INFORMATION TECHNOLOGY DISASTER RECOVERY PLAN

POLICY# OTECH-POL2017-005

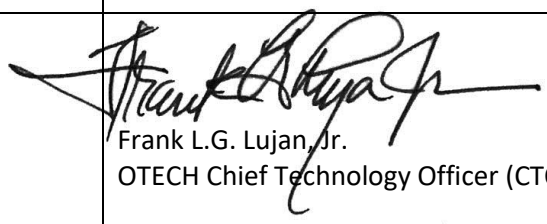
GOVERNMENT OF GUAM, OFFICE OF TECHNOLOGY
211 ASPINAL AVENUE HAGATNA, GUAM 96910
Otech.guam.gov

OFFICE OF TECHNOLOGY
GOVERNMENT OF GUAM

AUGUST 4, 2017

Contents

Overview

Policy Number:	OTECH-POL2017-005
Title:	Information Technology Disaster Recovery Plan
Purpose:	To define protocols and procedures in the event OTECH experiences a disaster.
Publication Date:	August 4, 2017
Policy Approval:	 Frank L.G. Lujan, Jr. OTECH Chief Technology Officer (CTO)
Target Audience:	Office of Technology employees
Contact Details:	**Office of Technology** 211 Aspinall Avenue Hagåtña, Guam 96910 O: 671.635.4500 F: 671.472.9508 otech.guam.gov

Revision History

Date of Change	Responsible	Summary of Change
July 2017	OTECH Systems Support	Draft policy
July 2017	OTECH Data Processing Manager and CTO	Review policy
August 2017	CTO	Approve policy
December 2021 March 2022	OTECH Systems Support	(a) Update policy format (b) Update Designated Team member subsections (c) Remove non-personnel, add new personnel (d) Remove DPHSS as virtual environment DR site (e) Add Review & Internal Audit section
March 2022	CTO OTECH CTO, *Frank LG Lujan, Jr.* Date: March 30, 2022	Review and Approve policy updates for dissemination.
February 2024	OTECH Systems Support	(a) Update roles and responsibilities (b) Update Organizational Chart (c) Update Communication with Employees
March 2024	CTO OTECH CTO, *Frank LG Lujan, Jr.* Date: March 1, 2024	Review and Approve policy updates for dissemination.

Introduction

This Disaster Recovery Plan (DRP) captures, in a single repository, all of the information that describes the Office of Technology's (OTECH) ability to withstand a disaster as well as the processes that must be followed to achieve disaster recovery within the Government of Guam's (GovGuam) information technology infrastructure and systems.

OTECH is committed to providing a highly reliable, secure and cost effective oversight, leadership and direction for activities relating to information technology to all agencies across GovGuam.

Definition of a Disaster

A disaster can be caused by man or nature and results in any of the GovGuam line agencies not being able to perform all or some of their regular roles and responsibilities for a period of time. OTECH defines disasters as the following:

- *One or more vital systems are non-functional*
- *The building is not available for an extended period of time but all systems are functional within it*
- *The building is available but all systems are non-functional*
- *The building and all systems are non-functional*

The following events can result in a disaster, requiring this Disaster Recovery document to be activated:

- *Fire*
- *Tsunami*
- *Pandemic*
- *Power Outage*
- *Theft*
- *Terrorist Attack*
- *Typhoon*
- *Earthquake*
- *Cyber Attack*

Purpose

The purpose of this DRP document is twofold: first to capture all of the information relevant to OTECH's ability to withstand a disaster, and second to document the steps that OTECH will follow if a disaster occurs.

Note that in the event of a disaster the first priority of OTECH is to prevent the loss of life. Before any secondary measures are undertaken, OTECH 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 OTECH will be to enact the steps outlined in this DRP to bring all of the organization's groups and departments back to business-as-usual as quickly as possible.

