

|  |
| --- |
| Office of  information  security |
| (System Acronym) Information System Contingency Plan  Security Categorization: |
| {DATE} |

DOCUMENT CHANGE CONTROL RECORD

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION | RELEASE DATE | SUMMARY OF CHANGES | NAME |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contingency Plan Approval

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

I further attest that this ISCP for **system acronym** will be tested at least annually. This plan was last tested on **last date tested.** The test, training and exercise material associated with this test are found in the VA plan repository. This document is 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/

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

<Name>

<Job Title>

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

<Name>

<Job Title>

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

<Name>

<Job Title>

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

<Name>

<Job Title>

ISCP Plan Distribution

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

|  |  |
| --- | --- |
| NAME | TITLE |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Table of Contents

[1 INTRODUCTION 1](#_Toc365614739)

[1.1 Background 2](#_Toc365614740)

[1.2 Critical Exposure Report of IS Services 3](#_Toc365614741)

[1.3 Scope 3](#_Toc365614742)

[1.4 Assumptions 4](#_Toc365614743)

[1.5 Threats and Vulnerabilities 4](#_Toc365614744)

[2 CONCEPT OF OPERATIONS 1](#_Toc365614745)

[2.1 System Description 1](#_Toc365614746)

[2.2 Overview of ISCP Phases 3](#_Toc365614747)

[2.4 Roles and Responsibilities 4](#_Toc365614748)

[3 ACTIVATION AND NOTIFICATION 6](#_Toc365614749)

[3.1 Activation Criteria and Procedures 6](#_Toc365614750)

[3.2 Notification Procedures 6](#_Toc365614751)

[3.4 Outage Assessment 7](#_Toc365614752)

[4 RECOVERY 8](#_Toc365614753)

[4.1 Sequence of Recovery Activities 8](#_Toc365614754)

[4.2 Escalation Notices/Awareness 8](#_Toc365614755)

[5 RECONSTITUTION 9](#_Toc365614756)

[5.1 Concurrent Processing 9](#_Toc365614757)

[5.2 Data Validation and Functionality Testing 9](#_Toc365614758)

[5.3 Reconstitution Declaration 9](#_Toc365614759)

[5.4 Notifications (Users) 9](#_Toc365614760)

[5.5 Cleanup 9](#_Toc365614761)

[5.6 Offsite Data Storage 9](#_Toc365614762)

[5.7 Data Backup 9](#_Toc365614763)

[5.8 Event Documentation 10](#_Toc365614764)

[5.9 Deactivation 10](#_Toc365614765)

[6 TEST, TRAINING AND EXERCISE 11](#_Toc365614766)

[7 DOCUMENT MANAGEMENT 13](#_Toc365614767)

[7.1 Document Ownership 13](#_Toc365614768)

[7.2 Plan Review and Maintenance 13](#_Toc365614769)

[7.3 Document Distribution 13](#_Toc365614770)

[Appendix A : Personnel Contact Data - VA A-1](#_Toc365614771)

[Appendix B : Call Tree B-1](#_Toc365614772)

[Appendix C : Personnel Contact Data - Vendors C-1](#_Toc365614773)

[Appendix D : Recovery Site D-1](#_Toc365614774)

[Appendix E : Alternate Storage Facility E-1](#_Toc365614775)

[Appendix F : Alternate Processing Procedures F-1](#_Toc365614776)

[Appendix G : Outage Assessment Checklist G-1](#_Toc365614777)

[Appendix H : Alternate Data/Voice Telecommunications H-1](#_Toc365614778)

[Appendix I : Data Backup I-1](#_Toc365614779)

[Appendix J : Detailed Recovery Procedures J-1](#_Toc365614780)

[Appendix K : Data and Functionality Validation Testing Procedures K-1](#_Toc365614781)

[Appendix L : Concurrent Processing L-1](#_Toc365614782)

[Appendix M : Cleanup M-1](#_Toc365614783)

