IT DISASTER RECOVERY PLAN

<<Name of School/Department>>

Rev. **<< Revision Number >>**

DOCUMENT CHANGE CONTROL RECORD

VERSION	RELEASE DATE	SUMMARY OF CHANGES	NAME

IT Disaster Recovery Plan Attestation

As the designated authority for IT systems, I hereby certify that this IT Disaster Recovery Plan (DRP) is complete and that the information contained in this DRP provides an accurate representation of applications, hardware, software, and telecommunication components. I further certify that this document identifies the criticality of systems as it relates to the mission of the university, and that the recovery strategies identified will provide the ability to recover system functionality in the most expedient and cost-beneficial method in keeping with its level of criticality.

I further attest that this DRP for IT systems 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 Fire Safety & Emergency Planning Office plan repository.

_____ _____

(Print Name) (Job Title)

_____

(Signature)

As the department head for this unit, I hereby certify that this IT Disaster Recovery Plan (DRP) is complete and that the information contained in this DRP provides an accurate representation of the applications, hardware, software, and telecommunication components necessary to operate critical university functions.

_____ _____

(Print Name) (Dean or Department Head Title)

_____

(Signature)

IT Disaster Recovery Plan Distribution

Distribution of the IT DRP 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

INTRODUCTION

This Disaster Recovery Plan (DRP) captures, in a single repository, all of the information that describes **<<Organization Name>>**'s ability to recover from a disaster as well as the processes that must be followed to restore functionality after the disaster has been cleared.

Note that in the event of a disaster the first priority of **<<Organization Name>>** is to ensure the safety and well-being of our employees. Before any secondary measures are undertaken, **<<Organization Name>>** will ensure that all employees, and any other individuals on the organization's premises, are safe and secure.

After all individuals have been brought to safety, the next goal of **<<Organization Name>>** will be to enact the steps outlined in this DRP to bring all of the organization's critical systems into operational mode as quickly as possible. The main goals of this DRP include:

- Edit this list to reflect your organization's goals
- *Preventing the loss of the organization's resources such as hardware, data and physical IT assets*
- *Minimizing downtime related to IT*
- *Keeping the business running in the event of a disaster*

This DRP document will also detail how this document is to be maintained and tested.

SCOPE

The **<<Organization Name>>** IT DRP takes all of the following areas into consideration:

- Describe the systems/applications that this plan takes into consideration as well as dependencies for enterprise services or services provided by third parties.
- *Network Infrastructure*
- *Server Infrastructure*
- *Telephony System*
- *Data Storage and Backup Systems*
- *Data Output Devices*
- *End-user Computers*
- *Organizational Software Systems*
- *Database Systems*
- *IT Documentation*

This DRP does not take into consideration any non-IT, personnel, human resources, or real-estate-related disasters. For any disasters that are not addressed in this document, please refer to the business continuity plan created by **<<Organization Name>>** or contact **<<Business Continuity Lead>>** at **<<Business Continuity Lead Contact Information>>**.

ASSUMPTIONS

The following assumptions were used when developing this IT DRP:

- <<Insert Assumptions>>
- <<Insert Assumptions>>

This plan does not apply to the situations described below:

- <<Insert Assumptions>>
- <<Insert Assumptions>>

OVERVIEW OF IT DISASTER RECOVERY PLAN PHASES

This IT DRP has been developed to recover **critical services** 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 IT DRP phases are:

1. **Activation and Notification Phase –** Activation of the IT DRP occurs after a disruption or outage that may reasonably extend beyond the recovery time objective (RTO) established for a system.

   Once the IT DRP 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.

2. **Recovery Phase –** The recovery phase provides formal recovery operations that begin after the IT DRP has been activated, outage assessments have been completed, 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 IT components, repair of damage, and resumption of operational capabilities at the original or new permanent location. At the completion of the recovery phase, **critical services** will be functional and capable of performing the intended functions

3. **Reconstitution Phase –** The reconstitution phase defines the actions taken to reconstitute systems in the original data center or in extreme cases, in the new permanent data center. This phase consists of two major activities: validation of 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 normal 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. **<<Modify as appropriate to your area>>**

