**Name of Organization**

**Information Technology Disaster Recovery Plan**

**Template**

December 2021

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Instructions

The (Name of Organization) Information Technology Disaster Recovery Plan is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute this document to individuals on a need-to-know basis. Distribution by other individuals without prior authorization is prohibited. This document is unclassified but contains sensitive information.

**Table of Contents**

[I. Introduction and Purpose 6](#_Toc87942630)

[II. Scope 6](#_Toc87942631)

[III. Assumptions 6](#_Toc87942632)

[IV. Concept of Operations 7](#_Toc87942633)

[System Description 7](#_Toc87942634)

[Overview of ITDRP Phases 8](#_Toc87942635)

[Roles and Responsibilities 9](#_Toc87942636)

[V. Activation and Notification 9](#_Toc87942637)

[Activation Criteria and Procedure 9](#_Toc87942638)

[Notification 10](#_Toc87942639)

[Outage Assessment 10](#_Toc87942640)

[VI. Recovery 10](#_Toc87942641)

[Sequence of Recovery Activities 10](#_Toc87942642)

[Recovery Procedures 11](#_Toc87942643)

[Recovery Escalation Notices/Awareness 11](#_Toc87942644)

[VII. Reconstitution 11](#_Toc87942645)

[Concurrent Processing 11](#_Toc87942646)

[Validation Data Testing 12](#_Toc87942647)

[Validation Functionality Testing 12](#_Toc87942648)

[Recovery Declaration 12](#_Toc87942649)

[Notifications (Users) 12](#_Toc87942650)

[Cleanup 13](#_Toc87942651)

[Offsite Data Storage 13](#_Toc87942652)

[Data Backup 13](#_Toc87942653)

[Event Documentation 13](#_Toc87942654)

[Deactivation 14](#_Toc87942655)

[VIII. Personnel Contact List 14](#_Toc87942656)

[IX. Vendor Contact List 15](#_Toc87942657)

[X. Detailed Recovery Procedures 15](#_Toc87942658)

[XI. Alternate Processing Procedures 16](#_Toc87942659)

[XII. System Validation Test Plan 16](#_Toc87942660)

[XIII. Alternate Storage, Site, and Telecommunications 16](#_Toc87942661)

[XIV. Diagrams (System and Input/Output) 18](#_Toc87942662)

[XV. Hardware and Software Inventory 18](#_Toc87942663)

[XVI. Interconnections Table 18](#_Toc87942664)

[XVII. Test and Maintenance Schedule 19](#_Toc87942665)

[XVIII. Associated Plans and Procedures 19](#_Toc87942666)

[XIX. Business Impact Analysis 20](#_Toc87942667)

# Introduction and Purpose

Information systems are vital to Organization mission/business processes. It is critical that services provided by [System/System Name] can operate effectively without excessive interruption. This Information Technology Disaster Recovery Plan (ITDRP) document establishes a comprehensive procedure to recover [System/System Name] quickly and effectively following a service disruption.  
  
The following recovery plan objectives have been established:

* 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/System Name] operations; and
  + **Reconstitution phase** to ensure that [System/System Name] is validated through testing and that normal operations are resumed.
* Identify the activities, resources, and procedures to carry out [System/System Name] processing requirements during prolonged interruptions to normal operations.
* Assign responsibilities to designated Organizational personnel and provide guidance for recovering [System/System Name] during prolonged periods of interruption to normal operations.
* Ensure coordination with other personnel responsible for Organization contingency planning strategies. Ensure coordination with external points of contact and vendors associated with [System/System Name] and execution of this plan.

# Scope

This ITDRP has been developed for [System/System Name], which is classified as a *“high/medium/low”* impact system, in accordance with Federal Information Processing Standards (FIPS) 199 – Standards for Security Categorization of Federal Information and Information Systems. Procedures in this ITDRP are for *“high/medium/low”* impact systems and designed to recover [System/System Name] within Recovery Time Objective (RTO) expectations of XX hours. This plan does not address replacement or purchase of new equipment, short-term disruptions lasting less than RTO expectations, or loss of data at the onsite facility or at the user-desktop levels.

