Warnings and Notices

*This document contains sensitive information regarding system recovery procedures and should be treated as confidential. Access should be limited to authorized personnel who require this information to perform their duties. Unauthorized disclosure may compromise system security and recovery capabilities.*

# Scope and Purpose

This system recovery plan is developed for **<system name>** application service. Procedures in this system recovery plan are designed to recover this system within the RTO provided in the Recovery Section. This plan does not address replacement or purchase of new equipment, short-term disruptions lasting less than the RTO timeframe, or loss of data at the onsite facility or at the user-desktop level.

## Assumptions

The following assumptions were used when developing this system recovery plan:

* Alternate processing sites and offsite storage are required and have been established for this system.
* Current backups of the system software and data are intact and available at the offsite storage facility.
* Alternate facilities have been established and are available if needed for relocation of this system.
* The system is inoperable and cannot be recovered within the agreed upon RTO.
* Key personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the systems disaster recovery plan.
* All enterprise dependencies are assumed to be active prior to the restoration of any agency system.  This includes but is not limited to network connectivity and security systems.
* Procurement of replacement equipment is outside the scope of this system recovery plan.
* This system is backed up using the standard NDIT backup and restore infrastructure in accordance with the policies configured within the NDIT restoration system.

# System Information

## System Description

<Provide a high-level description of the system, its business purpose, and critical functions.>

Hosting Model: <Internal / Vendor-Hosted / Hybrid>

Primary Vendor: <if applicable>

## Key Contacts

Include contact information for any contacts internal or external to your organization. *(Examples have been provided in the below table, adapt as necessary for your organization.)*

| Title/Function | Primary Resource | Backup Resource | Recovery Role |
| --- | --- | --- | --- |
| Business System Owner |  |  | Execute functional test scripts to validate functionality and data availability.  Consult with IT to determine what actions to take during an incident. |
| System Administrator |  |  | Coordinate cutover to the alternate data center with other Admins. |
| Database Administrator |  |  | Coordinate cutover to the alternate data center with other Admins. |
| Network Administrator |  |  | Ensure network connectivity and security configurations. |
| Test Team |  |  | Execute validation test scripts and verify system functionality before return to service. |
| Recovery Team Lead |  |  | Coordinate overall recovery operations, resource allocation, and stakeholder communications. |
| Vendor Support |  |  | Provide technical assistance and escalation support. |

## System Components

| Hardware/Software | Description and Notes |
| --- | --- |
| Servers |  |
| Databases |  |
| Applications |  |
| Network Components |  |
| Storage Systems |  |
| Security Components |  |
| Monitoring Tools |  |

## System Documentation

Identify and note the location of any essential records, including system documentation, required to recover this service. The location should be backed up, protected, and quickly available in the event of a disaster.

| Description | Location |
| --- | --- |
| System Architecture Diagrams |  |
| Configuration Documentation |  |
| Installation Procedures |  |
| User Manuals |  |
| Vendor Contracts/SLAs |  |
| Security Configurations |  |
| Test Scripts and Procedures |  |

## System Dependencies

INBOUND: Describe the resources this system depends on to function. (Examples: applications, systems, services, people, teams, hardware, etc.)

| Dependency | Description/Notes |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

OUTBOUND: Describe the systems that depend on this system. (Examples: applications, systems, services, people, teams, hardware, etc.)

| Dependency | Description/Notes |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Recovery

## Recovery Objectives

|  |  |
| --- | --- |
| Recovery Time Objective (RTO)\* |  |
| Recovery Point Objective (RPO)\* |  |
| Recovery Time Capability |  |
| Maximum Tolerable Downtime (MTD)\* |  |
| Data Backup Frequency |  |
| Data Backup Retention |  |
| Data Replication Method |  |
| Backup Location (cloud, DC, etc.) |  |

\* See your organization’s Service Level Agreement for information on the recovery time framework.

## Recovery

| Step | Disaster Recovery Steps | Responsible Team/Role |
| --- | --- | --- |
| **ASSESSMENT PHASE** | | |
| 1. | Confirm incident scope and impact | Recovery Team Lead |
| 2. | Determine if recovery or restoration is required | System Admin |
| 3. | Verify all system components are offline before beginning recovery | System Admin |
| 4. | Notify stakeholders of recovery initiation | Business System Owner |
| **PREPARATION PHASE** | | |
| 5. | Prepare alternate site for recovery activities | Network Admin |
| 6. | Verify backup integrity and availability | Backup Admin |
| 7. | Confirm recovery team availability | Recovery Team Lead |
| **RECOVERY EXECUTION** | | |
| 8. | Restore infrastructure components (network, storage, etc.) | Network Admin |
| 9. | Restore database from backup | Database Admin |
| 10. | Restore system from backup | System Admin |
| 11. | Apply security configuration | Network Admin |
| 12. | Perform system configuration validation | System Admin |
| **TESTING AND VALIDATION** | | |
| 13. | Execute pre-defined test scripts (see Validation section) | Test Team |
| 14. | Conduct user acceptance testing | Business System Owner |
| 15. | Validate data integrity and completeness | Database Admin |
| **RETURN TO SERVICE** | | |
| 16. | Notify users of system availability | Recovery Team Lead |
| 17. | Monitor system performance | System Admin |
| 18. | Document lessons learned | Recovery Coordinator |
| **RETURN TO PRIMARY SITE** | | |
| 19. | Begin planning return to primary site | Recovery Team Lead |
| 20. | Assess primary site readiness and safety | Network Admin |
| 21. | Plan data synchronization approach | Database Admin |
| 22. | Schedule return-to-primary window | Recovery Team Lead |
| 23. | Execute return procedures | All Teams |
| 24. | Validate primary site operations | Test Team |
| 25. | Return alternate site resources to previous status (decommission as needed) | All Admins |