IT DRP ROLE	JOB TITLE	RESPONSIBILITIES
IT DRP Director	**<<Insert Job Title>>**	• Has overall responsibility for the development, execution, and maintenance of the IT DRP. • Ensures that the IT DRP is developed with the cooperation of personnel associated with the processes supported by the system. • Confirms expected duration of the system disruption with the IT DRP coordinator based on the outage assessment. • Declares activation of the IT DRP. • Determines if interim/secondary processing procedures and activities should be initiated to maintain current operations or if operations should be suspended until the system has been recovered. • Contacts **<<school/department>>** leadership if the situation needs to be escalated. • Is responsible for the testing, maintenance, and distribution of the IT DRP, which may be delegated to other personnel • Authorizes all changes to the IT DRP.
IT DRP Coordinator	**<<Insert Job Title>>**	• Activates the remote site. • Monitors recovery team activities until the system is fully recovered. • Ensures that recovery operations are performed consistent with service level agreements/service level requirements. • Provides periodic status updates to the IT DRP director. • Files an after action report (AAR) upon resumption of normal operations. • Assists the IT DRP director in testing, maintenance, and distribution of the IT DRP.
Alternate IT DRP Director	**<<Insert Job Title>>**	• Has same responsibilities as IT DRP director. • Is activated when the IT DRP director is unavailable.
Alternate IT DRP Coordinator	**<<Insert Job Title>>**	• Has same responsibilities as IT DRP coordinator. • Is activated when the IT DRP coordinator is unavailable.
Recovery Team	**<<Insert Job Title>>**	• Determines the expected duration of the failover to the alternate site. • Prioritizes the sequence of resource recovery. • Performs all system recovery and resumption activities. • Ensures voice and data communications are functioning. • Provides IP numbers and network routing information to appropriate personnel. • Includes validation testing teams or personnel.
Department Head	**<<Insert Job Title>>**	• Has overall responsibility for the unit. • Declares a disaster and authorizes the recovery operations to the remote site.
Alternate Department Head	**<<Insert Job Title>>**	• Has same responsibilities as department head. • Is activated when the department head is unavailable.

Table 1: Roles and Responsibilities (Primary and Alternate)

PHASE 1: ACTIVATION AND NOTIFICATION

The activation and notification phase defines initial actions taken once a disruption has been detected or appears to be imminent. This phase includes activities to conduct an outage assessment, activate the IT DRP, and notify recovery personnel. At the completion of the activation and notification phase, IT DRP staff will be prepared to perform recovery measures to restore system functions.

OUTAGE ASSESSMENT

The first step in the activation process is a thorough outage assessment to determine the extent of the disruption, any damage, potential for further disruption or system damage, and an expected recovery time of the system and/or primary data center.

The outage assessment is conducted by the outage assessment team. Assessment results are provided to the IT DRP coordinator to assist in the coordination of the recovery.

In the outage assessment, you will need to address the following questions:

- What is the cause of the outage?
- Are personnel safe and free from danger?
- Can you access the primary data site?
- Can systems be reached remotely?
- Can recovery occur in the primary location?
- How long does it take to reach the alternate recovery location?
- How long will it take to get hardware and software to the alternate location?
- How long will it take to get backup media to the remote location?
- Considering how long it takes to reactivate the system(s) or service(s), does recovery need to happen at the remote site to meet the RTO?

In this section, you should describe the process for capturing the information to answer the above questions. **Appendix E** is a placeholder for the outage assessment checklist.

ACTIVATION CRITERIA AND PROCEDURES

The **<<School/Department>>** IT DRP may be activated when one or more of the following criteria are met:

1. The type of outage indicates **critical systems** will be down at the primary site for more than the RTO hours.

2. The IT DRP Director determines that **critical services** cannot be recovered on the primary site.

Additionally, the decision to activate the IT DRP may require the IT DRP director to consult with **<<School/Department>>** leadership.

NOTIFICATION PROCEDURES

The first step following activation of the IT DRP 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 point of contact (POC), business continuity management (BCM) coordinator, school/department 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.
- Alerts and/or notification messages.

Call trees are an effective means of conveying the communication sequence in which leadership, recovery personnel, and school/department POCs should be alerted.

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

A call tree model for this IT DRP is available in **Appendix B**.

ESCALATION NOTICES/AWARENESS

Notifications include problem escalation to leadership and status awareness to system owners and users. Escalation procedures should be documented and should be included in the call tree of **Appendix B**.

PHASE 2: RECOVERY

The recovery phase provides formal recovery operations that begin after the IT DRP has been activated, outage assessments have been completed, 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 IT components, repair of damage, and resumption of operational capabilities at the original or new permanent location. At the completion of the recovery phase, **critical services** will be functional and capable of performing the intended functions.

SEQUENCE OF RECOVERY ACTIVITIES

The following high-level activities occur during the 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 system(s) from detailed recovery procedures (refer to **Appendix E**).
5. Perform validation and functional system tests (refer to **Appendix F**).