# Assumptions

The following assumptions were used when developing this ITDRP:

* [System/System Name] has been established as a “high/medium/low”-impact system, in accordance with FIPS 199.
* 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 in [City, State/Provider].
* Alternate facilities have been established at [City, State/Provider] and are available if needed for relocation of [System/System Name].
* The [System/System Name] is inoperable at the Organization and cannot be recovered within [RTO hours].
* Key [System/System Name] personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the [System/System Name] Disaster Recovery Plan.
* *Additional assumptions as appropriate.*

The [System/System Name] ITDRP does not apply to the following situations:

* **Overall recovery and continuity of mission/business operations.** A Business Continuity Plan (BCP) and Continuity of Operations Plan (COOP) (as applicable) address continuity of business operations, not necessarily individual systems.
* **Emergency evacuation of personnel.** An Occupant Emergency Plan (OEP) (as applicable) addresses employee evacuation.
* *Any additional constraints and associated plans should be added to this list.*

# Concept of Operations

The Concept of Operations section provides details about [System/System Name], an overview of the three phases of the ITDRP (Activation and Notification, Recovery, and Reconstitution), and a description of roles and responsibilities of Organization personnel during a Disaster Recovery activation.

## System Description

*NOTE: Information for this section should be available from the system’s System Security Plan (SSP) (if applicable) and can be copied from the SSP or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan.* ***Provide a general description of system architecture and functionality.***

*Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures.*

## Overview of ITDRP Phases

This ITDRP has been developed to recover the [System/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 system recovery phases are:

**Activation and Notification Phase** – Activation of the ITDRP occurs after a disruption or outage that may reasonably extend beyond the RTO established for a system. The outage event may result in severe damage to the facility that houses the system, severe damage or loss of equipment, or other damage that typically results in long-term loss.

Once the ITDRP is activated, system owners and users are notified of a possible long-term 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.

**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.

**Reconstitution** – The Reconstitution phase defines the actions taken to test and validate system capability and functionality at the original or new permanent location. This phase consists of two major activities: validating successful reconstitution 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 events.

## Roles and Responsibilities

The ITDRP establishes several roles for [System/System Name] recovery and reconstitution support. Persons or teams assigned ITDRP roles have been trained to respond to a contingency event affecting [System/System Name].

Describe each team and role responsible for executing or supporting system recovery and reconstitution. Include responsibilities for each team/role, leadership roles, and coordination with other recovery and reconstitution teams, as applicable. At a minimum, a role should be established for a system owner or business unit point of contact, a recovery coordinator, and a technical recovery point of contact.

Leadership roles should include an ITDRP Director, who has overall management responsibility for the plan, and an ITDRP Coordinator, who is responsible to oversee recovery and reconstitution progress, initiate any needed escalations or awareness communications, and establish coordination with other recovery and reconstitution teams as appropriate.

# Activation and Notification

The Activation and Notification Phase defines initial actions taken once a [System/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 ITDRP. At the completion of the Activation and Notification Phase, [System/System Name] ITDRP staff will be prepared to perform recovery measures.

## Activation Criteria and Procedure

The [System/System Name] ITDRP may be activated if one or more of the following criteria are met:

1. The type of outage indicates [System/System Name] will be down for more than RTO expectations
2. The facility housing [System/System Name] is damaged and may not be available within RTO expectations
3. *Other criteria, as appropriate.*

The following persons or roles may activate the ITDRP if one or more of these criteria are met:

Role/Person

Role/Person

Role/Person

Role/Person

***Establish one or more roles that may activate the plan based on activation criteria.*** *Authorized persons may include the system or business owner, or the operations point of contact (POC) for system support.*

## Notification

The first step upon activation of the [System/System Name] ITDRP is notification of appropriate business and system support personnel. Contact information for appropriate POCs is included in [Contact List Document Name].

For [System/System Name], the following method and procedure for notifications are used:

***Describe established notification procedures.*** *Notification procedures should include who makes the initial notifications, the sequence in which personnel are notified (e.g., system owner, technical POC, ITDRP Coordinator, business unit or user unit POC, and recovery team POC), and the method of notification (e.g., email blast, call tree, automated notification system, etc.).*

## Outage Assessment

Following notification, a thorough outage assessment is necessary to determine the extent of the disruption, any damage, and expected recovery time. This outage assessment is conducted by [name of recovery team]. Assessment results are provided to the ITDRP Coordinator to assist in the coordination of the recovery of [System/System Name].