This includes:

- *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*

Scope

The OTECH DRP takes all of the following areas into consideration:

- *Network Infrastructure*
- *Servers 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 and real estate related disasters. For any disasters that are not addressed in this document, please refer to the respective GovGuam agency business continuity plan.

1.0 Disaster Recovery Teams & Responsibilities

In the event of a disaster, different groups will be required to assist the IT department in their effort to restore normal functionality to the employees of OTECH. The different groups and their responsibilities are as follows:

- *Disaster Recovery Lead(s)*
- *Disaster Management Team*
- *Network Team*
- *Server Team*
- *Applications Team*
- *Operations Team*

The lists of roles and responsibilities in this section have been created by OTECH and reflect the likely tasks that team members will have to perform. Disaster Recovery Team members will be responsible for performing all of the tasks below. In some disaster situations, Disaster Recovery Team members will be called upon to perform tasks not described in this section.

1.1 Disaster Recovery Lead

The Disaster Recovery Lead is responsible for making all decisions related to the Disaster Recovery efforts. This person's primary role will be to guide the disaster recovery process and all other individuals involved in the disaster recovery process will report to this person in the event that a disaster occurs at OTECH regardless of their department and existing managers.

1.1.1 Role and Responsibilities

- *Make the determination that a disaster has occurred and trigger the DRP and related processes.*
- *Initiate the DR Call Tree.*
- *Be the single point of contact for and oversee all of the DR Teams.*
- *Organize and chair regular meetings of the DR Team leads throughout the disaster.*
- *Present to the Management Team on the state of the disaster and the decisions that need to be made.*
- *Organize, supervise and manage all DRP test and author all DRP updates.*

1.1.2 Designated Team Members

Role/Title
Primary Disaster Lead, ***Chief Technology Officer***
Secondary Disaster Lead, ***Data Processing Manager***

1.2 Disaster Management Team

The Disaster Management Team that will oversee the entire disaster recovery process. They will be the first team that will need to take action in the event of a disaster. This team will evaluate the disaster and will determine what steps need to be taken to get the organization back to business as usual.

1.2.1 Role & Responsibilities

- *Set the DRP into motion after the Disaster Recovery Lead has declared a disaster*
- *Determine the magnitude and class of the disaster*
- *Determine what systems and processes have been affected by the disaster*
- *Communicate the disaster to the other disaster recovery teams*
- *Determine what first steps need to be taken by the disaster recovery teams*
- *Keep the disaster recovery teams on track with pre-determined expectations and goals*
- *Keep a record of money spent during the disaster recovery process*
- *Ensure that all decisions made abide by the DRP and policies set by OTECH*
- *Get the secondary site ready to restore business operations*
- *Ensure that the secondary site is fully functional and secure*
- *Notify the relevant parties once the disaster is over and normal business functionality has been restored*

1.2.2 Designated Team Members

Role/Title
Chief Technology Officer
Data Processing Manager
Systems & Programming Administrator
Administrative Officer

1.3 Network Team

The Network Team will be responsible for assessing damage specific to any network infrastructure and for provisioning data and voice network connectivity including WAN, LAN, and any telephony connections internally within the enterprise as well as telephony and data connections with the outside world. They will be primarily responsible for providing baseline network functionality and may assist other IT DR Teams as required.

1.3.1 Role & Responsibilities

- *In the event of a disaster that does not require migration to standby facilities, the team will determine which network services are not functioning at the primary facility*
- *If multiple network services are impacted, the team will prioritize the recovery of services in the manner and order that has the least business impact.*
- *If network services are provided by third parties, the team will communicate and co-ordinate with*

these third parties to ensure recovery of connectivity.