[Appendix N : Business Impact Analysis (BIA) N-1](#_Toc365614784)

[Appendix O : ISCP Glossary O-1](#_Toc365614785)

[Appendix P : ISCP Acronym List P-1](#_Toc365614786)

Table of Figures

Figure 1: System Diagram 5

Figure 2: Call Tree B-1

List of Tables

Table 1: Critical Exposure Report for IS SERVICE 3

Table 2: Contingency Planning Controls Addressed in this ISCP 4

Table 3: Facility Name IS Threat Assessment 5

Table 4: Facility Name IS Vulnerability Assessment 5

Table 5: IS System Components 2

Table 6: Associated Plans 2

Table 7: Information Systems That Connect with IS System name 2

Table 8: Facility Name ISCP Roles and Responsibilities (Primary and Alternate) 5

Table 9: Facility Name TT&E Calendar 1

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

Table 11: ISCP Personnel Contact Data – Recovery Teams A-1

Table 12: ISCP Vendor Contact Data C-1

Table 13: Recovery Priority J-1

Table 14: Step 1 – Critical Business Process Mapping/IS Services N-1

Table 15: Step 1 – Business/Service Line Maximum Tolerable Downtime (MTD) N-1

Table 16: Step 2 – IS Service Recovery Time Objective (RTO) N-1

Table 17: Step 2 Business/Service Line MTD/RTO Gap Analysis N-2

Table 18: Acronym List P-1

In the event of an actual emergency, please

go directly to:

**SECTION 3: Activation and Notification**

# INTRODUCTION

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

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

* Federal Information Security Management Act of 2002
* Office of Management and Budget Circular A-130, Management of Federal Information Resources, Appendix III, November 2000
* Federal Continuity Directive 1, Federal Executive Branch National Continuity Program and Requirements, February 2008
* National Security Presidential Directive-51/Homeland Security
* Homeland Security Presidential Directive 20, National Continuity Policy, May 2007
* National Continuity Policy Implementation Plan, August 2007
* National Response Framework, March 22, 2008
* 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*, April 2013
* 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, October 2009
* OI&T Comprehensive Emergency Management Homeland Security Test, Training & Exercise Program Strategy (Draft), January 2010

## Background

This ***System name*** **system acronym** ISCP establishes procedures to recover **system acronym** following a disruption. The following recovery plan objectives have been established to:

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

## Critical Exposure Report of IS Services

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

Office of Information and Technology (OIT) system owners must develop ISCPs for IS services ranked high after the ISCPA. The Critical Exposure report, as shown in Table 1, is the culmination of the ISCPA process, in that it uses data and values gathered and assigned during the process to produce the IS exposure description for each IS service. This description is calculated by inserting threat, vulnerability, and business impact values into the following algorithm: **Threat x Vulnerability x Impact = Critical Exposure**. Table 1 below, shows a critical exposure report for IS Service.

| THREAT | THREAT VALUE | VULNERABILITY | VULNERABILITY RATING | IMPACT VALUE | EXPOSURE VALUE |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

Table : Critical Exposure Report for IS SERVICE

## Scope

This ISCP has been developed for ***system acronym,*** which has produced a ranking of “HIGH” after the ISCPA. Procedures in this ISCP are developed for high exposure systems and designed to assist in the recovery of System Acronym within  ***RTO*** hours at the primary site. IS Component RTOs and IS Service RTOs identified in the ISCPA are documented in this plan to assist in developing recovery strategies for the system. This plan does not address replacement or purchase of new equipment, short-term disruptions, and loss of data at the onsite facility or at the user-desktop levels.

