IT Disaster Recovery Manual

Company: Metro Global Holdings Corporation
Document Version: 1.0
Last Updated: May 18, 2025
Document Owner: E.Hui, ITG

Table of Contents

8. Data Backup and Restoration Procedures (Detailed)
    8.1. General Data Restoration Principles
    8.2. Restoration from Local Backups
    8.3. Restoration from Offsite Cloud Backups
    8.4. Restoration from Physical Offsite Media
    8.5. Database Restoration Procedures (General)
    8.5.1. SQL Server Restoration Example
    8.6. File Server Data Restoration
    8.7. SaaS Data Restoration (e.g., Microsoft 365, Salesforce)
    8.8. Data Validation and Integrity Checks

9. DR Site and Facilities Operations (If Applicable)
    9.1. DR Site Activation
    9.2. Site Management and Security
    9.3. Logistics and Support at DR Site
    9.4. Deactivation of DR Site and Return to Primary

10. Plan Testing, Maintenance, and Training
    10.1. Testing Program Overview
    10.2. Types of DR Tests
    10.2.1. Checklist Review
    10.2.2. Walkthrough Test (Tabletop Exercise)
    10.2.3. Simulation Test
    10.2.4. Parallel Test

11. 10.2.5. Full Interruption Test (Cutover Test)
    10.3. Test Planning and Scheduling
    10.4. Test Execution and Evaluation
    10.5. Post-Test Reporting and Remediation
    10.6. Plan Maintenance and Updates (Cross-reference to 1.7)
    10.7. Training and Awareness Program
    10.7.1. DR Team Training
    10.7.2. Employee Awareness
    10.7.3. Specialized Technical Training

1. Introduction

1.1. Purpose of the Manual

This IT Disaster Recovery (DR) Manual provides a framework for Metro Global Holdings Corporation to respond to and recover from significant IT disruptions that could adversely affect business operations. The primary purpose of this manual is to ensure the timely and effective restoration of critical IT services, applications, and data, thereby minimizing financial losses, operational disruptions, reputational damage, and legal or regulatory impacts.

A disaster, in the context of this manual, is defined as any event, natural or man-made, that renders critical IT systems, infrastructure, or facilities inoperable for an unacceptable period, exceeding the predefined Recovery Time Objectives (RTOs). This includes, but is not limited to, events such as fires, floods, earthquakes, power outages, cyber-attacks (e.g., ransomware, DDoS), hardware failures, software corruption, and human error.

This manual outlines the necessary procedures, roles, responsibilities, and resources required to:

- Identify and assess potential threats to IT operations.
- Implement preventative measures to mitigate risks.
- Establish clear criteria for activating the DR plan.
- Define the steps for recovering critical IT systems and business functions.
- Ensure effective communication among stakeholders during a disaster.
- Facilitate a smooth transition back to normal operations post-disaster.
- Regularly test, review, and update the DR plan to maintain its effectiveness.

The successful implementation of this DR manual is crucial for the resilience and continuity of Metro Global Holdings Corporation's operations, safeguarding its assets, client relationships, and market position. It serves as a guide for all personnel involved in the disaster recovery process and ensures a coordinated and efficient response.

1.2. Scope

This IT Disaster Recovery Manual applies to all IT systems, infrastructure, data, and personnel managed by or supporting Metro Global Holdings Corporation across all its locations, including [List Main Office Location(s) and any Branch Offices]. The scope encompasses:

- **All Critical IT Infrastructure:** This includes, but is not limited to, servers (physical and virtual), storage area networks (SANs), network-attached storage (NAS), networking equipment (routers, switches, firewalls), communication systems (VoIP, email servers), and data centers or server rooms.
- **All Critical Business Applications:** This includes core applications such as Front-End Customer-Facing access points, Customer Relationship Management

(CRM) software, property management systems, transaction management platforms, financial and accounting software, and internal/external websites and portals.
- **All Company Data:** This includes client databases, property information, transaction records, financial data, employee records, legal documents, and all other forms of electronic data essential for business operations.
- **Recovery Processes:** Procedures for data backup, system restoration, network recovery, and resumption of IT services at primary and alternate locations (if applicable).
- **Personnel:** All employees, contractors, and third-party vendors who have responsibilities related to IT systems and disaster recovery.

Out of Scope:
While this manual focuses on IT disaster recovery, it is designed to integrate with the broader Business Continuity Plan (BCP) of Metro Global Holdings Corporation. Aspects outside the direct scope of IT recovery, such as:

- Non-IT related business process recovery (e.g., manual workarounds for an extended period not directly tied to IT system restoration).
- Physical security of buildings (beyond IT facilities).
- Human resources aspects like payroll continuity through non-IT means or employee counseling (though IT systems supporting these are in scope).
- Long-term business strategy changes post-disaster.

These out-of-scope items are expected to be addressed in separate, relevant company policies or the overall BCP. This IT DR manual specifically addresses the restoration of technology services and infrastructure necessary to support the resumption of critical business functions.

1.3. Objectives

The primary objectives of this IT Disaster Recovery Manual are to:

1. **Minimize Business Impact:** Reduce the duration and impact of IT disruptions on critical business operations of Metro Global Holdings Corporation, including client service, transaction processing, and financial management.
2. **Ensure Timely Recovery:** Restore critical IT systems, applications, and data within predefined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) as determined by the Business Impact Analysis (BIA).
3. **Protect Company Assets:** Safeguard critical data, hardware, software, and intellectual property from loss or damage during and after a disaster.
4. **Maintain Client Confidence:** Demonstrate a robust capability to recover from disasters, thereby maintaining the trust and confidence of clients, partners, and stakeholders.
5. **Meet Regulatory and Compliance Requirements:** Ensure compliance with relevant legal, regulatory, and contractual obligations related to data protection, availability, and business continuity (e.g., data privacy laws, service level agreements).

6. **Provide Orderly Recovery:** Establish clear procedures, roles, and responsibilities to ensure a structured, coordinated, and efficient recovery process.
7. **Reduce Financial Losses:** Minimize direct financial losses (e.g., lost revenue, repair costs) and indirect losses (e.g., damage to reputation, loss of market share) resulting from an IT outage.
8. **Ensure Safety of Personnel:** While the primary focus is IT, the plan supports overall business continuity efforts which include considerations for personnel safety during disaster events.
9. **Facilitate Effective Communication:** Establish communication channels and protocols for internal and external stakeholders during a disaster recovery effort.
10. **Promote Continuous Improvement:** Implement a framework for regular testing, review, and updating of the DR plan to adapt to changing business needs, technology environments, and threat landscapes.

Achieving these objectives will enhance the overall resilience of Metro Global Holdings Corporation and its ability to withstand and recover from unforeseen disruptive events.

1.4. Assumptions

The development and execution of this IT Disaster Recovery Manual are based on the following assumptions:

1. **Business Impact Analysis (BIA) Accuracy:** The BIA, which identifies critical systems and acceptable downtime (RTO/RPO), is accurate and reflects the current business needs of Metro Global Holdings Corporation.
2. **Executive Support:** There is ongoing commitment and support from executive management for the DR program, including allocation of necessary resources (financial, personnel, technical).
3. **Availability of Key Personnel:** Key personnel with defined roles and responsibilities in the DR plan will be available and able to perform their duties during a disaster. Contingency plans for unavailable key personnel are considered.
4. **Data Backup Integrity:** Data backups are performed regularly as scheduled, are complete, and are restorable. Offsite backups are secure and accessible.
5. **Vendor Cooperation:** Critical third-party vendors (e.g., software providers, cloud service providers, hardware suppliers, ISP) will cooperate and provide support in accordance with their service level agreements (SLAs) or contractual obligations during a disaster.
6. **Alternate Site Availability (if applicable):** If an alternate recovery site (hot, warm, or cold) is part of the strategy, it is assumed to be available and equipped as specified. For remote work strategies, it's assumed employees have or will be provided with necessary access and resources.
7. **Communication Infrastructure:** Basic communication channels (e.g., mobile phones, alternative internet access) will be available for the DR team, even if

primary company communication systems are down.

8. **Plan Maintenance:** This DR manual will be regularly reviewed, tested, and updated (at least annually or upon significant changes to IT infrastructure, business processes, or personnel).
9. **Employee Training:** Relevant employees and DR team members are trained on their roles and responsibilities as outlined in this manual.
10. **Worst-Case Scenario Consideration:** The plan is designed to address a significant disaster that renders primary IT facilities or systems inoperable.
11. **Partial Disasters:** The plan is flexible enough to be invoked for partial disasters affecting only specific systems or locations.
12. **Security Measures:** Appropriate security measures are in place at primary and recovery locations to protect data and systems during and after a disaster.
13. **Integration with BCP:** This IT DR Manual is a component of a broader Business Continuity Plan (BCP) for Metro Global Holdings Corporation. Non-IT related recovery aspects are addressed within the BCP.
14. **Financial Resources for Recovery:** Metro Global Holdings Corporation has, or can access, the necessary financial resources to cover the costs associated with disaster recovery efforts (e.g., equipment replacement, vendor services, overtime).

If any of these assumptions prove to be incorrect at the time of a disaster, the effectiveness of this plan may be compromised, and recovery efforts may need to be adjusted accordingly.

1.5. Audience

The intended audience for this IT Disaster Recovery Manual includes, but is not limited to:

- **Executive Management and Leadership Team:** To understand the DR strategy, resource commitments, and their roles in authorizing plan activation and overseeing recovery efforts.
- **IT Department Staff:** All members of the IT department, who will be responsible for executing technical recovery procedures. This includes system administrators, network engineers, database administrators, application support specialists, and help desk personnel.
- **Disaster Recovery Coordinator (DRC) and DR Team Members:** Individuals specifically assigned roles and responsibilities within the DR team structure. This manual is their primary guide for action.
- **Department Heads and Business Unit Managers:** To understand how IT recovery will support their respective business functions and their roles in coordinating with the DR team.
- **Departmental Coordinators:** Representatives from various business units who will liaise with the DR team and assist in validating recovered systems and data.
- **Key Business Personnel:** Employees identified as critical for the recovery and resumption of essential business processes dependent on IT.

- **Compliance and Audit Teams:** To review the plan for adequacy, completeness, and compliance with relevant regulations and standards.
- **Relevant Third-Party Vendors and Partners:** Sections of the plan may be shared with key vendors or partners whose services are critical for recovery.

The level of detail and specific sections relevant to each audience member may vary. All individuals with assigned responsibilities within this manual are expected to be familiar with its contents, particularly the sections pertaining to their roles. A summarized version or specific procedural documents may be distributed to a wider employee base for general awareness.

1.6. Confidentiality

This IT Disaster Recovery Manual contains sensitive information regarding Metro Global Holdings Corporation's IT infrastructure, security measures, recovery procedures, and contact details for key personnel. Unauthorized disclosure of this information could compromise the security and effectiveness of the DR plan and potentially expose the company to risks.