- *In the event of a disaster that does require migration to standby facilities the team will ensure that all network services are brought online at the secondary facility*
- *Once critical systems have been provided with connectivity, employees will be provided with connectivity in the following order:*
  - *All members of the DR Teams*
  - *All Executive Staff*
  - *All IT employees*
  - *All remaining employees*
- *Install and implement any tools, hardware, software and systems required in the standby facility*
- *Install and implement any tools, hardware, software and systems required in the primary facility*

1.3.2 Designated Team Members

Role/Title
System Programmers
System Analysts

1.4 Server Team

The Server Team will be responsible for providing the physical server infrastructure required for the enterprise to run its IT operations and applications in the event of and during a disaster. They will be primarily responsible for providing baseline server functionality and may assist other IT DR Teams as required.

1.4.1 Role & Responsibilities

- *In the event of a disaster that does not require migration to standby facilities, the team will determine which servers are not functioning at the primary facility*
- *If multiple servers are impacted, the team will prioritize the recovery of servers in the manner and order that has the least business impact. Recovery will include the following tasks:*
  - *Assess the damage to any servers*
  - *Restart and refresh servers if necessary*
- *Ensure that secondary servers located in standby facilities are kept up-to-date with system patches*
- *Ensure that secondary servers located in standby facilities are kept up-to-date with application patches*
- *Ensure that secondary servers located in standby facilities are kept up-to-date with data copies*
- *Ensure that the secondary servers located in the standby facility are backed up appropriately*
- *Install and implement any tools, hardware, and systems required in the standby facility*
- *Install and implement any tools, hardware, and systems required in the primary facility*

1.4.2 Designated Team Members

Role/Title
Data Processing Manager
Systems & Programming Administrator
Systems Programmers
Systems Analysts

1.5 Applications Team

The Applications Team will be responsible for ensuring that all enterprise applications operates as required to meet business objectives in the event of and during a disaster. They will be primarily responsible for ensuring and validating appropriate application performance and may assist other IT DR Teams as required.

1.5.1 Role & Responsibilities

- *In the event of a disaster that does not require migration to standby facilities, the team will determine which applications are not functioning at the primary facility*
- *If multiple applications are impacted, the team will prioritize the recovery of applications in the manner and order that has the least business impact. Recovery will include the following tasks:*
  - *Assess the impact to application processes*
  - *Restart applications as required*
  - *Patch, recode or rewrite applications as required*
- *Ensure that secondary servers located in standby facilities are kept up-to-date with application patches*
- *Ensure that secondary servers located in standby facilities are kept up-to-date with data copies*
- *Install and implement any tools, software and patches required in the standby facility*
- *Install and implement any tools, software and patches required in the primary facility*

1.5.2 Designated Team Members

Role/Title
Data Processing Manager
Systems & Programming Administrator
Programmer Analyst Supervisor
Data Processing Supervisor
System Programmers
System Analysts

1.6 Operations Team

This team's primary goal will be to provide employees with the tools they need to perform their roles as quickly and efficiently as possible. They will need to provision all OTECH employees in the standby facility and those working from home with the tools that their specific role requires.

1.6.1 Role & Responsibilities

- *Maintain lists of all essential supplies that will be required in the event of a disaster*
- *Ensure that these supplies are provisioned appropriately in the event of a disaster*
- *Ensure sufficient spare computers and laptops are on hand so that work is not significantly disrupted in a disaster*
- *Ensure that spare computers and laptops have the required software and patches*
- *Ensure sufficient computer and laptop related supplies such as cables, wireless cards, laptop locks, mice, printers and docking stations are on hand so that work is not significantly disrupted in a disaster*
- *Ensure that all employees that require access to a computer/laptop and other related supplies are provisioned in an appropriate timeframe*
- *If insufficient computers/laptops or related supplies are not available the team will prioritize distribution in the manner and order that has the least business impact*
- *This team will be required to maintain a log of where all of the supplies and equipment were used*