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

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

| CONTINGENCY PLANNING CONTROLS | RELEVANT SECTION OF ISCP |
| --- | --- |
| CP-1 Policy & Procedures | 1.3, 3.1, 3.2.1, 4.2 |
| CP-2 Contingency Plan | Plan Distribution, Section 7.3 |
| CP-3 Contingency Training | Plan Approval, Section 6 |
| CP-4 Testing & Exercises | Plan Approval, 5.2, 5.3, Section 6 |
| CP-6 Alternate Storage Site | 5.7, Appendix E |
| CP-7 Alternate Processing Site | 5.7, Appendix D |
| CP-7 DR Testing Site | Not Applicable |
| CP-8 Alternate Telecomm Services | Appendix H |
| CP-9 System Backup | 1.4, 2.1.1, 4.1, 5.2, 5.8, Appendix I |
| CP-10 Recovery and Reconstitution | Section 4, Section 5, Appendix J |
| CP-11 Alternate Communications Protocols | Not Applicable |
| CP-12 Safe Mode | Not Applicable |
| CP-13 Alternate Security Mechanisms | Not Applicable |

Table : Contingency Planning Controls Addressed in this ISCP

## Assumptions

The following assumptions were used when developing this ISCP:

* ***System Acronym*** has one or more critical rated as “high” exposures identified during the ISCPA process.
* Recovery sites and offsite storage are required for High and Moderate systems, optional for Low systems, and have been established for this system as described in Appendices D and E.
* Alternate processing procedures have been established by Business/Service lines, as summarized in Appendix F. Alternate processing procedures are manual procedures that can be initiated in lieu of the application to maintain business operations during an outage.
* Current backups of the system software and data are intact and available at the offsite storage facility or facilities as described in Appendices XXX, unless a Risk-Based exception has been approved for the facility.
* The ***System Acronym*** at the ***Facility Name***is inoperable and cannot be recovered within ***RTO***hours required to allow the facility to continue to operate normally.
* IS Service component restoration priorities have been established.
* Key ***System Name*** personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the ***System Acronym*** ISCP.

This plan does not apply to the situations described below:

* Catastrophes rendering primary facilities unavailable for an indeterminate period.
* Emergency evacuation of personnel addressed by the occupant evacuation plan.
* Overall recovery of business operations. Business/Service line owners should address recovery of business operations in a separate business recovery plan.

## Threats and Vulnerabilities

The current ISCPA process uses a seven-step data gathering method designed to assist in evaluating and calculating information that helps in the determination of critical exposures to a business/service line’s Critical IS Services. Through the ISCPA, a Business Impact Analysis (BIA) for VA facilities and a summation of each site’s critical exposures to the critical IS Services are provided for both non-VA and VA sites. The ISCP planning and development process will leverage the data and analysis (specifically the threat and vulnerability assessments) previously conducted as a result of the ISCPA.

| IS THREAT | LIKELIHOOD | CAPACITY | THREAT RATING |
| --- | --- | --- | --- |
|  |  |  |  |

Table : Facility Name IS Threat Assessment

| IS THREAT | VULNERABILITY | MITIGATION STRATEGY | EXPLOIT VALUE | VULNERABILITY VALUE | MITIGATIONS |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

Table : Facility Name IS Vulnerability Assessment

# CONCEPT OF OPERATIONS

The Concept of Operations section provides details about ***System Acronym***, an overview of the three phases of the ISCP (Activation and Notification, Recovery, and Reconstitution), and a description of the roles and responsibilities for **Facility Name**’s personnel during a contingency activation.

## System Description

### System Architecture



Figure 1: System Diagram

* The system’s operating environment

Click here to enter text.

* Physical locations
* General location of users

Click here to enter text.

* Partnerships with external organizations/system

Click here to enter text.

* Special technical considerations important for recovery purposes, such as unique backup procedures.

Click here to enter text.