Therefore, this document is classified as **CONFIDENTIAL**.

- **Distribution:** Distribution of this manual, in whole or in part, is restricted to authorized personnel who have a legitimate need to know as defined by their roles and responsibilities in the disaster recovery process. A distribution list will be maintained by the Document Owner (E.Hui, ITG or designated DR Coordinator).
- **Storage:** Electronic copies should be stored securely with access controls. Physical copies should be kept in secure locations (e.g., locked cabinets).
- **Handling:** Personnel with access to this manual must handle it with care and take precautions to prevent unauthorized access, copying, or dissemination.
- **Destruction:** Obsolete or outdated versions of this manual should be destroyed securely (e.g., shredding for physical copies, secure deletion for electronic copies).
- **Third-Party Sharing:** If sections of this manual need to be shared with third-party vendors or consultants, appropriate Non-Disclosure Agreements (NDAs) must be in place. Only relevant sections should be shared.

All personnel who receive a copy of this manual are responsible for maintaining its confidentiality. Any suspected or actual breach of confidentiality should be reported immediately to the Document Owner or a member of Executive Management.

1.7. Document Control and Maintenance

Document Owner: E.Hui, ITG or designated Disaster Recovery Coordinator.

Version Control:
This document will be version controlled. Each update will result in a new version number and an updated "Last Updated" date. A summary of changes will be recorded in a version

history log (see Appendix [J] – Version History).

Version	Date	Author(s)	Summary of Changes	Approved By
1.0	May 18, 2025	E.Hui	Initial Draft	E.Hui
[x.x]	[Date]	[Name]	[Description of changes]	[Approver]

Review Schedule:
This IT Disaster Recovery Manual will be reviewed and updated:

- **Annually:** A comprehensive review will be conducted at least once every 12 months.
- **Post-Incident/Test:** Following any disaster recovery invocation or major DR test, the plan will be reviewed for lessons learned and necessary modifications.
- **Significant Changes:** When there are significant changes to the IT environment (e.g., new critical systems, major infrastructure upgrades), business operations, or key personnel.

Update Process:

1. Proposed changes should be submitted to the Document Owner.
2. The Document Owner, in consultation with the DR Team and relevant stakeholders, will review proposed changes.
3. Approved changes will be incorporated into the manual.
4. The version number and last updated date will be revised.
5. The updated manual will be distributed to all authorized personnel, and outdated versions will be recalled or instructions for their destruction provided.
6. A log of all changes will be maintained in the version history.

Distribution List:
A formal distribution list for this manual will be maintained by the Document Owner. This list will include all individuals and teams who require a copy of the plan. (See Appendix [X] – Distribution List). Note: Appendix X is a generic placeholder, the correct appendix for Distribution List is TBD or should be named.

Storage of the Plan:

- **Electronic Copies:** Securely stored on [Specify location, e.g., a restricted network share, secure cloud storage] with appropriate access controls. At least one electronic copy should be accessible from an offsite location or through means not dependent on the primary site's infrastructure.
- **Physical Copies:** A limited number of physical copies should be maintained in secure, accessible locations, including [Specify primary office location] and an offsite location [Specify offsite storage location, e.g., home of DR Coordinator, bank safe deposit box]. Physical copies should be clearly marked with the

version number and date.

It is the responsibility of each individual on the distribution list to ensure they have the latest version of the manual.

2. Roles and Responsibilities

Effective disaster recovery depends on clearly defined roles and responsibilities. This section outlines the structure of the Metro Global Holdings Corporation Disaster Recovery Team (DRT) and the specific duties of its members and other key stakeholders.

2.1. Disaster Recovery Team Structure

Metro Global Holdings Corporation will establish a Disaster Recovery Team (DRT) responsible for developing, maintaining, testing, and executing the IT DR plan. The DRT is a cross-functional team composed of individuals with the necessary skills and authority.

Core Disaster Recovery Team (DRT) Structure:

- **Disaster Recovery Coordinator (DRC):** Overall lead for DR planning and execution.
- **IT Management Team:** Provides oversight and technical leadership. Includes [CIO/IT Director, IT Managers].
- **Technical Recovery Teams:** Specialized teams focused on specific areas:
  - **Infrastructure Team:** Servers, storage, virtualization.
  - **Network Team:** Network connectivity, security, remote access.
  - **Applications Team:** Critical business applications (CRM, Financials, etc.).
  - **Database Team:** Database administration and recovery.
  - **Communications Systems Team:** Email, VoIP recovery.
- **Departmental Coordinators:** Representatives from key business units (e.g., Sales, Property Management, Finance, Legal, Marketing).
- **Communications Team Lead:** Manages internal and external communications during a disaster.
- **Administrative Support:** Provides logistical and administrative assistance to the DRT.

Supporting Roles (involved as needed):

- **Executive Management:** Provides overall authority, approves plan invocation, and allocates resources.
- **Security Officer:** Addresses security aspects of the disaster and recovery process.
- **Facilities Management:** Manages physical site issues and alternate workspace logistics.
- **Human Resources:** Addresses personnel issues, safety, and communication with employees.

- **Legal Counsel:** Advises on legal and regulatory implications.
- **Third-Party Vendors:** Key suppliers of hardware, software, and services.

2.2. Key Roles and Responsibilities

2.2.1. Disaster Recovery Coordinator (DRC)

- **Primary Contact:** E.Hui, ITG, eph@metroglobalholdings.com
- **Alternate Contact:** S.Alcantara, Head of Audit, ssa@metroglobalholdings.com
- **Responsibilities:**
  - Leads and coordinates all DR planning, development, and maintenance activities.
  - Chairs DRT meetings.
  - Ensures the DR plan is regularly tested, reviewed, and updated.
  - Coordinates DR training for team members and awareness for employees.
  - During a disaster:
    - Assesses the situation and recommends plan activation to Executive Management.
    - Oversees the execution of the DR plan.
    - Serves as the central point of contact for DR activities.
    - Coordinates efforts of all DRT members and technical teams.
    - Liaises with Departmental Coordinators and Executive Management.
    - Manages the DR budget and resources during an event.
    - Ensures proper documentation of the recovery process.
    - Oversees the transition back to normal operations (resumption).
    - Conducts post-incident reviews and updates the DR plan.

2.2.2. IT Management Team

- **Members:** A.Mejia, ITG COS, amejia@metroglobalholdings.com
- **Responsibilities:**
  - Provide strategic direction and oversight for the DR program.
  - Approve the DR plan and significant updates.
  - Ensure adequate resources (budget, personnel, tools) are allocated for DR.
  - Support the DRC in their role.
  - During a disaster:
    - Participate in the decision to declare a disaster.
    - Provide leadership and direction to the technical recovery teams.
    - Authorize emergency expenditures.
    - Interface with Executive Management on recovery progress.
    - Assist in prioritizing recovery efforts based on business needs.

2.2.3. Technical Recovery Teams

(e.g., Infrastructure, Network, Applications, Database, Communications Systems Teams)

- **Team Leads:** F.Ramos, ITG Member, framos@metroglobalholdings.com
- **Responsibilities (General):**

    - Develop and document detailed recovery procedures for their respective systems and services.
    - Participate in DR tests and exercises.
    - Maintain an inventory of relevant hardware, software, and configurations.
    - During a disaster:
        - Execute the specific recovery procedures for their assigned systems.
        - Work under the direction of the DRC and IT Management.
        - Troubleshoot and resolve technical issues during recovery.
        - Validate system functionality post-recovery.
        - Provide regular status updates to the DRC.
        - Secure systems and data during the recovery process.
    - **Specific Team Responsibilities:**
        - **Infrastructure Team:** Recover servers (physical/virtual), storage systems, backup systems, and core data center facilities.
        - **Network Team:** Restore local and wide area networks, internet connectivity, VPNs, firewalls, and other network security devices.
        - **Applications Team:** Restore critical business applications (MLS, CRM, Financials, etc.), ensuring data integrity and user access. Coordinate with application vendors if necessary.
        - **Database Team:** Recover and restore databases, ensuring data consistency and integrity. Perform data validation.
        - **Communications Systems Team:** Restore email systems, VoIP phone systems, and other critical communication platforms.

2.2.4. Departmental Coordinators

- **Representatives from:** Sales, Property Management, Finance, Legal, Marketing, Operations, etc.
- **Responsibilities:**
    - Represent their department's interests in DR planning.
    - Assist in identifying critical business processes and their IT dependencies within their department.
    - Communicate DR plan updates and procedures to their respective departments.
    - During a disaster:
        - Act as the primary point of contact between their department and the DRT.
        - Communicate recovery status and instructions to their department staff.
        - Coordinate user acceptance testing (UAT) of recovered systems for their department.
        - Assist in identifying and prioritizing recovery of departmental data and functions.
        - Report any issues or specific departmental needs to the DRC.

2.2.5. Executive Management

- **Members:** [CEO, COO, CFO, and other key executives]
- **Responsibilities:**
  - Provide overall sponsorship and endorsement of the DR program.
  - Approve the DR Manual and associated budget.
  - During a disaster:
    - Make the final decision to declare a disaster and activate the DR plan based on recommendations from the DRC and IT Management.
    - Provide high-level direction and support to the recovery effort.
    - Authorize significant emergency expenditures or policy exceptions.
    - Act as the public face of the company if required, in coordination with the Communications Team.
    - Interface with the Board of Directors and key external stakeholders.

2.2.6. Communications Team Lead

- **Primary Contact:** R.Encilla, ITG Admin, ruffaencilla@fiterasystems.com
- **Responsibilities:**
  - Develop and maintain a crisis communication plan (which may be separate but linked to the IT DR Manual).
  - During a disaster:
    - Manage all internal and external communications in coordination with the DRC and Executive Management.
    - Prepare and disseminate official statements to employees, clients, media, and other stakeholders.
    - Monitor media and public sentiment.
    - Establish and manage an emergency communication hotline or information portal if needed.

2.2.7. Administrative Support

- **Primary Contact:** R.Encilla, ITG Admin, ruffaencilla@fiterasystems.com
- **Responsibilities:**
  - Provide logistical and administrative support to the DRT during planning and execution.
  - During a disaster:
    - Assist with documentation, record-keeping, and tracking of recovery activities.
    - Manage procurement of emergency supplies or services.
    - Coordinate meeting logistics for the DRT.
    - Help manage communication flow (e.g., answering phones, relaying messages).

2.3. Disaster Recovery Team Contact List

A comprehensive contact list for all DRT members, key stakeholders, and relevant third-party vendors must be maintained and readily accessible. This list should include multiple contact methods (e.g., office phone, mobile phone, email, home

phone if appropriate).

This list is considered highly confidential and will be included in **Appendix A: Master Contact List**. Appendix A should be regularly updated and verified. It should also be available in both electronic and physical formats, stored securely, and accessible offsite.