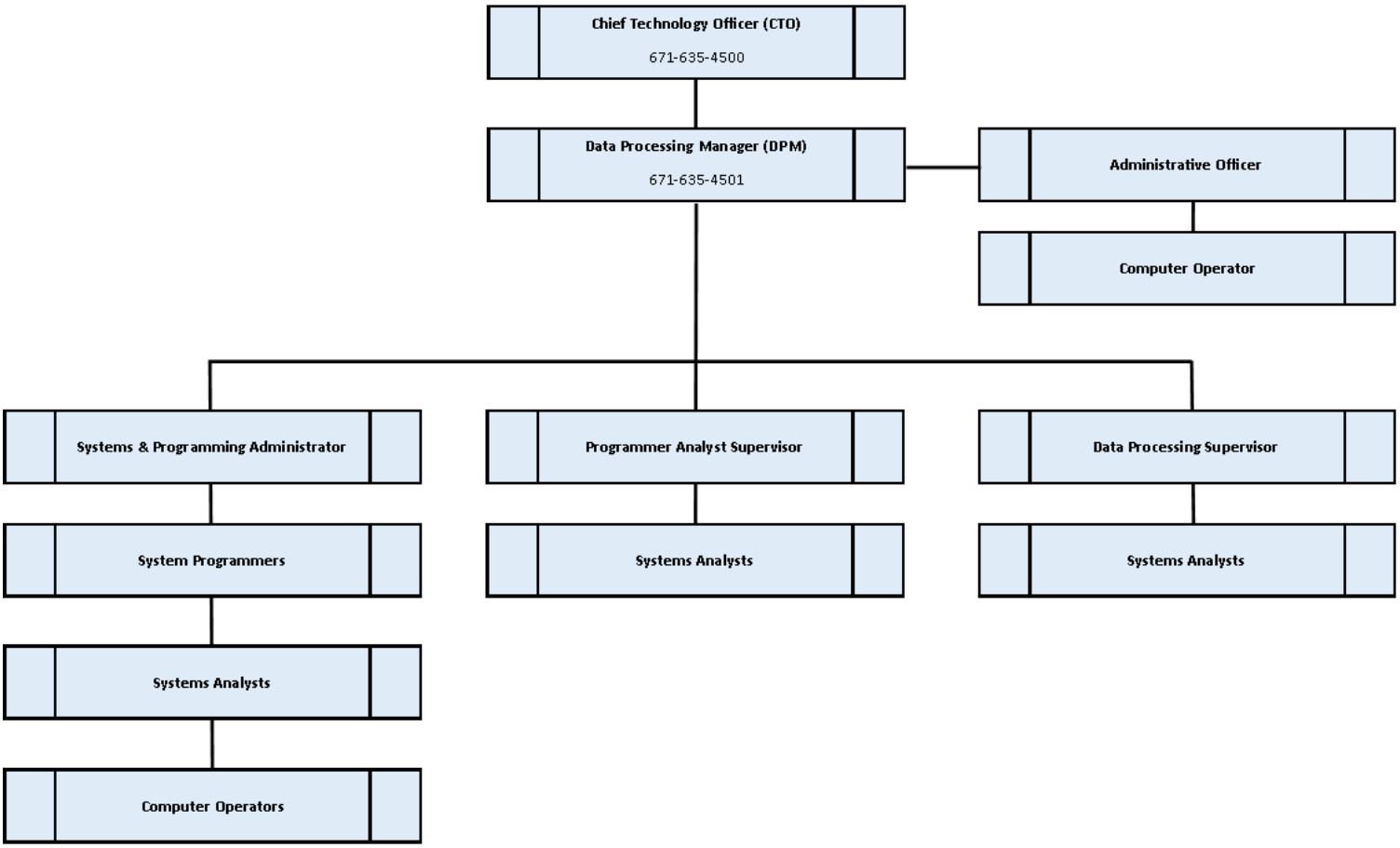
1.6.2 Designated Team Members

Role/Title
Systems & Programming Administrator
Computer Analysts
Computer Operators

2.0 Disaster Recovery Call Tree

In a disaster recovery or business continuity emergency, time is of the essence so OTECH will make use of a Call Tree to ensure that appropriate individuals are contacted in a timely manner.