### IS System Inventory of Components

| APPLICATION | TYPE | DATA STORAGE | NAME | MODEL | RPO (where applicable) | RTO |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |

Table : IS System Components

### System Interconnections and Associated Plans

Associated Plans

| ISCP OR OTHER  (Full Name) | VERSION # | LOCATION  (URL if Web-Based) | POC Title |
| --- | --- | --- | --- |
|  |  |  |  |

Table : Associated Plans

\*Refer to Appendix A for POC contact information

Interconnected Systems (ISA and MOU/A)

| INFORMATION SYSTEM | INFORMATION TRANSFERRED OR SUPPORT PROVIDED | POC Title | POC’s Organization |
| --- | --- | --- | --- |
|  |  |  |  |

Table : Information Systems That Connect with IS System name

\*Refer to Appendix A for POC contact information

## Overview of ISCP Phases

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

The three ISCP phases are:

1. **Activation and Notification Phase –** Activation of the ISCP occurs after a disruption or outage that may reasonably extend beyond the RTO established for a system.

Once the ISCP is activated, system owners and users are notified of an outage and a thorough outage assessment is performed for the system. Information from the outage assessment is presented to system owners and may be used to modify recovery procedures specific to the cause of the outage.

1. **Recovery Phase –** The Recovery phase details the activities and procedures for recovery of the affected system. Activities and procedures are written at a level that an appropriately skilled technician can recover the system without intimate system knowledge. This phase includes notification and awareness escalation procedures for communication of recovery status to system owners and users.
2. **Reconstitution Phase –** The Reconstitution phase defines the actions taken to test and validate system capability and functionality. This phase consists of two major activities: validating successful recovery and deactivation of the plan. During validation, the system is tested and validated as operational prior to returning operation to its normal state. Validation procedures may include functionality or regression testing, concurrent processing, and/or data validation. The system is declared recovered and operational by system owners upon successful completion of validation testing. Deactivation includes activities to notify users of system operational status. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, and readying resources for any future recovery events.

## 

## Roles and Responsibilities

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

| ISCP ROLE | JOB TITLE | RESPONSIBILITIES |
| --- | --- | --- |
| **ISCP Director** |  | * Overall responsibility for the development, execution, and maintenance of the ISCP. * Ensures that the ISCP is developed with the cooperation of managers associated with the business processes supported by the system. * Confirms expected duration of the system disruption with the ISCP Coordinator based on the outage assessment. * Declares activation of the ISCP. * Determines if interim/secondary processing procedures activities should be initiated to maintain current business operations or if operations should be suspended until the system has been recovered. * Contacts ***organization*** officials if the situation needs to be escalated * Responsible for the testing, maintenance, and distribution of the ISCP, which may be delegated to other personnel * Authorizes all changes to the ISCP |
| **ISCP Coordinator** |  | * Monitors Recovery Team activities until the system is fully recovered * Ensures that recovery operations are being performed consistent with service level agreements/ service level requirements * Provides periodic status updates to the ISCP Director * Files an after action report (AAR) upon resumption of normal operations * Assists the ISCP Director in testing, maintenance, and distribution of the ISCP |
| **Business/Service Line POC(s)** |  | * Represent the recovery and restoration interests of affected Business/Service line. |
| **Recovery Team** |  | * Determines the expected duration of the failover to the alternate site. * Prioritizes the sequence of resource recovery * Performs all system recovery and resumption activities * Powers on/off systems * Retrieves backup tapes * Configures systems * Ensures voice and data communications are functioning, activate pagers, sat phones * Provides IP numbers and network routing information * Includes validation testing teams or personnel |
| **Alternate ISCP Director** |  | * Same responsibilities as ISCP Director * Activated when the ISCP Director is unavailable |
| **Alternate ISCP Coordinator** |  | * Same responsibilities as ISCP Coordinator * Activated when the ISCP Coordinator is unavailable |

Table : Facility Name ISCP Roles and Responsibilities (Primary and Alternate)

# ACTIVATION AND NOTIFICATION

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

## Activation Criteria and Procedures

The  ***system name*** ISCP may be activated when or more of the following criteria are met:

1. The type of outage indicates ***system acronym*** will be down for more than  ***RTO*** hours.
2. The ISCP Director determines that ***system acronym***  can be recovered on the primary site***.***

Additionally, the decision to activate the ***system acronym*** ISCP may require the ISCP Director to consult with the facility leadership. The ***system acronym*** leadership may include:

* Facility Telecommunications Manager
* Network CIO

## Notification Procedures

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

Notification procedures may include:

Identification of who makes the initial notifications;

The sequence in which personnel are notified (e.g., 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.