The Master Contact List should include:

- Internal DR Team Members (Name, Title, Role in DRT, Mobile, Email, Alternate Contact).
- Executive Management.
- Departmental Coordinators.
- Key IT Personnel not formally on the DRT but essential for recovery.
- Critical Third-Party Vendors (Company, Service, Contact Person, Phone, Email, SLA details).
    - ISP Provider
    - Cloud Service Providers (IaaS, SaaS, DRaaS)
    - Key Software Vendors (MLS, CRM, Financials)
    - Hardware Maintenance Providers
    - Telecommunications Provider
    - Data Center/Colocation Provider (if applicable)
- Emergency Services (Police, Fire, Medical).
- Utility Companies (Power, Water).
- Insurance Provider.

3. Risk Assessment and Business Impact Analysis (BIA) Summary

Understanding the potential risks to IT operations and the impact of disruptions on Metro Global Holdings Corporation's business functions is fundamental to effective disaster recovery planning. This section summarizes the key findings from the Risk Assessment and Business Impact Analysis (BIA) processes. The full Risk Assessment and BIA reports should be maintained as separate, detailed documents and reviewed regularly.

3.1. Introduction to Risk Assessment

A risk assessment is the process of identifying potential threats to Metro Global Holdings Corporation's IT assets, assessing the likelihood (probability) of those threats occurring, and evaluating the potential impact (consequences) if they do. The goal is to understand the overall risk exposure and prioritize mitigation efforts.

Key steps in the risk assessment process include:

1. **Asset Identification:** Identifying all critical IT assets (hardware, software, data, infrastructure, documentation).

2. **Threat Identification:** Identifying potential natural, man-made, and environmental threats (e.g., hardware failure, cyber-attack, power outage, fire, flood, human error).
3. **Vulnerability Assessment:** Identifying weaknesses in systems, processes, or controls that could be exploited by threats.
4. **Likelihood Assessment:** Estimating the probability of each identified threat occurring.
5. **Impact Assessment:** Evaluating the potential consequences if a threat materializes, considering financial, operational, reputational, legal, and regulatory impacts.
6. **Risk Determination:** Combining likelihood and impact to determine the level of risk for each threat/asset combination.
7. **Risk Treatment:** Identifying and implementing controls or strategies to mitigate, transfer, accept, or avoid identified risks.

The findings of the risk assessment directly inform the DR strategy by highlighting the most significant threats that the DR plan must address.

3.2. Introduction to Business Impact Analysis (BIA)

A Business Impact Analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident, or emergency. The BIA quantifies the impact of disruptions over time and helps to establish recovery priorities.

Key objectives of the BIA for Metro Global Holdings Corporation include:

1. **Identifying Critical Business Processes:** Determining which business processes are essential for the survival and continued operation of the company (e.g., property sales, client management, lease administration, financial reporting).
2. **Identifying Dependencies:** Mapping critical business processes to the IT systems, applications, data, personnel, and third-party services they depend on.
3. **Determining Impact of Disruption:** Assessing the quantitative (e.g., financial loss, penalties) and qualitative (e.g., reputational damage, loss of client trust, legal implications) impacts of a disruption to each critical business process over time.
4. **Establishing Recovery Time Objectives (RTO):** Defining the maximum acceptable downtime for each critical IT system and business process after which the impact of the disruption becomes unacceptable.
5. **Establishing Recovery Point Objectives (RPO):** Defining the maximum acceptable amount of data loss, measured in time, for each critical IT system. This dictates the required frequency of data backups.

The BIA provides the foundation for defining recovery requirements and priorities within this DR plan.

3.3. Key Business Processes for Metro Global Holdings Corporation

Based on the BIA, the following are identified as key business processes for Metro Global Holdings Corporation, critical for its operations and revenue generation. (This list should be customized based on the specific company's BIA results).

Priority	Business Process	Description	Key Departments Involved
1 (High)	Client Relationship Management	Maintaining client communication, lead generation, and service delivery.	Sales, Marketing, Support
2 (Med)	Financial Transactions & Reporting	Processing payments, commissions, payroll, and generating financial reports.	Finance, Accounting
2 (Med)	Marketing & Lead Generation	Online and offline marketing campaigns, website operations.	Marketing, Sales
3 (Low)	Internal Communications & Collaboration	Day-to-day operational communication and project management.	All Departments
3 (Low)	Human Resources & Payroll	Employee administration and payroll processing.	HR, Finance

3.4. Critical IT Systems and Applications

The BIA identifies the IT systems and applications that support the key business processes. The recovery of these systems is prioritized in the DR plan.

3.4.1. Client Relationship Management (CRM) Systems

- **Description:** Software used to manage interactions with current and potential clients, track leads, manage communication history, and automate sales and marketing workflows.
- **Impact of Loss:** Loss of client data, inability to track leads or manage client communications effectively, potential damage to client relationships.
- **Key Dependencies:** Database servers, application servers, email integration, internet connectivity.
- **Example System(s) at Metro Global Holdings Corporation:** [Specify CRM software, e.g., Salesforce, HubSpot, Top Producer, custom system]

3.4.2. Transaction Management Systems

- **Description:** Platforms used to manage the real estate transaction lifecycle, including document management, e-signatures, compliance tracking, and communication between parties (agents, clients, lawyers, lenders).
- **Impact of Loss:** Disruption to ongoing deals, inability to process paperwork or meet deadlines, potential legal and compliance issues.
- **Key Dependencies:** Application servers, database servers, document storage, e-signature services, internet connectivity.
- **Example System(s) at Metro Global Holdings Corporation:** [Specify Transaction Management software, e.g., SkySlope, DocuSign Transaction Rooms, Dotloop]

3.4.3. Financial and Accounting Systems

- **Description:** Software used for general ledger, accounts payable/receivable, commission processing, payroll, financial reporting, and trust accounting.
- **Impact of Loss:** Inability to process financial transactions, pay agents or vendors, manage trust accounts, or generate financial reports. Potential regulatory and compliance violations.
- **Key Dependencies:** Database servers, application servers, secure network access.
- **Example System(s) at Metro Global Holdings Corporation:** [Specify Accounting software, e.g., QuickBooks, Xero, Lone Wolf, Yardi]

3.4.4. Communication Systems (Email, VoIP)

- **Description:** Email servers (e.g., Microsoft Exchange, Google Workspace) and Voice over IP (VoIP) phone systems used for internal and external communication.
- **Impact of Loss:** Severe disruption to all business operations, inability to communicate with clients, agents, or partners.
- **Key Dependencies:** Email servers/cloud service, phone system servers/cloud service, internet connectivity, network infrastructure.

3.4.5. File Servers and Document Management Systems

- **Description:** Centralized storage for company documents, contracts, marketing materials, legal files, and other important electronic records.
- **Impact of Loss:** Loss of critical business records, inability to access necessary documents for operations and client service.
- **Key Dependencies:** File servers (physical/virtual), storage devices, network access, backup systems.
- **Example System(s) at Metro Global Holdings Corporation:** [Specify DMS, e.g., SharePoint, Google Drive, Dropbox, network shares]

3.4.6. Company Website and Client Portals

- **Description:** Public-facing website (e.g., Metro Global Holdings

Corporation.com) for marketing, lead generation, property search, and client portals for secure access to information.
- **Impact of Loss:** Damage to brand reputation, loss of online leads, inability for clients to access information or services.
- **Key Dependencies:** Web servers, database servers, DNS, internet connectivity.

3.4.7. Network Infrastructure

- **Description:** Core networking components including routers, switches, firewalls, wireless access points, VPNs, and internet connectivity.
- **Impact of Loss:** Complete loss of access to all IT systems and services, both internal and cloud-based.
- **Key Dependencies:** Physical hardware, power, ISP services.

3.5. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)

Based on the BIA, RTOs and RPOs have been established for critical IT systems. These objectives guide the selection of recovery strategies and the urgency of recovery efforts.

Critical System/Application	RTO (Max Acceptable Downtime)	RPO (Max Acceptable Data Loss)	Priority Tier
CRM System	4 hours	24 Hours	1
Transaction Management System	4 Hours	24 Hours	1
Financial & Accounting System (Core)	4 Hours	24 Hours	1
Email System	4 hours	24 Hours	1
VoIP Phone System	4 hours	24 Hours	1
Primary File Servers (Active Deals)	8 hours	48 Hours	2
Company Website (Lead Gen Features)	24 hours	72 Hours	2
Network Infrastructure (Core)	4 hours	24 Hours	1
Other Departmental Applications	24 hours	72 Hours	3

Priority Tiers:

- **Tier 1 (Critical):** Systems essential for immediate operations, client interaction, and revenue generation. Shortest RTOs/RPOs.
- **Tier 2 (Urgent):** Systems important for ongoing operations but can tolerate slightly longer downtime.
- **Tier 3 (Important):** Systems that support less time-sensitive functions.

3.6. Potential Threats and Vulnerabilities

The Risk Assessment identified several key threats and vulnerabilities relevant to Metro Global Holdings Corporation's IT environment.

Natural Disasters:

- Fire (at primary office or data center)
- Flood/Water Damage (internal plumbing failure, external flooding)
- Earthquake
- Severe Weather (typhoons, hurricanes, storms leading to power outages or physical damage)

Technical Failures:

- Hardware Failure (servers, storage, network devices)
- Software Corruption (operating systems, applications, databases)
- Power Outage (utility failure, internal electrical issues, UPS/generator failure)
- Telecommunications Failure (internet service provider outage, internal network failure)
- Cooling System Failure (No HVAC in server room leading to overheating)

Cyber Threats:

- Ransomware Attacks
- Malware Infections (viruses, worms, spyware)
- Phishing and Social Engineering Attacks
- Denial of Service (DoS) / Distributed Denial of Service (DDoS) Attacks
- Unauthorized Access / Data Breach
- Insider Threats (malicious or accidental)

Human Error:

- Accidental deletion or modification of data
- Incorrect system configuration
- Physical damage to equipment
- Failure to follow procedures

Other Threats:

- Theft of equipment or data
- Vandalism

- Pandemic/Epidemic (affecting staff availability and remote access needs)
- Supply Chain Disruptions (affecting replacement hardware/software)
- Loss of Key Personnel

For each identified high-risk threat, specific preventative and mitigative controls should be documented in the full Risk Assessment report and considered in the recovery strategies outlined in the next section.

4. Recovery Strategies

This section outlines the overarching strategies Metro Global Holdings Corporation will employ to recover its IT systems and data in the event of a disaster. These strategies are designed to meet the RTOs and RPOs defined in the BIA and address the identified risks.

4.1. Overview of Recovery Strategies

Metro Global Holdings Corporation's IT recovery approach is multi-faceted, incorporating a combination of preventative measures, data protection techniques, infrastructure resilience, and alternative operational capabilities. The chosen strategies aim for a balance between recovery speed, cost-effectiveness, and comprehensiveness.

