MSLA-ID	***Disaster Recovery Policy and Plan***

Overview

This document is for exclusive use by MSLA.

Version	Description [or description of changes]	Author	Creation date	Approved by	Date approval
1.5	Updated version	MSLA IT Department	10/21/2024	Luis Rios	10/25/2024

TABLE OF CONTENTS

Purpose

The purpose of the MSLA ID Business Continuity and Disaster Recovery Policy and Plan is to provide direction and general rules for the creation, implementation, and management of the MSLA ID Disaster Recovery Plan (DRP).

Audience

The MSLA ID Disaster Recovery Policy and Plan applies to individuals accountable for ensuring a disaster recovery plan is developed, tested, and maintained.

Policy

- MSLA ID must create and implement a Business Continuity and Disaster Recovery Plan ("BDRP").
- The DRP must be periodically tested and the results should be used as part of the ongoing improvement of the DRP.
- The DRP, at a minimum, will identify and protect against risks to critical systems and sensitive information in the event of a disaster.
- The DRP shall provide for contingencies to restore information and systems if a disaster occurs. The concept of a disaster recovery includes business resumption.
- MSLA ID disaster recovery planning must ensure that:
    - an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience, and competence;
    - personnel with the necessary responsibility, authority, and competence to manage an incident and maintain information security are nominated;
    - documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security continuity objectives.

Disaster Recovery Plan

For MSLA disaster recovery plan, the following three elements should be addressed.

- **Emergency Response Procedures**

  To document the appropriate emergency response to a fire, natural disaster, or any other activity in order to protect lives and limit damage.

- **Backup Operations Procedures**

  To ensure that essential data processing operational tasks can be conducted after the disruption.

- **Recovery Actions Procedures**

  To facilitate the rapid restoration of a data processing system following a disaster.

I. Disaster action checklist

1. Plan Initiation
    - Notify senior management
    - Contact and set up disaster recovery team
    - Determine degree of disaster
    - Implement proper application recovery plan dependent on extent of disaster
    - Monitor progress
    - Contact backup site and establish schedules
    - Contact all other necessary personnel--both user and data processing
    - Contact vendors--both hardware and software
    - Notify users of the disruption of service
2. Follow-Up Checklist
    - List teams and tasks of each
    - Obtain emergency cash and set up transportation to and from backup site, if necessary
    - Set up living quarters, if necessary
    - Set up eating establishments, as required
    - List all personnel and their telephone numbers
    - Establish user participation plan

- Set up the delivery and the receipt of mail
- Establish emergency office supplies
- Rent or purchase equipment, as needed
- Determine applications to be run and in what sequence
- Identify number of workstations needed
- Check out any off-line equipment needs for each application
- Check on forms needed for each application
- Check all data being taken to backup site before leaving and leave inventory profile at home location
- Set up primary vendors for assistance with problems incurred during emergency
- Plan for transportation of any additional items needed at backup site
- Take directions (map) to backup site
- Take copies of system and operational documentation and procedural manuals.
- Ensure that all personnel involved know their tasks
- Notify insurance companies

II. *Recovery start-up procedures for use after a disaster*

- Notify CEO of the need to utilize service and of recovery plan selection.
- Provide Administration Officer with an equipment delivery site address (when applicable), a contact, and an alternate contact for coordinating service and telephone numbers at which contacts can be reached 24 hours a day.
- Contact power and telephone service suppliers and schedule any necessary service connections.
- Notify CEO immediately if any related plans should change.

III. *Restoring the entire system*

To get your system back to the way it was before the disaster, use the procedures on recovering after a complete system loss in the Backup and Recovery, SC41-5304-06.

Before You Begin: Find the following tapes, equipment, and information from the on-site tape vault or the off-site storage location:

- If you install from the alternate installation device, you need both your tape media and the CD-ROM media containing the Licensed Internal Code.

- All tapes from the most recent complete save operation
- The most recent tapes from saving security data (SAVSECDTA or SAVSYS)
- The most recent tapes from saving your configuration, if necessary
- All tapes containing journals and journal receivers saved since the most recent daily save operation
- All tapes from the most recent daily save operation
- PTF list (stored with the most recent complete save tapes, weekly save tapes, or both)
- Tape list from most recent complete save operation
- Tape list from most recent weekly save operation
- Tape list from daily saves
- History log from the most recent complete save operation
- History log from the most recent weekly save operation
- History log from the daily save operations
- The Software Installation book
- The Backup and Recovery book
- Telephone directory
- Modem manual
- Tool kit

IV. Testing the disaster recovery plan

In successful contingency planning, it is important to test and evaluate the plan regularly. Data processing operations are volatile in nature, resulting in frequent changes to equipment, programs, and documentation. These actions make it critical to consider the plan as a changing document. Use these checklists as your conduct your test and decide what areas should be tested.

Table 1. Conducting a recovery test

Item	Yes	No	Applicable	Not Applicable	Comments
Select the purpose of the test. What aspects of the plan are being evaluated?					
Describe the objectives of the test. How will you measure successful achievement of the objectives?					
Meet with management and explain the test and objectives. Gain their agreement and support.					
Have management announce the test and the expected completion time.					
Collect test results at the end of the test period.					
Evaluate results. Was recovery successful? Why or why not?					
Determine the implications of the test results. Does successful recovery in a simple case imply successful recovery for all critical jobs in the tolerable outage period?					
Make recommendations for changes. Call for responses by a given date.					
Notify other areas of results. Include users and auditors.					
Change the disaster recovery plan manual as necessary.					

Table 2.Areas to be tested

Item	Yes	No	Applicable	Not Applicable	Comments
Recovery of individual application systems by using files and documentation stored off-site.					
Reloading of system tapes and performing an IPL by using files and documentation stored off-site.					
Ability to process on a different computer.					
Ability of management to determine priority of systems with limited processing.					
Ability to recover and process successfully without key people.					
Ability of the plan to clarify areas of responsibility and the chain of command.					
Effectiveness of security measures and security bypass procedures during the recovery period.					
Ability to accomplish emergency evacuation and basic first-aid responses.					
Ability of users of real-time systems to cope with a temporary loss of on-line information.					
Ability of users to continue day-to-day operations without applications or jobs that are considered noncritical.					
Ability to contact the key people or their designated alternates quickly.					
Ability of data entry personnel to provide the input to critical systems by using alternate sites and different input media.					
Availability of peripheral equipment and processing, such as printers and scanners.					
Availability of support equipment, such as air conditioners and dehumidifiers.					
Availability of support: supplies, transportation, communication.					
Distribution of output produced at the recovery site.					
Availability of important forms and paper stock.					
Ability to adapt plan to lesser disasters.					

Waivers

Waivers from certain policy provisions may be sought following the MSLA ID Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.