***Outline detailed procedures to include how to determine the cause of the outage; identification of potential for additional disruption or damage; assessment of affected physical area(s); and determination of the physical infrastructure status, IS equipment functionality, and inventory.*** *Procedures should include notation of items that will need to be replaced and estimated time to restore service to normal operations.*

# Recovery

The Recovery Phase provides formal recovery operations that begin after the ITDRP 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, repair damage, and resume operational capabilities at the original or an alternate location. At the completion of the Recovery Phase, [System/System Name] will be functional and capable of performing the functions identified in the System Description section of this plan.

## Sequence of Recovery Activities

The following activities occur during recovery of [System/System Name]:

*Modify the following list as appropriate for the selected system recovery strategy:*

1. Identify recovery location (if not at original location)
2. Identify required resources to perform recovery procedures
3. Retrieve backup and system installation media
4. Recover hardware and operating system (if required)
5. Recover system from backup and system installation media.

## Recovery Procedures

The following procedures are provided for recovery of [System/System Name] at the original or established alternate location. Recovery procedures are outlined per team and should be executed in the sequence presented to maintain an efficient recovery effort.

***Provide general procedures for the recovery of the system from backup media.*** *Specific keystroke-level procedures may be provided in another section. If specific procedures are provided in another section, a reference to that section should be included in this section. Teams or persons responsible for each procedure should be identified.*

## Recovery Escalation Notices/Awareness

***Provide appropriate procedures for escalation notices during recovery efforts.*** *Notifications during recovery include problem escalation to leadership and status awareness to system owners and users. Teams or persons responsible for each escalation/awareness procedure should be identified.*

# Reconstitution

Reconstitution is the process by which 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. A determination must be made on whether the system has undergone significant change and will require reassessment and reauthorization. The phase consists of two major activities: validating successful reconstitution, and deactivation of the plan.

## Concurrent Processing

*“high/medium/low”-impact systems are not required to have concurrent processing as part of the validation effort. If concurrent processing does occur for the system prior to making it operational, procedures should be inserted here. Procedures should include length of time for concurrent processing, processing information on both concurrent systems, and validating information on the new permanent system.*

*For “high/medium/low”-impact systems without concurrent processing, this section may either be removed, or the following may be used:*

In concurrent processing, a system operates at two separate locations concurrently until there is a level of assurance that the recovered system is operating correctly. [System/System Name] does/does not have concurrent processing as part of validation. Once the system has been tested and validated, it will be placed into normal operations.

## Validation Data Testing

Validation data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely. The following procedures will be used to determine that the recovered data is complete and current to the last available backup:

***Provide procedures for testing or validation of recovered data to ensure that data is correct and up to date.*** *This section may be combined with the Functionality Testing section if procedures test both the functionality and data validity. Teams or persons responsible for each procedure should be identified. An example of a validation data test for a “high/medium/low”-impact system would be to log into the system database and check the audit logs to determine that all transactions and updates are current. Detailed data test procedures may be provided in System Validation Test Plan.*

## Validation Functionality Testing

Validation functionality testing is the process of verifying that [System/System Name] functionality has been tested, and the system is ready to return to normal operations.

***Provide system functionality testing and validation procedures to ensure that the system is operating correctly.*** *This section may be combined with the Data Testing section if procedures test both the functionality and data validity. Teams or persons responsible for each procedure should be identified. An example of a functional test for a “high/medium/low”-impact system may be logging into the system and running a series of operations as a test or real user to ensure that all parts of the system are operating correctly. Detailed functionality test procedures may be provided in System Validation Test Plan.*

## Recovery Declaration

Upon successfully completing testing and validation, the ITDRP Director will formally declare recovery efforts complete, and that [System/System Name] is in normal operations. [System/System Name] business and technical POCs will be notified of the declaration by the ITDRP Coordinator.

## Notifications (Users)

Upon return to normal system operations, [System/System Name] users will be notified by ITDRP Director using predetermined notification procedures (e.g., email, broadcast message, phone calls, etc.).

## Cleanup

Cleanup is the process of cleaning up or dismantling any temporary recovery locations, restocking supplies used, returning manuals or other documentation to their original locations, and readying the system for a possible future contingency event.