Key components of our recovery strategy include:

1. **Robust Data Backup and Replication:** Ensuring that current copies of critical data are regularly backed up, stored securely offsite, and can be restored efficiently.
2. **Resilient Infrastructure:** Utilizing redundant hardware, virtualization, and potentially cloud-based resources to minimize single points of failure and facilitate quicker system recovery.
3. **Defined System Recovery Procedures:** Documented, step-by-step procedures for restoring critical applications, databases, and network services in a prioritized order.
4. **Network Redundancy and Failover:** Implementing measures to ensure continued network connectivity or rapid restoration of network services.
5. **Remote Work Capabilities:** Enabling employees to work remotely if primary office locations are inaccessible.
6. **Vendor Partnerships:** Leveraging support and services from key technology vendors and service providers.
7. **Regular Testing and Validation:** Ensuring that recovery strategies are effective and that personnel are prepared through periodic testing.

The specific strategies for different components of the IT environment are detailed below.

4.2. Data Backup and Recovery Strategy

Data is one of Metro Global Holdings Corporation's most critical assets. A comprehensive data backup and recovery strategy is essential.

4.2.1. Backup Types and Frequency

- **Full Backups:** A complete copy of all selected data.
  - Frequency: Weekly
- **Incremental/Differential Backups:** Copies of data that has changed since the last full or incremental/differential backup.
  - Frequency: Daily
- **Transaction Log Backups (for databases like SQL Server):** Captures all transactions since the last log backup.
  - Frequency: 15 Minutes
- **Cloud-to-Cloud Backups (for SaaS applications like Microsoft 365, Salesforce):** Specific backup solutions for data residing in cloud applications.
  - Frequency: Daily
- **System State Backups:** Backups of operating system configurations.
  - Frequency: Monthly

4.2.2. Backup Media and Storage

- **Primary Backup Media:** Disk-based backup appliances, Network Attached Storage (NAS)
- **Backup Software:** Windows Server Backup
- **Encryption:** All backups containing sensitive data will be encrypted with AES-256. Encryption keys will be securely managed.
- **Retention Policy:** Backup data will be retained according to a defined policy that balances recovery needs, storage costs, and regulatory requirements.

4.2.3. Offsite Backup Storage

To protect against site-wide disasters, copies of backups must be stored offsite.

- **Method 1: Cloud Backup/Replication:**
  - Description: Critical data backups are replicated to a secure cloud storage provider maintained by Alphabet.
  - Frequency of Replication: Daily
- **Method 2: Physical Offsite Storage (if applicable):**
  - Description: Physical media (e.g., tapes, external hard drives) are transported to a secure offsite location
  - Frequency of Transport: Monthly
  - Location: Baguio City, Benguet
- **Verification:** Offsite backups will be periodically tested for restorability.

4.2.4. Data Restoration Priorities

Data will be restored based on the criticality of the associated systems and business processes, as defined by the RTOs/RPOs.

1. Tier 1 System Data (CRM, Financials, Email)

2. Tier 2 System Data (File Servers, Website)
3. Tier 3 System Data

Detailed data restoration procedures for each critical system are documented in Section 8.

4.3. System Recovery Strategies

4.3.1. Hardware Redundancy

- **Servers:** Critical physical servers will have redundant components (e.g., power supplies, RAID disk configurations, network interface cards).
- **Network Devices:** Core network switches and firewalls may have redundant units or failover configurations.
- **Storage:** SANs/NAS devices will utilize RAID and potentially replication to protect against disk or controller failure.

4.3.2. Virtualization

- **Platform:** Metro Global Holdings Corporation utilizes VMware vSphere and Microsoft Hyper-V for server virtualization.
- **Benefits for DR:**
  - **Rapid Provisioning:** Virtual machines (VMs) can be quickly restored or provisioned on available hardware.
  - **Hardware Independence:** VMs are decoupled from specific physical hardware, simplifying recovery to different hardware.
  - **Snapshots:** VM snapshots can provide quick rollback points (though not a replacement for backups).
  - **Replication:** VMs can be replicated to a secondary site or cloud environment for faster failover.
- **Strategy:** Critical servers are virtualized where possible. VM backups are a core part of the data backup strategy.

4.3.3. Cloud-Based Recovery (DRaaS - Disaster Recovery as a Service)

- **Consideration:** Metro Global Holdings Corporation is evaluating the use of DRaaS solutions for certain critical systems.
- **Description (if used):** DRaaS involves replicating critical servers (physical and virtual) to a cloud provider's infrastructure. In a disaster, these systems can be failed over to run in the cloud.
- **Provider(s):** Under Evaluation
- **Scope:** Email, CRM, and Software Security

4.3.4. Cold, Warm, Hot Sites (Traditional DR Sites)

- **Current Strategy:** Metro Global Holdings Corporation currently utilizes a Cold dedicated DR site providing basic infrastructure (power, cooling, space) but no hardware. Hardware must be procured and installed.
  - **Location:** Baguio City, Benguet
  - **Testing:** The DR site and failover procedures must be tested regularly.

4.4. Network Recovery Strategy

- **Internet Redundancy:** Converge Fiber and Infinivan Fiber facilities
- **Firewall/Router Configuration Backups:** Configurations of critical network devices are backed up regularly to Alphabet.
- **VPN Access:** Secure VPN access for remote users and site-to-site connections will be restored as a priority.
- **DNS Management:** External DNS records are managed by Alphabet and can be updated to point to recovery site IP addresses if necessary. Internal DNS server recovery is prioritized.
- **Network Documentation:** Up-to-date network diagrams and configuration details are maintained and accessible.

4.5. End-User Computing Recovery

- **Standardized Configurations:** Laptops and desktops use a standard operating environment (SOE) to simplify reimaging or replacement.
- **Data Synchronization:** Users are encouraged to store critical work files on network drives or approved cloud storage (e.g., Google Drive, OneDrive, SharePoint) that are centrally backed up, rather than solely on local hard drives.
- **Loaner Equipment:** A limited pool of loaner laptops may be maintained for critical staff if their primary devices are unavailable.
- **Remote Access Software:** Ensure remote access tools (e.g., VPN client, RDP, VDI client) are available for users needing to connect from alternate locations or personal devices (only if permitted by policy).

4.6. Supplier and Vendor Dependencies

- **Critical Vendor List:** A list of critical IT vendors (hardware, software, cloud services, ISPs) with contact information and SLA details is maintained by Audit.
- **Communication:** Procedures for contacting vendors during a disaster are established.
- **SLA Review:** SLAs with critical vendors are reviewed to ensure they meet DR requirements.
- **Alternative Suppliers:** For critical hardware or services, alternative suppliers may be identified where feasible.

4.7. Alternative Workplace Strategy

If the primary office location(s) of Metro Global Holdings Corporation become uninhabitable or inaccessible, an alternative workplace strategy is required.

4.7.1. Remote Work Capabilities

- **Primary Strategy:** Metro Global Holdings Corporation's primary alternative workplace strategy is to enable employees in critical roles to work remotely from home or other suitable locations.
- **Requirements:**
    - Sufficient internet bandwidth at employee homes.

    - Secure VPN access to company resources.
    - Access to necessary applications (cloud-based or via remote access).
    - Communication tools (e.g., VoIP softphones, collaboration platforms like Microsoft Teams/Slack).
    - Company-issued laptops for key staff.
    - Clear policies and guidelines for remote work, including security requirements.
- **Capacity:** Assess the number of employees who can effectively work remotely and any limitations.

4.7.2. Alternate Office Locations

- **Reciprocal Agreements:** Metro Global Holdings Corporation has not explored reciprocal agreements with other businesses for temporary office space.
- **Flexible Office Space:** Consideration of using Regus short-term leases or co-working spaces if a physical gathering point is needed for a small team.

5. Disaster Recovery Plan Invocation

This section details the criteria and procedures for formally invoking the IT Disaster Recovery Plan. A timely and appropriate invocation is critical to minimizing the impact of a disaster.

5.1. Disaster Declaration Criteria

The decision to declare a disaster and invoke the IT DR Plan will be based on an assessment of the event's impact on critical IT systems and business operations. One or more of the following criteria may trigger a disaster declaration:

1. **Major Facility Damage:** The primary data center or main office building is rendered unusable due to fire, flood, structural damage, or other physical catastrophe.
2. **Extended Utility Outage:** Prolonged loss of essential utilities (power, cooling, telecommunications) beyond the capacity of backup systems (UPS, generators) and with no immediate prospect of restoration, exceeding [4 hours for critical systems].
3. **Critical System Failure Exceeding RTO:** One or more Tier 1 IT systems (as defined in Section 3.5) are down, and initial troubleshooting indicates that restoration within the defined RTO at the primary site is unlikely or impossible.
4. **Widespread Cyber-Attack:** A severe cyber-attack (e.g., ransomware encrypting multiple critical servers, major data breach compromising system integrity) that cannot be quickly contained and remediated at the primary site.
5. **Data Loss or Corruption:** Significant data loss or corruption affecting critical databases or file systems, where restoration from primary backups at the production site is not feasible or timely.
6. **Denial of Access:** Physical access to the primary IT facilities is denied for an

extended period due to external events (e.g., civil unrest, hazardous material spill, pandemic lockdown).

7. **Cascading Failures:** Interdependent system failures that create a widespread outage across multiple critical services.
8. **Direction from Executive Management:** Based on their assessment of the overall business risk and impact, even if specific technical thresholds are not fully met.
9. **Anticipated Prolonged Disruption:** Reliable information indicates an impending event (e.g., approaching hurricane) that is highly likely to cause a prolonged disruption meeting other declaration criteria.

The Disaster Recovery Coordinator (DRC), in consultation with the IT Management Team and relevant technical experts, will evaluate the situation against these criteria.