Call Trees are an effective means of conveying the communication sequence in which leadership, recovery personnel and facility points of contact should be alerted.

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

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

## 

## Outage Assessment

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

This outage assessment is conducted by the Outage Assessment Team. Assessment results are provided to the ISCP Coordinator to assist in the coordination of the recovery of ***system acronym***. Outage Assessment checklist is located in Appendix G.

# RECOVERY

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

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

## Sequence of Recovery Activities

The following high-level activities occur during the ***system acronym*** recovery phase:

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

## 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.

# RECONSTITUTION

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

## Concurrent Processing

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

## Data Validation and Functionality Testing

Data validation and functionality testing is the process of testing and validating recovered data, data files or databases and functionality have been recovered completely . See Appendix K.

## Reconstitution Declaration

Upon successfully completing testing and validation, the **<role Recovery Declaration Designated Authority>** will formally declare recovery efforts complete. Facility leadership, business/service line and technical POCs will be notified of the declaration by the ISCP **< Notifier Role>.**

## Notifications (Users)

Upon return to normal system operations, **<facility name>** users will be notified by **<Notifier Role>** using predetermined notification procedures (e.g., email, broadcast message, phone calls; etc.).

## Cleanup

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

## 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. See Appendix E.

## Data Backup

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

## Event Documentation

It is important that all recovery events be well documented, including actions taken and problems encountered during the recovery effort, and lessons learned for inclusion and update to the ISCP. It is the responsibility of each recovery team or person to document their actions during the recovery effort, and to provide that documentation to the ISCP Coordinator. Alternatively, one of the recovery teams may be appointed the task of tracking the events.

* 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.

## Deactivation

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

# 

# TEST, TRAINING AND EXERCISE

Persons or teams with assigned ISCP roles must be trained to respond to a contingency event affecting the  ***system name*** efficiently and correctly. VA OIT has developed a test, training and exercise (TT&E) program to support the following objectives:

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

| **ACTIVITY** | **FREQUENCY** |
| --- | --- |
| **TESTS** | |
| Test ISCP notification/activation procedures. | Quarterly |
| Test ISCP communications. | Quarterly |
| 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. | Quarterly |
| Alert, Notification, and Activation Procedures Testing for mission critical/emergency personnel. | Quarterly for HQ, annually for all others |
| Test recovery of vital classified and unclassified records, critical information systems, services, and data. | Semi-Annually |
| Test primary and backup infrastructure systems and services at alternate operating facilities (e.g., power, water, fuel) | Annually |
| Continuity Facility Logistics Testing and exercising of required physical security capabilities at the identified continuity facility(s). | Annually |
| Internal and External Interdependency Testing of internal and external interdependencies identified in the OIT CEMP plans, with respect to performance of, and other agencies’ MEFs. | Annually |
| Documenting and reporting testing of the internal processes for formally documenting and reporting tests and their results. | Annually |
| Test reporting of the formal reporting processes of test results as directed by the Office of Information Security (OIS). 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 |
| **TRAINING** | |
| CEMP Awareness/Orientation training: a high-level overview presentation of CEMP concepts for all OIT staff (both mission critical/emergency personnel and non-mission critical/emergency personnel, to include contractors). | Annually |

Table : Facility Name TT&E Calendar

# 

# DOCUMENT MANAGEMENT

## Document Ownership

The contents of this document are the responsibility of **Facility Name**, which has assigned the ISCP Director responsibility for its content, modifications, currency, distribution to stakeholders, and its presence in the VA plan repository.