***Provide any specific cleanup procedures for the system, including preferred locations for manuals and documents and returning backup or installation media to its original location.***

## Offsite Data Storage

It is important that all backup and installation media used during recovery be returned to the offsite data storage location. The following procedures should be followed to return backup and installation media to its offsite data storage location.

***Provide procedures for returning retrieved backup or installation media to its offsite data storage location.*** *This may include proper logging and packaging of backup and installation media, preparing for transportation, and validating that media is securely stored at the offsite location.*

## 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. The procedures for conducting a full system backup are:

***Provide appropriate procedures for ensuring that a full system backup is conducted within a reasonable time frame, ideally at the next scheduled backup period.*** *This backup should go offsite with the other media in Offsite Data Storage section.*

## Event Documentation

It is important that all recovery events be well-documented, including actions taken and problems encountered during the recovery and reconstitution effort, and lessons learned for inclusion and update to this ITDRP. It is the responsibility of each ITDRP team or person to document their actions during the recovery and reconstitution effort, and to provide that documentation to the ITDRP Coordinator.

***Provide details about the types of information each ITDRP team member is required to provide or collect for updating the ITDRP with lessons learned.*** *Types of documentation that should be generated and collected after a contingency activation 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*
* *After Action Report.*

*Event documentation procedures should detail responsibilities for development, collection, approval, and maintenance.*

## Deactivation

Once all activities have been completed and documentation has been updated, the ITDRP Director will formally deactivate the ITDRP recovery and reconstitution effort. Notification of this declaration will be provided to all business and technical POCs.

# Personnel Contact List

***Provide contact information for each person with a role or responsibility for activation or implementation of the ITDRP, or coordination with the ITDRP.*** *For each person listed, at least one office and one non-office contact number is recommended. Note: Information may contain personally identifiable information and should be protected.*

|  |  |
| --- | --- |
| ITDRP Key Personnel | |
| Key Personnel | Contact Information |
| ITDRP Director  Name, Title | Work XXX.XXX.XXXX Mobile XXX.XXX.XXXX Email name@organization.com |
| ITDRP Director (ALTERNATE)  Name, Title | Work XXX.XXX.XXXX Mobile XXX.XXX.XXXX Email name@organization.com |
| ITDRP Coordinator  Name, Title | Work XXX.XXX.XXXX Mobile XXX.XXX.XXXX Email name@organization.com |
| ITDRP Coordinator (ALTERNATE)  Name, Title | Work XXX.XXX.XXXX Mobile XXX.XXX.XXXX Email name@organization.com |
| ROLE  Name, Title | Work XXX.XXX.XXXX Mobile XXX.XXX.XXXX Email name@organization.com |

# Vendor Contact List

*Contact information for all key maintenance or support vendors should be included here. Contact information, such as emergency phone numbers, contact names, contract numbers, and contractual response and onsite times should be included.*

|  |  |
| --- | --- |
| ITDRP Vendor Contacts | |
| Vendor Name | Contact Information |
| Vendor Name  Description/Purpose  Primary Contact Name, Title | Work XXX.XXX.XXXX Mobile XXX.XXX.XXXX Email name@organization.com |
| Vendor Name  Description/Purpose  Primary Contact Name, Title | Work XXX.XXX.XXXX Mobile XXX.XXX.XXXX Email name@organization.com |
| Vendor Name  Description/Purpose  Primary Contact Name, Title | Work XXX.XXX.XXXX Mobile XXX.XXX.XXXX Email name@organization.com |
| Vendor Name  Description/Purpose  Primary Contact Name, Title | Work XXX.XXX.XXXX Mobile XXX.XXX.XXXX Email name@organization.com |

# Detailed Recovery Procedures

*Provide detailed recovery procedures for the system, which may include items such as:*

* *Keystroke-level recovery steps*
* *System installation instructions from tape, CD, or other media*
* *Required configuration settings or changes*
* *Recovery of data from tape and audit logs*
* *Other system recovery procedures, as appropriate*

*If the system relies totally on another group or system for its recovery and reconstitution (such as a mainframe system), information provided should include contact information and locations of detailed recovery and reconstitution procedures for that supporting system.*