5.2. Invocation Authority

- **Recommendation to Invoke:** The Disaster Recovery Coordinator (DRC) or, in their absence, the designated alternate DRC or senior IT Manager present, is responsible for assessing the situation and recommending the invocation of the DR plan.
- **Final Invocation Authority:** The final authority to declare an IT disaster and formally invoke this DR Plan rests with:
  1. **Primary:** Chairman
  2. **Secondary (if Primary unavailable):** President
  3. **Tertiary (if Primary and Secondary unavailable):** ITG

5.3. Invocation Process Flow

1. **Initial Incident Detection & Alert:** An IT incident is detected by monitoring systems, staff, or users (see Section 6.1).
2. **Initial Assessment & Escalation:** The IT team on duty or the Help Desk performs an initial assessment. If the incident is severe, it is immediately escalated to the IT Management Team and the DRC.
3. **Damage and Impact Assessment (Rapid):** The DRC, with the IT Management Team and relevant Technical Recovery Teams, conducts a rapid assessment of the damage, identifies affected systems, and estimates the potential time to restore normal operations at the primary site. This involves:
   - Gathering information about the nature and extent of the event.
   - Determining which critical systems and business processes are affected.
   - Evaluating if RTOs for critical systems are likely to be breached.
   - Consulting the Disaster Declaration Criteria (Section 5.1).
4. **DRT Activation (Partial or Full):** The DRC may activate relevant members of the DRT to assist in the assessment and prepare for potential plan invocation.
5. **Recommendation to Invoke:** If the assessment indicates a disaster declaration is warranted, the DRC (or delegate) formally recommends invoking the DR plan

to the designated Invocation Authority. This recommendation should include:
    - A summary of the event.
    - Affected systems and business impacts.
    - Reasons why recovery at the primary site within RTO is unlikely.
    - Proposed recovery strategy (e.g., failover to DRaaS, activate alternate site, extensive remote work).
6. **Invocation Decision:** The Invocation Authority reviews the recommendation and makes the decision to invoke or not invoke the DR plan.
    - **If Invoked:** The Invocation Authority formally declares a disaster and authorizes the DRC to execute the IT DR Plan.
    - **If Not Invoked:** The incident is managed through standard incident response procedures or escalated operational recovery efforts. The decision and rationale are documented.
7. **Communication of Invocation:** Once invoked, the DRC, in conjunction with the Communications Team Lead, communicates the decision to:
    - All DRT members.
    - Executive Management.
    - Departmental Coordinators.
    - All employees (as appropriate, with guidance on what to expect).
    - Key third-party vendors (as needed for recovery efforts).
8. **Plan Execution:** The DRC and the DRT begin executing the recovery procedures outlined in this manual, prioritizing actions based on the RTOs of critical systems.
9. **Documentation:** All steps, decisions, and communications during the invocation process must be logged (see Appendix H for an Invocation Log Form).

5.4. Alerting and Notification Procedures

Upon confirmation of an incident that may require DR plan invocation, or upon the decision to invoke, the following alerting and notification procedures will be followed:

1. **DR Team Notification:**
    - **Method:** A multi-channel approach will be used:
        - Primary: Emergency notification system.
        - Secondary: Group SMS/text messages.
        - Tertiary: Phone call tree
        - Quaternary: Email (if systems are available).
    - **Content:** Initial notification should include:
        - Brief description of the incident.
        - Statement that DR plan invocation is being considered or has occurred.
        - Instructions for DRT members (e.g., report to a command center, join a conference call).
        - Link to or location of the DR plan.
    - **Responsibility:** DRC or designated IT Management.
2. **Executive Management Notification:**

    - **Method:** Direct phone call by the DRC or senior IT Manager to the primary Invocation Authority, followed by calls to other executives as per the agreed protocol.
    - **Content:** Summary of the situation, potential business impact, and recommendation for DR plan invocation (if applicable).
    - **Responsibility:** DRC or senior IT Manager.
3. **Departmental Coordinators Notification:**
    - **Method:** Phone call or SMS from the DRC or a designated DRT member, followed by email.
    - **Content:** Confirmation of DR plan invocation, expected impact on their departments, and instructions for communicating with their staff.
    - **Responsibility:** DRC or designated liaison.
4. **All Employee Notification (General):**
    - **Method:** Company-wide email (if available), intranet posting, emergency hotline message, or through departmental managers.
    - **Content:** General information about the IT disruption, confirmation of DR plan activation (if applicable), instructions regarding work (e.g., work remotely, await further instructions), and where to find updates.
    - **Responsibility:** Communications Team Lead, in coordination with DRC and HR.
5. **Key Vendor/Partner Notification:**
    - **Method:** Phone call or email to pre-defined vendor contacts
    - **Content:** Notification of the disaster, potential need for their support services as per SLAs, and contact person within Metro Global Holdings Corporation.
    - **Responsibility:** Relevant Technical Recovery Team Leads or DRC.

Regular updates will be provided through these channels throughout the recovery process.

5.5. Initial Damage Assessment

A rapid but thorough initial damage assessment is crucial for understanding the scope of the disaster and guiding recovery efforts. This assessment begins as soon as an incident is identified and continues until the DR plan is invoked.

Assessment Team: Led by the DRC, involving:

- IT Infrastructure Team Lead
- Network Team Lead
- Applications Team Lead
- Database Team Lead
- Facilities Manager (if physical damage to premises)
- Security Officer (if cyber-attack or physical security breach)

Assessment Steps:

1. **Confirm Safety:** Ensure the safety of personnel before attempting any physical

assessment of affected areas.
2. **Identify Nature of Disaster:** Determine the cause and type of disaster (e.g., fire, flood, power outage, ransomware).
3. **Assess Physical Infrastructure (if applicable):**
    - Inspect data center/server room for damage to hardware, power, cooling, and network cabling.
    - Check building integrity and accessibility.
4. **Assess IT Systems and Services:**
    - Identify which servers (physical and virtual) are down or affected.
    - Determine the status of storage systems (SAN, NAS) and data accessibility.
    - Check network connectivity (internal, internet, VPN).
    - Verify the status of critical applications and databases.
    - Assess the state of communication systems (email, VoIP).
5. **Estimate Scope of Impact:**
    - How many users/departments are affected?
    - Which key business processes are impacted? (Refer to Section 3.3)
    - Is data loss suspected? If so, to what extent?
6. **Estimate Time to Repair/Restore at Primary Site:**
    - Can the issue be resolved locally?
    - What resources (personnel, parts, vendor support) are needed?
    - Is restoration within RTOs feasible at the primary site?
7. **Assess Offsite Backup Status:**
    - Confirm availability and integrity of offsite backups (cloud, physical).
    - Verify accessibility of the recovery environment (DRaaS, alternate site).
8. **Identify Immediate Risks:** Are there ongoing risks (e.g., spreading malware, water damage continuing)?
9. **Document Findings:** Use an Initial Damage Assessment Form
10. **Report to DRC/Invocation Authority:** Provide a concise report to inform the DR plan invocation decision.

This assessment is iterative. As more information becomes available, the assessment will be updated. The priority is to gather enough information quickly to make an informed decision about invoking the DR plan.

6. Incident Response Procedures

While this DR Manual focuses on recovery from declared disasters, it is closely linked to the company's overall Incident Response (IR) capabilities. An effective IR process can often prevent an incident from escalating into a full-blown disaster. If an incident does escalate, the IR team's initial actions are crucial for a smooth transition to DR. This section outlines a high-level IR framework. A more detailed, standalone Incident Response Plan should exist or be developed.

6.1. Incident Detection and Reporting

Incidents can be detected through various means:

- **Automated Monitoring Systems:** Network monitoring tools, server performance alerts, security information and event management (SIEM) systems, intrusion detection/prevention systems (IDS/IPS), antivirus software.
- **User Reports:** Employees, clients, or partners reporting system unavailability, unusual system behavior, or suspected security issues via Help Desk, email, or phone.
- **IT Staff Observations:** IT personnel noticing anomalies during routine checks or operations.
- **Third-Party Notifications:** Alerts from ISPs, cloud providers, security vendors, or law enforcement.

Reporting Procedure:

1. All suspected IT incidents, regardless of perceived severity, must be reported immediately to the **IT Help Desk** at helpdesk@fiterasystems.com.
2. If the Help Desk is unavailable or the incident is deemed critical by the reporter (e.g., suspected major security breach, widespread outage), it should be escalated directly to francoramos@metroglobalholdings.com.
3. Users reporting incidents should provide as much detail as possible:
    - Their name and contact information.
    - Date and time the incident was observed.
    - Description of the incident (what happened, what systems are affected).
    - Any error messages received.
    - Impact on their work.
    - Any steps already taken.

The Help Desk or receiving IT personnel will log the incident in the Incident Tracking System Log and assign an initial priority.

6.2. Initial Response and Triage

Once an incident is reported and logged:

1. **Verification:** The IT team (Help Desk or escalated technical staff) will first verify the incident to confirm it is a genuine issue and not a user error or isolated problem.
2. **Triage and Prioritization:**
    - Assess the scope of the incident: How many users, systems, or locations are affected?
    - Determine the potential impact: What business processes are affected? Is there data loss or risk of data loss? Is there a security risk?
    - Assign/confirm priority based on severity and impact (e.g., Critical, High, Medium, Low).
3. **Incident Commander Assignment:** For significant incidents, an Incident Commander (typically an IT Manager or senior technical lead, or the DRC if it appears to be a disaster scenario) will be assigned to coordinate the response.
4. **Initial Diagnosis:** Perform a quick diagnosis to understand the nature of the

problem.

5. **Escalation (if necessary):** If the incident is beyond the capability of the initial responders or meets pre-defined escalation criteria (e.g., affects Tier 1 systems, suspected security breach), it must be escalated to:
    - Relevant Technical Recovery Teams.
    - IT Management.
    - Security Officer (for security incidents).
    - Disaster Recovery Coordinator (if disaster potential is identified).

6.3. Containment

The goal of containment is to stop the incident from spreading and prevent further damage. The specific containment strategy will vary depending on the type of incident.

- **Short-term Containment:** Immediate actions to limit the scope. Examples:
    - Isolating affected systems from the network (e.g., disconnecting network cable, blocking IP addresses at the firewall).
    - Disabling compromised user accounts.
    - Blocking malicious processes.
    - Temporarily shutting down a non-critical affected service.
- **Long-term Containment:** More permanent solutions to prevent recurrence while eradication and recovery are planned. Examples:
    - Applying temporary security patches.
    - Implementing temporary network segmentation.

Considerations during Containment:

- **Evidence Preservation:** For security incidents, containment actions should be performed in a way that preserves evidence for later forensic analysis if required. Document all actions taken.
- **Service Impact:** Balance the need for containment against the impact on critical business services.
- **DR Plan Invocation Checkpoint:** If containment is not possible or the incident is too widespread/severe, this is a key point to consider escalating to a disaster declaration (Section 5).

6.4. Eradication

Once the incident is contained, the next step is to eradicate the root cause and any remnants of the threat.

- **Identify Root Cause:** Conduct a thorough investigation to determine how the incident occurred.
- **Remove Threat:**
    - For malware: Clean infected systems using antivirus/anti-malware tools, or rebuild from a known good state.
    - For vulnerabilities: Apply patches, reconfigure systems.
    - For compromised accounts: Reset passwords, implement multi-factor

authentication.
- **System Hardening:** Improve security configurations to prevent similar incidents.

It is crucial to ensure that the threat is completely removed before moving to recovery. Restoring systems before complete eradication may lead to reinfection or recurrence.

6.5. Recovery (Link to DR Procedures)

After eradication, systems and data are restored to normal operation.