RECOVERY SITE

In the section below, describe the recovery location(s), considering the following attributes:

- *City and state of recovery site and distance from primary facility.*
- *Name and points of contact for the recovery site (this should also be in the vendor contact section of Appendix C).*
- *Procedures for accessing and using the recovery site, and access security features of 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 the recovery site in the event of a widespread disruption or disaster and SLAs or other agreements for use of recovery site, available office/support space, set up times, etc.*

ALTERNATE STORAGE FACILITY

In the section below, describe the alternate storage location(s), considering the following attributes:

- *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.*

ALTERNATE DATA/VOICE TELECOMMUNICATIONS

In the section below, describe how will you communicate with IT DRP staff before, during, and after a disaster, considering the following attributes:

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

DATA VALIDATION AND FUNCTIONALITY TESTING

Data validation and functionality testing is the process of testing and validating that recovered data, data files or databases, and functionality have been completely recovered. See **Appendix F** for detailed data validation and functionality testing procedures.

PHASE 3: RECONSTITUTION

During reconstitution, recovery activities are completed and normal system operations are resumed. If the original facility where the **system(s)/services** reside 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 IT DRP.

In theory, reconstitution should follow a similar process as recovery. Schools/departments will need to make a determination as to how to recover back to the primary location or, in some cases, how to recover to the new primary location. These steps, as well as the steps to deactivate the IT DRP, should be documented in **Appendix G**.

EVENT DOCUMENTATION

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

Information to be tracked and added to the IT DRP includes:

- 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.

Documentation of the after action report, lessons learned, and testing results must be submitted to the USC Information Security Office (usc-ciso@usc.edu), as soon as possible after the event.

DEACTIVATION

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

TRAINING AND TESTING EXERCISES

In the chart below, describe the training and testing exercises to be performed, considering the following attributes:

- Ensure that **<<school/department>>**'s personnel are familiar with the IT DRP and its associated activation and recovery and reconstitution procedures.
- Annually validate IT DRP 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 and functional.

ACTIVITY	FREQUENCY
EXERCISES	
Test IT DRP notification/activation procedures.	*Annually*
Test IT DRP communications.	*Annually*
Test primary and backup systems and services at alternate operating facilities (where applicable).	*Annually*
TRAINING	
IT DRP awareness/orientation training: a high-level overview presentation of IT DRP concepts for all personnel.	*Annually*

*Table 2: **<<School/Department>>** T&E Calendar*

CONCURRENT PROCESSING

If concurrent processing occurs for the system to be tested, see **Appendix H** for the appropriate procedures.

DOCUMENT MANAGEMENT

DOCUMENT OWNERSHIP

The contents of this document are the responsibility of **<<School/Department>>**, which has assigned the IT DRP director responsibility for its content, modifications, currency, and distribution to stakeholders.

PLAN REVIEW AND MAINTENANCE

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

The formal attestation page (page iii of this document) must be executed and submitted to the USC Information Security Office (usc-ciso@usc.edu), on an annual basis.

DOCUMENT DISTRIBUTION

A copy of this IT DRP will be distributed to the personnel identified in the table on page iv of this document and:

- Provided to system stakeholders who have an interest or responsibility for the development or testing of this plan.

- Held electronically, in hard copy, or both by every member of the recovery team in a place that is easily accessible in an emergency.

- Stored in an off-site location in both soft and hard copy format for ease of use under a wide range of circumstances.

APPENDICES

APPENDIX A: PERSONNEL CONTACT DATA

This section should be completed by all organizations. This section captures the contact information for all personnel involved in the recovery process.

IT DRP LEADERSHIP	
KEY PERSONNEL	**CONTACT INFORMATION**
DEPARTMENT HEAD	**Work #:**
Name, Title	
Street Address	
Room Number	**Mobile #:**
City, State, and ZIP Code	**Email: (NOTE: company email may not be functional)**
DR LEAD	**Work #:**
Name, Title	
Street Address	
Room Number	**Mobile #:**
City, State, and ZIP Code	**Email:**
DR LEAD – ALTERNATE	**Work #:**
Name, Title	
Street Address	
Room Number	**Mobile #:**
City, State, and ZIP Code	**Email:**
IT DRP COORDINATOR	**Work #:**
Name, Title	
Street Address	
Room Number	**Mobile #:**
City, State, and ZIP Code	**Email:**
IT DRP COORDINATOR – ALTERNATE	**Work #:**
Name, Title	
Street Address	
Room Number	**Mobile #:**
City, State, and ZIP Code	**Email:**
IT DRP COORDINATOR – ALTERNATE	**Work #:**
Name, Title	
Street Address	