In the event a team member is unavailable, the initial caller assumes responsibility for subsequent calls.



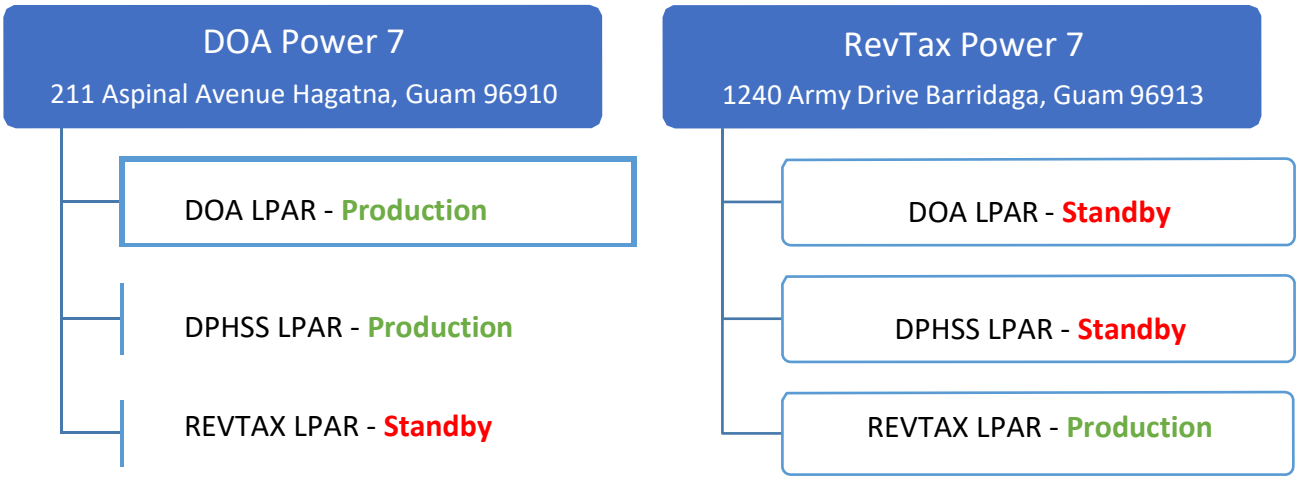
3.0 Recovery Facilities

In order to ensure that OTECH is able to withstand a significant outage caused by a disaster, it has provisioned separate dedicated standby facilities. This section of this document describes those facilities and includes operational information should those facilities have to be used.

3.1 Description of Recovery Facilities

The DR Standby facility will be used after the Disaster Recovery Lead has declared that a disaster has occurred. The affected system will determine which Standby system is activated and promoted to production. OTECH operates three (3) production datacenters to support GovGuam IT operations. Should the Disaster Recovery Lead declare a disaster at one of the production datacenters, the identified standby datacenter facility will be restored, rebuilt or promoted to reinstate end-user IT operations and support. The availability of resources will determine how the standby facility will be restored. Refer to diagram below for standby facilities.

System: Power 7 (Partial automatic failover in place)



System: Virtual Environments (Manual process to rebuild and restore servers based on availability of resources)

The standby facility will be used by the IT department and the Disaster Recovery teams; it will function as a central location where all decisions during the disaster will be made. It will also function as a communications hub for OTECH.

3.2 Data and Backups

Refer to the OTECH Backup Policy and Procedures for information on the backups. Servers will be restored based on the order of criticality.