- **Restore from Backups:** If data was lost or corrupted, restore from the most recent known good backup (see Section 8 for detailed procedures).
- **Rebuild Systems:** If systems were severely compromised, they may need to be rebuilt from scratch or from gold images, then data restored.
- **Test and Validate:** Thoroughly test restored systems to ensure they are fully functional and secure. Departmental Coordinators and users should participate in UAT.
- **Monitor Systems:** Closely monitor recovered systems for any signs of recurrence or new issues.

If a disaster was declared and the DR plan invoked, this "Recovery" phase aligns with the execution of the DR plan's recovery strategies (Section 4) and system-specific procedures (Section 7). The DR plan provides the framework for recovering multiple critical systems, potentially at an alternate site.

6.6. Post-Incident Activities (Lessons Learned)

After the incident is resolved and normal operations are restored:

1. **Incident Report:** Prepare a detailed incident report, including:
    - Timeline of the incident.
    - Detection method.
    - Impact and scope.
    - Actions taken for containment, eradication, and recovery.
    - Root cause analysis.
    - Resources involved.
2. **Lessons Learned Meeting (Post-Mortem):**
    - Conduct a meeting with all involved parties (IT team, IR team, DRC if involved, relevant business stakeholders).
    - Review what happened, what went well, what could have been improved.
    - Identify gaps in procedures, tools, or training.
3. **Action Plan:** Develop an action plan to address identified weaknesses and improve future responses. This may include:
    - Updating security policies or configurations.
    - Improving monitoring capabilities.
    - Providing additional training.
    - Revising the Incident Response Plan or this DR Manual.

4. **Follow-up:** Track the implementation of action items.

This continuous improvement cycle is vital for enhancing Metro Global Holdings Corporation's resilience.

6.7. Incident Classification

Incidents should be classified to help determine the appropriate response level, communication, and reporting requirements. Classification can be based on factors like:

- **Severity/Impact:**
  - **Critical (Disaster Potential):** Widespread outage, significant data loss, major security breach, direct threat to life/safety, RTOs for Tier 1 systems likely to be exceeded. May require DR Plan invocation.
  - **High:** Significant outage affecting multiple users or a critical service, moderate data loss, contained security incident. Requires immediate attention.
  - **Medium:** Localized outage affecting a small group of users or a non-critical service, minor data loss, minor security concern.
  - **Low:** Minor issue affecting a single user or a minor system feature, no data loss.
- **Type of Incident:**
  - Denial of Service
  - Malicious Code (Virus, Worm, Ransomware)
  - Unauthorized Access
  - Data Breach / Loss of Confidentiality
  - Equipment Failure
  - Software Failure
  - User Error
  - Natural Event

A clear classification matrix should be developed as part of the detailed Incident Response Plan to guide initial assessment and escalation.

7. System-Specific Recovery Procedures

7.1. Introduction

This section is intended to house detailed, step-by-step recovery procedures for each critical IT system and application identified in Section 3.4. These procedures are the "cookbooks" that the Technical Recovery Teams will follow during a disaster.

Key Principles for System-Specific Procedures:

- **Clarity and Detail:** Procedures should be clear, concise, and detailed enough for a qualified technical team member to follow, potentially under pressure. Avoid ambiguity.
- **Accuracy:** Procedures must be kept up-to-date with current system

configurations, software versions, and recovery methods.
- **Accessibility:** These procedures must be accessible even if primary systems are down (e.g., stored in hard copy offsite, on secure cloud storage accessible via alternate means).
- **Testability:** Procedures should be designed to be testable during DR exercises.
- **Prioritization:** Recovery steps within each procedure should align with overall recovery priorities (Tier 1 first).
- **Dependencies:** Clearly note dependencies on other systems or services (e.g., "Active Directory must be available before restoring Application X").
- **Verification Steps:** Include steps to verify that the system has been successfully restored and is functioning correctly.

Metro Global Holdings Corporation IT Department is responsible for developing, maintaining, and testing these detailed procedures for all systems within their purview.

7.2. Recovery Procedure Template

Each system-specific recovery procedure should follow the standardized templates:

System Name: [e.g., Corporate Email System – Google Workspace]
System ID: [Internal System Identifier, e.g., APP-EMAIL-01]
Priority Tier: [1, 2, or 3, as per BIA]
RTO: [e.g., 2 Hours]
RPO: [e.g., 15 Minutes]
Technical Recovery Team Responsible: [e.g., Communications Systems Team]
Team Lead: [Name and Contact]
Alternate Lead: [Name and Contact]
Last Tested Date: [Date]
Last Updated Date: [Date]
1. Overview & Purpose:
* Brief description of the system and its business function.
* Purpose of this recovery procedure.
2. Recovery Strategy Summary:
* High-level approach (e.g., "Restore from replicated VMs in DRaaS environment," "Rebuild server and restore from cloud backup").
* Location of recovery (e.g., DRaaS provider, alternate site, primary site if partial disaster).
3. Prerequisites & Dependencies:
* List any other systems or services that must be recovered before this system (e.g., Active Directory, DNS, core network, SAN).
* Required access credentials (note where to find them, not the credentials themselves).
* Necessary software/media (e.g., OS installation media, application installers, license keys - note location).
* Required hardware (if rebuilding).
4. Recovery Steps (Detailed):
* Step-by-step instructions. Use clear, actionable language.
* Include specific commands, configuration settings, and GUI steps where appropriate.
* Example sub steps:

* 4.1. Verify prerequisite systems are online.
* 4.2. Provision/Access recovery hardware/VM.
* 4.3. Install Operating System (if applicable).
* 4.4. Configure network settings.
* 4.5. Install application software.
* 4.6. Restore application data from backup (refer to Section 8 for specific backup source and method).
* 4.7. Restore configurations.
* 4.8. Start services.
5. Data Restoration Specifics (Cross-reference to Section 8):
* Backup source to use (e.g., "Veeam backup repository X," "Azure Site Recovery replica").
* Specific backup job name or data set.
* Tools to use for restoration.
* Expected time for data restoration.
6. Verification & Testing:
* Steps to confirm the system is operational.
* Key functionalities to test (e.g., "Send/receive test email," "Log in to CRM and access client record").
* Performance checks.
* Involve Departmental Coordinators/Users for UAT.
7. Post-Recovery Configuration/Adjustments:
* Any settings that need to be changed after initial recovery (e.g., DNS updates, re-establishing links to other systems).
8. Troubleshooting Common Issues:
* List potential problems and their solutions.
9. Escalation Contacts:
* Key internal contacts for this system.
* Vendor support contact information and contract/SLA details.
10. Rollback Procedure (if applicable):
* Steps to revert to a previous state if recovery fails.

7.3. Example: CRM System Recovery (High-Level Outline)

System Name: Client Relationship Management (CRM) System (Google Workspace)
Priority Tier: 1
RTO: 4 Hours
RPO: 1 Hour
Technical Recovery Team Responsible: Applications Team / Database Team
1. Overview & Purpose: Manages client data, leads, communication history. Vital for sales and marketing.
2. Recovery Strategy Summary: [e.g., If SaaS: Dependent on vendor's DR. If on-prem: Restore application server VM and database from replicated backups in DRaaS/alternate site].
3. Prerequisites: Core Network, Internet, DNS, Active Directory, Database Server (if separate), Email System (for integrations).
4. Recovery Steps (assuming on-prem recovery):
* 4.1. [e.g., Provision recovery VM for CRM application server].
* 4.2. [e.g., Restore CRM database from most recent valid backup to recovery database

server].
* 4.3. [e.g., Install CRM application software on recovery VM].
* 4.4. [e.g., Configure application to connect to restored database].
* 4.5. [e.g., Restore any specific configurations or integrations (e.g., email marketing links)].
* 4.6. [e.g., Start CRM application services].
5. Data Restoration: Refer to Section 8 and Appendix B for CRM database backup details.
6. Verification:
* Sales/Marketing staff can log in.
* Can access and update client records.
* Lead tracking functions correctly.
* Email integration (if any) is working.
7. Troubleshooting: [e.g., Data inconsistencies, performance issues, integration failures].
8. Escalation: [CRM Vendor Support, Internal DB Admin, Applications Team Lead].

7.4. Example: Email System Recovery (High-Level Outline)

System Name: Corporate Email System ([e.g., Microsoft Exchange / Google Workspace])
Priority Tier: 1
RTO: 2 Hours
RPO: 15 Minutes
Technical Recovery Team Responsible: Communications Systems Team
1. Overview & Purpose: Critical for all internal and external communication.
2. Recovery Strategy Summary:
* If Cloud-based (Google Workspace/Microsoft 365): Primarily reliant on cloud provider's resilience. Focus on restoring access, DNS, and potentially recovering specific mailboxes from third-party cloud-to-cloud backup if provider outage is extensive or data loss occurs within their system.
* If On-Premise Exchange: [e.g., Activate Exchange DAG members at DR site / Restore Exchange server VMs and databases from backups].
3. Prerequisites: Core Network, Internet, DNS, Active Directory.
4. Recovery Steps (assuming on-prem Exchange recovery):
* 4.1. [e.g., Verify health of Exchange DAG members at DR site and perform switchover OR Restore Exchange server VMs from backup].
* 4.2. [e.g., Mount mailbox databases].
* 4.3. [e.g., Verify mail flow (internal and external)].
* 4.4. [e.g., Update MX records in DNS if public IPs have changed].
* 4.5. [e.g., Restore individual mailboxes/items if necessary from granular backups].
5. Data Restoration:
* Cloud: Refer to third-party cloud-to-cloud backup solution procedures.
* On-Prem: Refer to Section 8 and Appendix B for Exchange database backup details.
6. Verification:
* Users can send/receive internal and external emails.
* Outlook clients connect. Mobile devices sync.
* Calendar sharing works.
7. Troubleshooting: [e.g., Mail flow issues, database corruption, client connectivity problems].
8. Escalation: [Microsoft Support (if applicable), Internal Exchange Admin, Network Team].

8. Data Backup and Restoration Procedures (Detailed)

This section provides more detailed procedures for data restoration, complementing the system-specific recovery steps in Section 7 and the overview in Section 4.2. Effective data restoration is paramount to meeting RPOs.

8.1. General Data Restoration Principles

- **Prioritize:** Restore data for Tier 1 systems first, then Tier 2, then Tier 3.
- **Most Recent Good Backup:** Always aim to restore from the most recent backup that is known to be uncorrupted and within the RPO.
- **Point-in-Time Recovery:** For databases, utilize transaction log backups to recover to the closest possible point before the disaster, minimizing data loss.
- **Test Restorations:** Regularly test backup restoration as part of DR testing (Section 10) to ensure procedures work and RPOs can be met.
- **Secure Location:** Restoration activities, especially if involving sensitive data, must be performed in a secure environment.
- **Verification:** After any data restoration, rigorously verify data integrity and completeness. Involve business users/Departmental Coordinators.
- **Documentation:** Log all restoration activities, including backup sets used, start/end times, and any issues encountered. (Use Restoration Log Form – Appendix H).
- **Backup Software Expertise:** Ensure that personnel performing restorations are proficient with the specific backup software being used

8.2. Restoration from Local Backups (Primary Site - Partial Disaster)

This applies if the primary data center is partially operational and the disaster is localized to specific servers or data, and local backups are intact and accessible.