# Alternate Processing Procedures

*This section should identify any alternate manual or technical processing procedures available that allow the business unit to continue some processing of information that would normally be done by the affected system. Examples of alternate processes include manual forms processing, input into workstations to store data until it can be uploaded and processed or queuing of data input.*

# System Validation Test Plan

*This section includes system acceptance procedures that are performed after the system has been recovered and prior to putting the system into full operation and returned to users. The system validation test plan may include the regression or functionality testing conducted prior to implementation of a system upgrade or change.*

Once [System/System Name] has been recovered, the following steps will be performed to validate system data and functionality:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Procedure | Expected Results | | Actual Results | | Status | Initials |
|  | |  |  |  | |  |
|  | |  |  |  | |  |
|  | |  |  |  | |  |
|  | |  |  |  | |  |

# Alternate Storage, Site, and Telecommunications

This section provides information for alternate storage, alternate processing site, and alternate telecommunications for the system. Alternate storage, site, and telecommunications information are strongly encouraged for “high/medium/low”-impact systems. Information that should be provided for each area includes:

**Alternate Storage:**

* 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, operating systems, and other critical information system software
* Other information as appropriate

**Alternate Processing Site:**

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

**Alternate Telecommunications:**

* Name and contact information of alternate telecommunications vendors
* Geographic locations of alternate telecommunications vendors facilities (such as central offices, switch centers, etc.)
* Contracted capacity of alternate telecommunications
* SLAs or other agreements for implementation of alternate telecommunications capacity
* Information on alternate telecommunications vendor contingency plans
* Names and contact information for those persons authorized to implement or use alternate telecommunications capacity
* Other information as appropriate

# Diagrams (System and Input/Output)

*NOTE: Information for this section should be available from the system’s System Security Plan (SSP) (if applicable) and can be copied from the SSP or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. Include any system architecture, input/output, or other technical or logical diagrams that may be useful in recovering the system. Diagrams may also identify information about interconnection with other systems.*

# Hardware and Software Inventory

*Provide or reference the hardware and software inventory for the system. Inventory information should include type of server or hardware on which the system runs, processors and memory requirements, storage requirements, and any other pertinent details. The software inventory should identify the operating system (including service pack or version levels, and any other applications necessary to operate the system, such as database software).*

# Interconnections Table

*NOTE: Information for this section should be available from the system’s System Security Plan (SSP) (if applicable) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. This section includes information on other systems that directly interconnect or exchange information with the system. Interconnection information should include the type of connection, information transferred, and contact person for that system.*

*If the system does not have any direct interconnections, then this section may be removed, or the following statement may be used:*

[System/System Name] does not directly interconnect with any other systems.

# Test and Maintenance Schedule

*All ITDRPs should be reviewed and tested at the Organization-defined frequency (e.g., annually) or whenever there is a significant change to the system. Provide information and a schedule for the testing of the system. The full functional test should include all ITDRP points of contact and be facilitated by an outside or impartial observer. A formal test plan is developed prior to the functional test, and test procedures are developed to include key sections of the ITDRP, including the following:*

* *Notification procedures*
* *System recovery on an alternate platform from backup media*
* *Internal and external connectivity*
* *Reconstitution procedures*

*Results of the test are documented in an After-Action Report, and Lessons Learned are developed for updating information in the ITDRP.*

*NOTE: Full functional tests of systems normally are 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.*

*Examples of functional tests that may be performed prior to a full functional test include:*

* *Full notification and response of key personnel to recovery location*
* *Recovery of a server or database from backup media*
* *Setup and processing from a server at an alternate location*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Process Step | Responsible Party | | Due | | Scheduled | Performed | Status |
|  | |  | MM/DD/YYY | MM/DD/YYY | | MM/DD/YYY |  |
|  | |  |  |  | |  |  |
|  | |  |  |  | |  |  |
|  | |  |  |  | |  |  |

# Associated Plans and Procedures

NOTE: Information for this section should be available from the system’s System Security Plan (SSP) (if applicable) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. ITDRPs for other systems that either interconnect or support the system should be identified in this appendix. The most current version of the ITDRP, location of ITDRP, and primary point of contact (such as the ITDRP Coordinator) should be noted.

# Business Impact Analysis

*Include or reference current/recent Business Impact Analysis (BIA) results.*