3.2.1 MIMIX Replication for Power I Systems

MIMIX Replication has been implemented for the following Power I Systems, also referred to as the AS400 systems:

- Dept. of Administration (DOA)
- Dept. of Revenue & Taxation (REVTAX)
- Dept. of Public Health & Social Services (DPHSS)

3.2.1.1 Third-Party Requirements for MIMIX Replication and Backups

Third-party vendors who support and maintain the DOA, REVTAX and DPHSS IBMi (AS400) systems are responsible for informing OTECH of all new files, programs, libraries and objects that require the system to function on the failover/MIMIX partition. This is essential to ensure the integrity of the failover system and process, should a role swap be initiated. Vendors are also responsible for informing OTECH of new files that need to be included in backup processes, as well as scheduled jobs that may be affected during daily, weekly and monthly backups.

4.0 Communicating During a Disaster

In the event of a disaster, the DR Lead or DR Management Lead will need to communicate with various parties to inform them of the effects on the business, surrounding areas and timelines. They will be responsible for contacting all stakeholders.

4.1 Communicating with the Authorities

The DR Lead or DR Management Lead's first priority will be to ensure that the appropriate authorities have been notified of the disaster, providing the following information:

- *The location of the disaster*
- *The nature of the disaster*
- *The magnitude of the disaster*
- *The impact of the disaster*
- *Assistance required in overcoming the disaster*
- *Anticipated timelines*

4.2 Communicating with Employees

The DR Lead or DR Management Lead's second priority will be to ensure that the entire company has been notified of the disaster. The best and/or most practical means of contacting all of the employees will be used with preference on the following methods (in order):

- *Text Message (via Whatsapp and/or Teams group chat)*
- *E-mail (via corporate e-mail where that system still functions)*
- *Telephone to employee work number*
- *Telephone to employee mobile phone number*

The employees will need to be informed of the following:

- *Whether it is safe for them to come into the office*
- *Where they should go if they cannot come into the office*

- *Which services are still available to them*
- *Work expectations of them during the disaster*

4.3 Communicating with Clients

After all of OTECH's employees have been informed of the disaster, the DR Lead or DR Management Lead will be responsible for informing clients of the disaster and the impact that it will have on the following:

- *Anticipated impact on service offerings*
- *Anticipated impact on delivery schedules*
- *Anticipated impact on security of client information*
- *Anticipated timelines*

Crucial clients will be made aware of the disaster situation first. All other clients will be contacted only after all crucial clients have been contacted.

4.4 Communicated with Vendors

After all of the organization's employees have been informed of the disaster, the DR Lead or DR Management Lead will be responsible for informing vendors of the disaster and the impact that it will have on the following:

- *Adjustments to service requirements*
- *Adjustments to delivery locations*
- *Adjustments to Designated Team Members*
- *Anticipated timelines*

Crucial vendors will be made aware of the disaster situation first. All other vendors will be contacted only after all crucial vendors have been contacted.

Vendors encompass those organizations that provide everyday services to the enterprise, but also the hardware and software companies that supply the IT department.

5.0 Dealing with a Disaster

If a disaster occurs in OTECH, the first priority is to ensure that all employees are safe and accounted for. After this, steps must be taken to mitigate any further damage to the facility and to reduce the impact of the disaster to the organization.

Regardless of the category that the disaster falls into, dealing with a disaster can be broken down into the following steps:

1) Disaster identification and declaration
2) DRP activation
3) Communicating the disaster
4) Assessment of current and prevention of further damage
5) Standby facility activation
6) Establish IT operations
7) Repair and rebuilding of primary facility

5.1 Disaster identification and Declaration

Since it is almost impossible to predict when and how a disaster might occur, OTECH must be prepared to find out about disasters from a variety of possible avenues. These can include:

- *First hand observation*
- *System Alarms and Network Monitors*
- *Environmental and Security Alarms in the Primary Facility*
- *Security staff*
- *Facilities staff*
- *End users*
- *3rd Party Vendors*
- *Media reports*

Once the Disaster Recovery Lead has determined that a disaster had occurred, s/he must officially declare that the company is in an official state of disaster. It is during this phase that the Disaster Recovery Lead must ensure that anyone that was in the primary facility at the time of the disaster has been accounted for and evacuated to safety according to the company's Evacuation Policy.