1. **Identify Scope:** Determine the exact data or system needing restoration.
2. **Locate Backup:** Identify the appropriate backup set (full, differential, incremental, transaction logs) on the local backup server/appliance [Specify local backup server name/IP and backup software].
3. **Isolate System (if necessary):** Prevent users from accessing the system being restored to avoid inconsistencies.
4. **Launch Backup Software Console:** Access the management console of the backup software.
5. **Select Restore Option:** Choose the appropriate restoration type (e.g., file/folder restore, VM restore, application-specific restore like SQL or Exchange).
6. **Select Source:** Specify the backup job, date/time, and specific items to restore.
7. **Select Destination:**
    - Restore to original location (overwrite existing if intended).
    - Restore to an alternate location (for verification or if original is unusable).
8. **Initiate Restore:** Start the restoration job.
9. **Monitor Progress:** Track the restoration progress through the backup software console.

10. **Verify Restoration:** Once complete, verify data integrity, file permissions, and application functionality (see Section 8.8).
11. **Communicate Completion:** Inform relevant stakeholders.

8.3. Restoration from Offsite Cloud Backups

This applies if the primary site is completely down or local backups are compromised, and cloud-based backups are the recovery source.

1. **Access Cloud Backup Portal:** Log in to the cloud backup provider's portal
2. **Identify Recovery Target Environment:**
    - If using DRaaS, this might involve failing over VMs that are already replicated.
    - If restoring to new VMs in the cloud (IaaS), provision the necessary VMs first.
    - If restoring to an alternate physical site, ensure connectivity and target servers are ready.
3. **Select Backup Set/Replication Point:** Choose the desired recovery point from the available cloud backups or replicas, respecting the RPO.
4. **Initiate Restoration/Failover:**
    - **DRaaS:** Follow the provider's procedure for initiating a failover
    - **Backup Restoration:** Select the data/VMs to restore and the target environment.
5. **Configure Network:** Adjust network configurations (IP addresses, DNS) for the recovered systems in the cloud environment.
6. **Monitor Progress:** Track via the cloud provider's console.
7. **Verify Restoration:** Once systems are up in the cloud, perform thorough verification (Section 8.8).
8. **Establish User Access:** Configure VPNs, remote access, or update public DNS to allow users to connect to the recovered systems in the cloud.

8.4. Restoration from Physical Offsite Media

This applies if physical tapes or hard drives stored offsite are the recovery source. This is generally slower than cloud-based methods.

1. **Recall Media:** Contact the offsite storage facility and request retrieval of the required backup media (specify tape numbers/labels based on backup logs).
2. **Arrange Secure Transport:** Ensure secure transportation of the media to the recovery location (alternate site or a temporary facility).
3. **Prepare Recovery Hardware:** Ensure compatible tape drives/servers are available at the recovery location.
4. **Inventory Media:** Upon arrival, inventory the received media and check for damage.
5. **Load Media:** Load tapes into drives or connect external drives.
6. **Catalog Media (if necessary):** Use the backup software to catalog the tapes/media if the catalog is not already available at the recovery site.

7. **Launch Backup Software Console:** Access the management console.
8. **Select Restore Option, Source, and Destination:** Similar to local restores, but source is the offsite media.
9. **Initiate Restore:** Start the job. This may be time-consuming.
10. **Monitor and Verify:** Track progress and verify thoroughly upon completion (Section 8.8).

8.5. Database Restoration Procedures (General)

Databases often require specific restoration steps to ensure transactional consistency.

1. **Ensure Clean Target:** The target database server should be ready (OS installed, database software installed and patched, sufficient disk space).
2. **No Users Connected:** Ensure no users or applications are attempting to connect to the database being restored.
3. **Restore Full Backup:** Using database management tools (e.g., SQL Server Management Studio, Oracle RMAN), restore the most recent full backup. Use `WITH NORECOVERY` or equivalent option if subsequent differential/log backups will be applied.
4. **Restore Differential Backup (if used):** Restore the most recent differential backup taken after the full backup. Use `WITH NORECOVERY` if log backups follow.
5. **Restore Transaction Log Backups:** Restore all subsequent transaction log backups in sequence, up to the desired point-in-time (or the last available log). The final log restoration should use `WITH RECOVERY` to bring the database online.
6. **Verify Database Integrity:** Run database consistency checks (e.g., `DBCC CHECKDB` in SQL Server).
7. **Test Application Connectivity:** Ensure applications can connect and query the database.

8.5.1. SQL Server Restoration Example (using T-SQL in SSMS)

(Specific scripts should be prepared and tested per each instance.)

```
-- Example: Restoring a database named 'RealEstateDB'

-- Step 1: Restore the latest FULL backup
RESTORE DATABASE RealEstateDB
FROM DISK = 'X:\Backups\RealEstateDB_Full_YYYYMMDD_HHMMSS.bak' -- Path to your full backup
WITH NORECOVERY, REPLACE; -- REPLACE if overwriting, NORECOVERY if applying logs
GO

-- Step 2: Restore the latest DIFFERENTIAL backup (if applicable)
RESTORE DATABASE RealEstateDB
FROM DISK = 'X:\Backups\RealEstateDB_Diff_YYYYMMDD_HHMMSS.bak' -- Path to your diff backup
WITH NORECOVERY;
GO
```

```
-- Step 3: Restore all subsequent TRANSACTION LOG backups in sequence
RESTORE LOG RealEstateDB
FROM DISK = 'X:\Backups\RealEstateDB_Log_YYYYMMDD_HHMMSS_01.trn' -- Path to log backup
WITH NORECOVERY;
GO

RESTORE LOG RealEstateDB
FROM DISK = 'X:\Backups\RealEstateDB_Log_YYYYMMDD_HHMMSS_02.trn' -- Path to next log
backup
WITH NORECOVERY;
GO

-- ... repeat for all necessary log backups ...

-- Step 4: Bring the database online with the final log restore (or if no logs after full/diff)
RESTORE DATABASE RealEstateDB
WITH RECOVERY;
GO

-- Step 5: Verify
DBCC CHECKDB ('RealEstateDB') WITH NO_INFOMSGS;
GO
```

8.6. File Server Data Restoration

1. **Identify Shares/Folders:** Determine the specific shares, folders, or files needing restoration.
2. **Use Backup Software:** Utilize the file-level restore capabilities of the backup software.
3. **Restore Permissions:** Ensure that file and folder permissions (ACLs) are restored correctly. Some backup software does this by default; verify settings.
4. **Handle Open Files (if restoring to live system):** Be aware of potential issues with restoring files that might be in use. Schedule during low activity or use tools that can handle locked files.
5. **Verify:** Check a sample of restored files for accessibility and integrity. Confirm share accessibility.

8.7. SaaS Data Restoration

Many SaaS applications have native recovery capabilities (e.g., recycle bins, version history), but these may be limited. For comprehensive protection, third-party cloud-to-cloud backup solutions are often used.

1. **Consult SaaS Provider Documentation:** Understand the provider's native data protection and recovery features first.
2. **Use Third-Party Backup Tool (if deployed):**
    - Log in to the management console of the third-party SaaS backup solution
    - Select the service to restore

    - Browse for the specific items (mailboxes, emails, files, records) and the desired recovery point.
    - Choose restore options (e.g., restore to original location, export, restore to alternate user).
    - Initiate and monitor the restore.
3. **Verify:** Confirm the data is restored correctly within the SaaS application.

8.8. Data Validation and Integrity Checks

This is a critical step after any restoration.

1. **Technical Validation (IT Team):**
    - **System Logs:** Check system and application event logs for errors.
    - **Database Consistency Checks:** Run `DBCC CHECKDB` or equivalent.
    - **File Counts/Sizes:** Compare file counts and sizes in restored directories with records from before the incident, if available.
    - **Service Status:** Ensure all related services are running.
    - **Connectivity Tests:** Verify network connectivity to and from the restored system.
2. **Business/User Validation (Departmental Coordinators & Users):**
    - **Application Functionality:** Users perform key business transactions or access critical reports.
    - **Data Accuracy:** Users check specific records or files to ensure data is current (as per RPO) and correct.
    - **Completeness:** Users confirm that expected data is present.
    - **User Acceptance Testing (UAT) Sign-off:** Obtain formal sign-off from business representatives that the restored data and system functionality meet their requirements. Use a UAT Form (Appendix H).

If validation fails, the restoration process may need to be repeated using an earlier backup or alternative methods. Document all validation steps and results.

9. DR Site and Facilities Operations

Metro Global Holdings Corporation utilizes a dedicated physical DR site (Cold) for recovery.

9.1. DR Site Activation

1. **Decision to Activate DR Site:** Made by the Invocation Authority based on DRC recommendation, typically when the primary site is unusable for an extended period.
2. **Notify DR Site Provider:** Contact the DR site provider to declare an emergency and activate the contract. Confirm site availability and access procedures.
3. **Dispatch Advance Team (if necessary):** A small team (e.g., DRC, key IT Infrastructure/Network leads, Facilities representative) may travel to the DR site to prepare for broader team arrival and system startup.
4. **Logistics for DRT:**

    - Arrange transport for DRT members to the DR site.
    - Arrange accommodation if the site is distant or recovery is expected to be prolonged.
    - Ensure DRT members have necessary access badges/credentials for the site.
5. **Establish Command Center:** Set up a temporary command center at the DR site for coordinating recovery efforts. Ensure it has basic communication (phones, internet), power, and workspace.
6. **Verify Site Readiness:**
    - Check power, cooling, and network connectivity at the DR site.
    - Verify pre-staged hardware is operational.
    - Ensure access to necessary documentation, software media, and offsite backups.

9.2. Site Management and Security

- **Access Control:** Implement strict access control to the DR site. Maintain a log of all personnel entering/leaving. Only authorized DRT members and essential support staff should be present.
- **Physical Security:** Coordinate with DR site provider security (if commercial) or implement company security protocols. Secure sensitive equipment and data.
- **Environmental Controls:** Monitor power, temperature, and humidity within the DR site's data center space.
- **Communications:** Establish reliable communication channels within the DR site and back to any remaining company personnel or external stakeholders.
- **Resource Management:** Manage allocation of workspace, computing resources, and consumables at the DR site.
- **Vendor Coordination:** Liaise with any vendors providing services or equipment at the DR site.