## Plan Review and Maintenance

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

## Document Distribution

A copy of this ISCP will be:

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

: Personnel Contact Data - VA

**ISCP LEADERSHIP**

| KEY PERSONNEL | CONTACT INFORMATION |
| --- | --- |
| **DRP Director** | **Work #:** |
| **Name, Title** |  |
| Street Address | Pager #: |
| Room Number | **VA Cellular #:** |
| City, State, and ZIP Code | **E-mail:** |
| **DRP DIRECTOR – ALTERNATE** | **Work #:** |
| **Name, Title** |  |
| Street Address | Pager #: |
| Room Number | **VA Cellular #:** |
| City, State, and ZIP Code | **E-mail:** |
| **DRP COORDINATOR** | **Work #:** |
| **Name, Title** |  |
| Street Address | Pager #: |
| Room Number | **VA Cellular #:** |
| City, State, and ZIP Code | **E-mail:** |
| **DRP COORDINATOR – ALTERNATE** | **Work #:** |
| **Name, Title** |  |
| Street Address | Pager #: |
| Room Number | **VA Cellular #:** |
| City, State, and ZIP Code | **E-mail:** |

Table : ISCP Personnel Contact Data – VA Leadership

**PRIMARY SITE RECOVERY TEAM KEY PERSONNEL**

**RECOVERY TEAM NAME\_\_\_\_\_**

| KEY PERSONNEL | CONTACT INFORMATION |
| --- | --- |
| **ROLE** | **Work #:** |
| **Name, Title** |  |
| Street Address | Pager #: |
| Room Number | **VA Cellular #:** |
| City, State, and ZIP Code | **E-mail:** |

Table : ISCP Personnel Contact Data – Recovery Teams

: Call Tree



Figure 2: Call Tree

: Personnel Contact Data – Vendors

**VENDOR CONTACT DATA**

| Vendor Contact Data | Comments |
| --- | --- |
| **Vendor Name** |  |
| **Vendor Type** |  |
| Address |  |
| City, State, and ZIP Code |  |
| Primary Contact Name |  |
| Office Phone Number |  |
| **Emergency Phone Number** |  |
| Secondary Contact Name |  |
| Email Address |  |
| Special Instructions |  |

Table : ISCP Vendor Contact Data

: Recovery Site

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

* City and state of recovery site, and distance from primary facility;
* Whether the recovery site is owned by the organization or is a third-party site provider;
* Name and points of contact for the recovery site;
* Procedures for accessing and using the recovery site, and access security features of recovery site;
* Names and contact information for those persons authorized to go to recovery site;
* Type of recovery site, and equipment available at site;
* Recovery site configuration information (such as available power, floor space, office space, telecommunications availability, etc.);
* Any potential accessibility problems to the recovery site in the event of a widespread disruption or disaster;
* Mitigation steps to access recovery site in the event of a widespread disruption or disaster; and

SLAs or other agreements of use of recovery site, available office/support space, set up times; etc.

: Alternate Storage Facility

* City and state of alternate storage facility, and distance from primary facility;
* Whether the alternate storage facility is owned by the organization or is a third-party storage provider;
* Name and points of contact for the alternate storage facility;
* Delivery schedule and procedures for packaging media to go to alternate storage facility;
* Procedures for retrieving media from the alternate storage facility;
* Names and contact information for those persons authorized to retrieve media;
* Alternate storage configuration features that facilitate recovery operations (such as keyed or card reader access by authorized retrieval personnel);
* Any potential accessibility problems to the alternate storage site in the event of a widespread disruption or disaster;
* Mitigation steps to access alternate storage site in the event of a widespread disruption or disaster;
* Types of data located at alternate storage site, including databases, application software, OSs, and other critical information system software; and

: Alternate Processing Procedures

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

: Outage Assessment Checklist

: Alternate Data/Voice Telecommunications

* Name and contact information of alternate data/voice telecommunications carrier (AT&T, Verizon, etc.)
* Geographic locations of alternate data/voice telecommunications vendors facilities (such as central offices, switch centers, etc.);
* Contracted capacity of alternate data/voice telecommunications;
* SLAs or other agreements for implementation of alternate data/voice telecommunications capacity;
* Information on alternate data/voice telecommunications vendor contingency plans; and

Names and contact information for those persons authorized to implement or use alternate data/voice telecommunications capacity.