Room Number	**Mobile #:**
City, State, and ZIP Code	**E-mail:**

Table 3: DRP Personnel Contact Data – Leadership (Modify as necessary to add roles)

PRIMARY/ALTERNATE SITE RECOVERY TEAM KEY PERSONNEL	
Recovery Team Name: _____	
KEY PERSONNEL	**CONTACT INFORMATION**
TEAM LEAD	**Work #:**
Name, Title	
Street Address	
Room Number	**Mobile #:**
City, State, and ZIP Code	**Email:**
SUB TEAM LEAD	**Work #:**
Name, Title	
Street Address	
Room Number	**Mobile #:**
City, State, and ZIP Code	**Email:**
ROLE	**Work #:**
Name, Title	
Street Address	
Room Number	**Mobile #:**
City, State, and ZIP Code	**Email:**
ROLE	**Work #:**
Name, Title	
Street Address	
Room Number	**Mobile #:**
City, State, and ZIP Code	**Email:**

Recovery Team Name:_____	
KEY PERSONNEL	**CONTACT INFORMATION**
TEAM LEAD	**Work #:**
Name, Title	
Street Address	
Room Number	**Mobile #:**
City, State, and ZIP Code	**Email:**
SUB TEAM LEAD	**Work #:**
Name, Title	
Street Address	
Room Number	**Mobile #:**

City, State, and ZIP Code	**Email:**
ROLE	**Work #:**
Name, Title	
Street Address	
Room Number	**Mobile #:**
City, State, and ZIP Code	**Email:**
ROLE	**Work #:**
Name, Title	
Street Address	
Room Number	**Mobile #:**
City, State, and ZIP Code	**Email:**

Table 4: DRP team contact list (add a table for each team)

APPENDIX B: CALL TREE

This section should be completed by all organizations. This section identifies the contact responsibilities during a disaster.