9.3. Logistics and Support at DR Site

- **Workspace:** Ensure adequate desks, chairs, and lighting for DRT members.
- **Network Access:** Provide network drops or secure Wi-Fi for DRT laptops.
- **Telephones:** Ensure working phones for key personnel.
- **Supplies:** Basic office supplies, refreshments, first aid.
- **Shift Management:** If recovery is prolonged, implement shift schedules for DRT members to prevent burnout. Ensure proper handovers between shifts.
- **Well-being:** Consider the well-being of staff working long hours under stress. Arrange for meals, breaks, and support.

9.4. Deactivation of DR Site and Return to Primary (Resumption)

Once the primary site is repaired and certified ready for operations, the process of returning to normal (resumption) begins. This must be carefully planned to minimize further disruption.

1. **Primary Site Certification:**

    - Facilities team confirms physical safety and environmental stability of the primary site.
    - IT team confirms repair/replacement of damaged IT infrastructure at the primary site.
    - Thorough testing of power, cooling, network, and core systems at the primary site.
2. **Resumption Plan Development:** The DRC, with the DRT, develops a detailed plan for migrating operations back to the primary site. This includes:
    - Order of system migration.
    - Data synchronization strategy (to ensure no data loss during switchback).
    - Timeline and resource allocation.
    - User communication plan.
3. **Data Synchronization/Replication:**
    - If data has been actively changing at the DR site, it must be synchronized back to the primary site systems. This might involve:
        - Restoring the latest backups from the DR site to the primary site.
        - Using replication tools to "failback" data (e.g., DRaaS failback procedures).
    - This step is critical and must ensure data consistency.
4. **System Migration (Phased Approach Recommended):**
    - Migrate systems back in a controlled, prioritized manner, often in reverse order of their recovery priority (less critical first, or by business unit).
    - Test each system thoroughly at the primary site after migration before making it live.
5. **User Cutover:**
    - Inform users of the schedule for switching back to primary systems.
    - Update DNS records, network configurations, and application pointers.
    - Provide support to users during the transition.
6. **Decommission DR Operations:**
    - Once all systems are successfully running at the primary site and validated:
        - Gracefully shut down systems at the DR site.
        - Ensure all company data is securely wiped from DR site equipment if it's shared or being returned (as per contract with provider).
        - Back up any final configurations or logs from the DR site.
7. **Notify DR Site Provider (if commercial):** Inform the provider that operations are ceasing and arrange for site checkout.
8. **DRT Stand-Down:** The DRC formally declares the end of the disaster recovery operation.
9. **Post-Resumption Review:** Conduct a review of the resumption process to identify lessons learned for future events. Update DR plan accordingly.

This resumption phase can be as complex as the initial recovery and requires careful management.

10. Plan Testing, Maintenance, and Training

A DR plan is only effective if it is regularly tested, consistently maintained, and if personnel are trained on their roles. This section outlines Metro Global Holdings Corporation's approach to these critical activities.

10.1. Testing Program Overview

Purpose of Testing:

- Validate the effectiveness and accuracy of the DR plan and procedures.
- Identify gaps, deficiencies, or outdated information in the plan.
- Train DRT members and other relevant staff on their roles and responsibilities.
- Verify the functionality of recovery systems and infrastructure (e.g., backup restorability, DR site capabilities, DRaaS failover).
- Ensure RTOs and RPOs can be met.
- Build confidence in the company's ability to recover from a disaster.
- Meet regulatory or compliance requirements for DR testing.

Testing Frequency:

- Different types of tests will be conducted at varying frequencies.
- A comprehensive test (Simulation or Parallel) should occur at least **annually**.
- Walkthroughs and checklist reviews can occur more frequently (e.g., semi-annually or quarterly).
- Specific system recovery procedures should be tested on a rotating basis.
- Testing should also occur after significant changes to IT infrastructure, applications, or the DR plan itself.

10.2. Types of DR Tests

Metro Global Holdings Corporation will utilize a variety of test types:

10.2.1. Checklist Review

- **Description:** DRT members review the DR plan document, checklists, and inventories to ensure they are accurate, complete, and up-to-date.
- **Frequency:** Annually
- **Objective:** Identify outdated contact information, incorrect configurations, missing procedures, or logical flaws without actual system impact.
- **Effort:** Low.

10.2.2. Walkthrough Test (Tabletop Exercise)

- **Description:** The DRT and other key stakeholders gather to discuss a simulated disaster scenario. They walk through the plan's response steps, discussing roles, responsibilities, procedures, and decision-making processes. No actual systems are activated.
- **Frequency:** Annually
- **Objective:** Familiarize team members with the plan, identify procedural gaps or

ambiguities, and assess coordination and communication.
- **Effort:** Low to Medium.

10.2.3. Simulation Test

- **Description:** A more active test where a disaster scenario is simulated, and recovery teams attempt to execute parts of the plan, potentially using test systems or isolated environments. This could involve actual restoration of some non-critical systems or failover to test DRaaS instances. No impact on production systems.
- **Frequency:** Annually
- **Objective:** Test the functionality of specific recovery procedures, technical capabilities of recovery solutions, and team coordination under simulated pressure.
- **Effort:** Medium to High.

10.2.4. Parallel Test

- **Description:** Critical systems are recovered and run at the DR site or in the cloud recovery environment in parallel with the production systems at the primary site. Production systems continue to operate normally. Data may be restored to the recovery systems, and business users may test functionality.
- **Frequency:** Annually
- **Objective:** Fully test the recovery environment's ability to run production workloads and meet RTOs/RPOs without impacting live operations.
- **Effort:** High.

10.2.5. Full Interruption Test (Cutover Test)

- **Description:** Production systems at the primary site are actually shut down (or disconnected), and operations are failed over to the DR site/recovery environment. This is the most comprehensive test but also carries the highest risk.
- **Frequency:** 3 years
- **Objective:** Provide the highest level of assurance that the DR plan and recovery environment will function in a real disaster.
- **Effort:** Very High. Requires significant planning, downtime window, and robust rollback plan.

10.3. Test Planning and Scheduling

1. **Annual Test Schedule:** The DRC, in consultation with IT Management and business stakeholders, will develop an annual DR test schedule outlining the types of tests, systems involved, and tentative dates.
2. **Test Plan Document:** For each significant test (Simulation, Parallel, Full Interruption), a detailed Test Plan document will be created, including:
    - Test objectives and scope.
    - Scenario description.
    - Date, time, and duration.

    - Participants and their roles.
    - Systems and procedures to be tested.
    - Success criteria (how will the test be deemed successful?).
    - Communication plan for the test.
    - Logistics (e.g., meeting rooms, conference bridges, access to DR site).
    - Risk assessment for the test itself and mitigation measures.
    - Rollback plan (how to undo test actions if needed).
3. **Approvals:** Test plans for major tests require approval from IT Management and potentially Executive Management.
4. **Notification:** All relevant stakeholders, including potentially impacted users (even for non-disruptive tests), should be notified in advance.

10.4. Test Execution and Evaluation

1. **Pre-Test Briefing:** Conduct a briefing for all participants before the test begins to review objectives, roles, and procedures.
2. **Test Execution:**
    - Follow the Test Plan.
    - The DRC or a designated Test Lead oversees the execution.
    - **Observers/Evaluators:** Appoint individuals to observe the test, record activities, note deviations from the plan, and identify issues. They should not participate directly in the recovery actions.
    - **Log All Activities:** Maintain a detailed log of actions taken, decisions made, timelines, and problems encountered (use Test Log Form - Appendix H).
3. **Problem Management:** If issues arise during the test, attempt to resolve them if possible within the test window. Document all issues and their resolutions (or lack thereof).
4. **Post-Test Debriefing (Hot Wash):** Immediately after the test, conduct a debriefing session with participants and observers to gather initial feedback, identify what went well, and what problems were encountered.

10.5. Post-Test Reporting and Remediation

1. **DR Test Report:** The DRC or Test Lead will prepare a formal DR Test Report within two weeks of the test. The report should include:
    - Summary of the test (objectives, scope, scenario).
    - Participants.
    - Execution timeline.
    - What worked well.
    - Issues identified, gaps, and deviations from the plan.
    - Analysis of whether RTOs/RPOs were met (if applicable).
    - Lessons learned.
    - Recommendations for improvement (to the DR plan, procedures, infrastructure, training).
2. **Action Plan:** Develop an action plan based on the recommendations, assigning responsibilities and deadlines for addressing identified issues.

3. **Track Remediation:** The DRC will track the implementation of corrective actions.
4. **Update DR Plan:** Incorporate necessary changes and improvements into the DR Manual and related procedural documents based on test findings.
5. **Distribute Report:** Share the Test Report and action plan with IT Management, Executive Management, and other relevant stakeholders.

10.6. Plan Maintenance and Updates

The IT DR Manual is a living document and must be kept current.

- **Scheduled Reviews:** At least annually, and after every major test or actual disaster invocation.
- **Triggered Updates:**
  - Significant changes in IT infrastructure (new critical systems, hardware/software upgrades, network changes).
  - Changes in business processes or priorities (updated BIA results).
  - Changes in key personnel (DRT members, invocation authorities).
  - Changes in vendor contracts or SLAs.
  - New threats or vulnerabilities identified.
- **Change Control Process:** (As outlined in Section 1.7) Proposed changes submitted to DRC, reviewed, approved, incorporated, version controlled, and distributed.

10.7. Training and Awareness Program

All personnel with DR responsibilities must be adequately trained. General employees also need awareness.

10.7.1. DR Team Training

- **Initial Training:** All new DRT members receive comprehensive training on the DR plan, their specific roles and responsibilities, and relevant recovery procedures.
- **Refresher Training:** Conducted annually for all DRT members to review the plan and any updates.
- **Scenario-Based Training:** Tabletop exercises and simulations serve as practical training.
- **Cross-Training:** Where feasible, cross-train team members on critical tasks to provide redundancy if key individuals are unavailable.
- **Technical Training:** Specific technical training on backup/recovery tools, DRaaS platforms, or specialized systems.

10.7.2. Employee Awareness

- **New Employee Onboarding:** Include a brief overview of business continuity and IT DR as part of new employee orientation.
- **Annual Awareness:** Provide general awareness information to all employees annually (e.g., via email, intranet, short presentations) covering:

    - Importance of DR.
    - How to report an incident.
    - What to expect during an IT disruption (e.g., communication channels, remote work procedures if applicable).
    - Their role in data protection (e.g., saving files to network drives).
- **Specific Instructions:** Provide clear instructions to employees on actions to take if the DR plan is invoked (e.g., where to find updates, how to work remotely).

10.7.3. Specialized Technical Training

IT staff responsible for executing specific recovery procedures may require specialized training from vendors or on particular technologies (e.g., database recovery, SAN administration, cloud platform management). This should be identified and budgeted for.

Training Records: Maintain records of all DR-related training completed by personnel.

END OF IT DISASTER RECOVERY MANUAL