: Data Backup

: Detailed Recovery Procedures

| **RECOVERY PRIORITY** | **PROCEDURE NAME** | **POC TITLE** |
| --- | --- | --- |
| **1** |  |  |
| **2** |  |  |
| **3** |  |  |

Table : Recovery Priority

**Recovery Priority 1 Detailed Procedures:**

**Recovery Priority 2 Detailed Procedures:**

**Recovery Priority 3 Detailed Procedures:**

: Data Validation and Functionality Testing Procedures

: Concurrent Processing

: Cleanup

: Business Impact Analysis (BIA)

This Business Impact Analysis (BIA) was developed for VA facilities as a part of the contingency planning process for the ***system name (system acronym*). This appendix is not valid for Managed Services hosted at Non-VA facilities.**

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

The BIA is composed of the following three steps:

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

The following reports are derived from the BIA:

| BUSINESS PROCESSES DEPENDENT ON THIS SERVICE |
| --- |
|  |

Table : Step 1 – Critical Business Process Mapping/IS Services

| BUSINESS/SERVICE LINE | MTD |
| --- | --- |
|  |  |

Table : Step 1 – Business/Service Line Maximum Tolerable Downtime (MTD)

| IS SERVICE | RTO |
| --- | --- |
|  |  |

Table : Step 2 – IS Service Recovery Time Objective (RTO)

| BUSINESS/SERVICE LINE | MTD | RTO | GAP |
| --- | --- | --- | --- |
|  |  |  |  |

Table : Step 2 Business/Service Line MTD/RTO Gap Analysis

: ISCP Glossary

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

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

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

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

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

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

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

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

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

**IS Contingency Plan (ISCP)**—OMB Circular A-130, Appendix III, requires the development and maintenance of continuity of support plans for general support systems and contingency plans for major applications. Because an IT contingency plan should be developed for each major application and general support system, multiple contingency plans may be maintained within the organization’s business continuity plan**.**

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

**Contingency Plan Assessment (ISCPA) Process**—The four step process (BIA, IS Services Analysis, Threat Assessment, and Vulnerability Assessment,) that is the precursor for contingency planning within VA.

**Maximum Tolerable Downtime (MTD)** —The MTD represents the total amount of time leaders/managers are willing to accept for a business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave continuity planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail, which will be required when developing recovery procedures, including their scope and content.

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

**Recovery Time Objective (RTO)**—The maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.

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

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

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

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

: ISCP Acronym List

*Ensure all acronyms used in the document are accounted for in Table 10. Conversely, ensure all acronyms in this list are accounted for in the document text. Add acronyms not listed here, if applicable.*

| TERM/ABBREVIATION | DESCRIPTION |
| --- | --- |
| **AAR** | After Action Report |
| **BIA** | Business Impact Assessment |
| **CBP** | Critical Business Process |
| **DRP** | Disaster Recovery Plan |
| **IS** | Information System |
| **ISCP** | Information System Contingency Plan |
| **ISCPA** | Information System Contingency Planning Assessment |
| **LAN** | Local Area Network |
| **MTD** | Maximum Tolerable Downtime |
| **NIST** | National Institute of Standards and Technology |
| **OIT** | Office of Information Technology |
| **OS** | Operating System |
| **PBX** | Private Branch Exchange |
| **POC** | Point of Contact |
| **RTO** | Recovery Time Objective |
| **SOP** | Standard Operating Procedure |
| **SP** | Special Publication |
| **SSP** | System Security Plan |
| **TT&E** | Tests, Training, and Exercises |
| **VA** | Department of Veterans Affairs |

Table : Acronym List