**ADDITIONAL NOTES:**

* Refer to system documentation for detailed recovery/restoration procedures
* Ensure all dependencies are restored before proceeding with system recovery
* Maintain communication with stakeholders throughout the recovery process

# Validation Testing Framework

## Purpose of Validation Testing

Validation testing ensures that recovered systems function correctly and meet business requirements before returning to production. These tests should verify both technical functionality and business processes.

## Test Script Development Guidelines

When creating validation test scripts, include:

1. **Pre-Recovery Baseline Tests**
   * Document expected system performance metrics
   * Capture current data states and counts
   * Record configuration checksums
2. **Post-Recovery Functional Tests** 
   * Core business process validation
   * System integration verification
   * User authentication and authorization
   * Data accessibility and integrity
3. **Performance Validation** 
   * Response time benchmarks
   * Throughput measurements
   * Resource utilization checks
4. **Security Validation** 
   * Access control verification
   * Encryption status checks
   * Security policy enforcement

## Validation Test Script Template

*Below is a sample test script to provide some examples. Remove the sample data and update to create the validation test script for this system.*

| Step | Action | Expected Result | Actual Result | Pass/Fail | Notes |
| --- | --- | --- | --- | --- | --- |
| 1. | Verify that all critical services are running | All services snow “running” status |  |  |  |
| 2. | Test user authentication with test account | User successfully logs in without errors |  |  |  |
| 3. | Verify database connectivity and responsiveness | Database queries return results within acceptable time |  |  |  |
| 4. | Execute primary business function (be specific) | Function completes successfully within normal timeframe |  |  |  |
| 5. | Test data modification (create a test record) | New record created and saved successfully |  |  |  |
| 6. | Test data retrieval (search for test record) | Test record found and displays correctly |  |  |  |

Test Execution Notes:

* Execute tests in order listed
* Stop testing if critical failures occur
* Document any anomalies in Notes column
* Get business owner sign-off before declaring system ready

# Communication Plan

For all communication procedures during system outages and recovery operations, refer to your organization's Crisis Management & Communication Plan.

The Crisis Management & Communication Plan includes:

* Stakeholder notification procedures and timelines
* Communication templates for system outages
* Internal and external notification requirements
* Media and regulatory communication protocols
* Escalation procedures for communications

System-Specific Communication Notes:

* Recovery Team Lead coordinates with Crisis Management Team for all communications
* Technical updates should be provided to the Crisis Communications Coordinator
* Do not communicate directly with external stakeholders without Crisis Management Team approval
* Document all communication activities for post-incident review

# Maintenance

## Review/Change Log

| Date | Description | Completed by |
| --- | --- | --- |
| yyyy-mm-dd |  |  |
|  |  |  |

## Testing and Exercise

| Date | Type | Outcome |
| --- | --- | --- |
| yyyy-mm-dd | DR Test or TTX | Pass/Fail/Findings/No Findings |
|  |  |  |
|  |  |  |

**Annual Review Checklist**

* Contact information updated
* System components and dependencies reviewed
* Recovery procedures tested and validated
* Test scripts updated for system changes
* Recovery time objectives reassessed
* Staff training completed
* Documentation updated

# Appendix A: Glossary

|  |  |
| --- | --- |
| RPO | Recovery Point Objective: the point in time to which data can be recovered when a disaster occurs. RPO refers to the time of the last successful data replication or backup. It focuses on data and is independent of the time it takes to get non-functional system components back on-line. |
| RTO | Recovery Time Objective: A measure of how long it takes for a system to resume operations after a disaster has been declared. |
| WRT | Work Recovery Time: The amount of time it will take to validate functionality and data availability in the system after recovery plus the time to input any backlogged information. |
| MTD | Maximum Tolerable Downtime: The total amount of time it takes to recover a system (RTO) plus the time required to validate functionality and data and catch-up on backlogged work accumulated while the system was unavailable (WRT). |
| PDC | Primary Data Center |
| SDC | Secondary Data Center |
| DC | Data Center |