While employees are being brought to safety, the Disaster Recovery Lead or the Disaster Recovery Management Lead will begin contacting the Authorities and all employees not at the impacted facility that a disaster has occurred.

5.2 DRP Activation

Once the Disaster Recovery Lead has formally declared that a disaster has occurred s/he will initiate the activation of the DRP by triggering the Disaster Recovery Call Tree. The following information will be provided in the calls that the Disaster Recovery Lead makes and should be passed during subsequent calls:

- *That a disaster has occurred*
- *The nature of the disaster (if known)*
- *The initial estimation of the magnitude of the disaster (if known)*
- *The initial estimation of the impact of the disaster (if known)*
- *The initial estimation of the expected duration of the disaster (if known)*
- *Actions that have been taken to this point*
- *Actions that are to be taken prior to the meeting of Disaster Recovery Team Leads*
- *Scheduled meeting place for the meeting of Disaster Recovery Team Leads*
- *Scheduled meeting time for the meeting of Disaster Recovery Team Leads*
- *Any other pertinent information*

If the Disaster Recovery Lead is unavailable to trigger the Disaster Recovery Call Tree, that responsibility shall fall to the Disaster Management Team Lead.

5.3 Communicating the Disaster

Refer to the "Communicating During a Disaster" section 4.0 of this document.

5.4 Assessment of Current and Prevention of Further Damage

Before any employees from OTECH can enter the primary facility after a disaster, appropriate authorities must first ensure that the premises are safe to enter.

During each team's review of their relevant areas, they must assess any areas where further damage can be prevented and take the necessary means to protect OTECH's assets. Any necessary repairs or preventative measures must be taken to protect the facilities.

5.5 Standby Facility Activation

The Standby Facility will be formally activated when the Disaster Recovery Lead determines that the nature of the disaster is such that the primary facility is no longer sufficiently functional or operational to sustain normal business operations.

The next steps will include:

1. *Determination of impacted systems*
2. *Criticality ranking of impacted systems*
3. *Recovery measures required for high criticality systems*
4. *Assignment of responsibilities for high criticality systems*
5. *Schedule for recovery of high criticality systems*
6. *Recovery measures required for medium criticality systems*
7. *Assignment of responsibilities for medium criticality systems*
8. *Schedule for recovery of medium criticality systems*
9. *Recovery measures required for low criticality systems*
10. *Assignment of responsibilities for recovery of low criticality systems*
11. *Schedule for recovery of low criticality systems*
12. *Determination of facilities tasks outstanding/required at Standby Facility*
13. *Determination of operations tasks outstanding/required at Standby Facility*
14. *Determination of communications tasks outstanding/required at Standby Facility*
15. *Determination of facilities tasks outstanding/required at Primary Facility*
16. *Determination of other tasks outstanding/required at Primary Facility*
17. *Determination of further actions to be taken*

5.6 Restoring IT Functionality

After the Standby Facility has been activated and the DR teams have restored the network, server and applications, the Operations team will be initiated to ensure that end users have the basic functions to perform their daily operations.

5.7 Repair & Rebuilding of Primary Facility

Before the enterprise can return operations to Primary Facilities, those facilities must be returned to an operable condition. The tasks required to achieve that will be variable depending on the magnitude and severity of the damage. Specific tasks will be determined and assigned only after the damage to Primary Facilities has been assessed.

Review and Internal Audit

This policy shall be reviewed and updated annually, on an as needed basis, or if there is a breach in protocol and procedures. OTECH shall initiate the review process on the first day of each Fiscal Year – 1st of October, or next business day. Policy review and updates shall be documented in the policy's *Revision History* section. The review process shall be completed before the end of the Fiscal Year's first quarter and the updated policy shall be disseminated (via OTECH website, Agency Memo or email) by December 31 of each year.