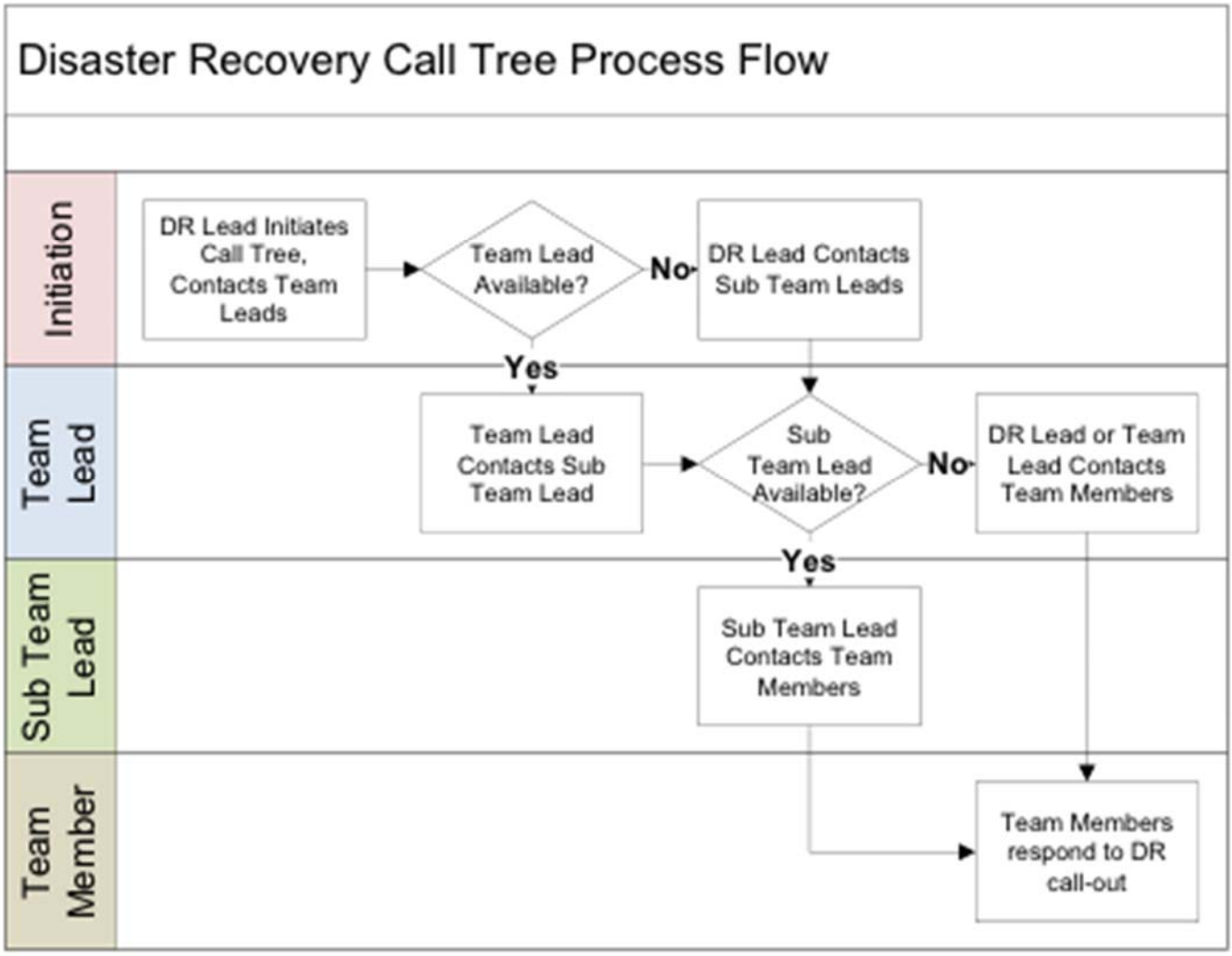

Figure 1: Call Tree <Sample shown above>

APPENDIX C: PERSONNEL CONTACT DATA – VENDORS

This section should be completed by all organizations. All vendors necessary to support the recovery of systems/services should be listed here. Most of these vendors will be hardware and software contacts but could also include systems contacts for third-party solutions.

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	
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 5: IT DRP Vendor Contact Data (Add a section for each vendor supporting the DRP)

APPENDIX D: OUTAGE ASSESSMENT CHECKLIST

This section is a placeholder for an outage assessment checklist to be used during the assessment phase.

APPENDIX E: DETAILED RECOVERY PROCEDURES

This section should be completed by all organizations. Edit this section to suit your organization's needs; lists should be made relevant to your organization.

RECOVERY PRIORITY	SYSTEM/SERVICE NAME	POC TITLE
1		
2		
3	Add additional lines to cover all components necessary to support critical services	

Table 6: Recovery Priority

Recovery Priority 1 Detailed Procedures:

<<Step by step instructions should be listed, providing sufficient detail to allow a similarly skilled individual to recover the system>>

Recovery Priority 2 Detailed Procedures:

<<Step by step instructions should be listed, providing sufficient detail to allow a similarly skilled individual to recover the system>>

Recovery Priority 3 Detailed Procedures:

<<Step by step instructions should be listed, providing sufficient detail to allow a similarly skilled individual to recover the system>>

<<Add additional sections to cover all components listed in the table above>>

This section below should be completed for each system considered in this plan. This section will likely be repeated to be made relevant to your organizations needs.

System Description

<<Insert system description>>

System Architecture

<<Insert system diagram>>

Figure 2: System Diagram

- The system's operating environment
  - *<<Insert text>>*
- Physical locations
  - *<<Insert text>>*
- General location of users
  - *<<Insert text>>*
- Partnerships with external organizations/system
  - *<<Insert text>>*
- Special technical considerations important for recovery purposes, such as unique backup procedures.
  - *<<Insert text>>*

IT System Inventory of Components

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

Table 7: IT System Components

Interconnected Systems

INFORMATION SYSTEM	INFORMATION TRANSFERRED OR SUPPORT PROVIDED	POC Title	POC's Organization

*Table 8: Information Systems That Connect with IT **System name***

*Refer to **Appendix A** for POC contact information

System Interconnections and Associated Plans

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

Table9: Associated Plans

*Refer to **Appendix A** for POC contact information

APPENDIX F: DATA VALIDATION AND FUNCTIONALITY TESTING PROCEDURES

This section should be completed by all organizations. Edit this section to suit your organization's needs. Lists and paragraphs should be made relevant to your organization. This section should document the data validation and functional testing to ensure systems are operating as expecting after recovery and/or reconstitution activities.

APPENDIX G: RECONSTITUTION

This section should be completed by all organizations. Edit this section to suit your organization's needs. Lists and paragraphs should be made relevant to your organization and describe the process to support concurrent processing during IT DRP testing exercises.

APPENDIX H: CONCURRENT PROCESSING

This section should be completed by all organizations. Edit this section to suit your organization's needs. Lists and paragraphs should be made relevant to your organization and describe the process to support concurrent processing during IT DRP testing exercises.