of availability zones (AZs). These zones are physically separate area within the Vets.gov enclave that allows for application load balancing but prevents application loss in the event that one location is render unusable.

Appendix A: 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 B: DRP Acronym List

Term / Abbreviation	Description
AAR	After Action Report
BIA	Business Impact Assessment
CBP	Critical Business Process
CUI	Clinician User Interface
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 3: Acronym List

This Page Intentionally Left Blank