



NAIC Climate Risk Disclosure Survey

**Group/Insurer
MCS Advantage, Inc.
MCS Life Insurance Company**

Submission Date: August 26, 2024

INDEX		
Background		3
Section 1 – CLIMATE RELATED FINANCIAL DISCLOSURES REPORT		5
	Governance	5
	Strategy	6
	Risk Management	7
	Metrics & Targets	8
Section 2 – CLOSE-ENDED QUESTIONS		10
	Governance	10
	Strategy	10
	Risk Management	10
	Metrics & Targets	11
MCS Attachment		12

Background

MCS Healthcare Holdings, LLC., a subsidiary of Medical Card System, Inc. (MCS), provides third-party administration services to its three subsidiaries, MCS Life Insurance Company (MCS Life), which in turn provide health and life insurance plans; MCS Advantage, Inc. (MCS Advantage), which in turn provide health plans; and MCS General Insurance Agency, Inc. (MCS GIA), a general agency. The subsidiaries support health insurance services to Puerto Rico's both private and public sectors.

Using a centralized operational structure, MCS's subsidiaries: MCS Advantage, MCS Life and MCS GIA, operate in the Medicare Advantage, Commercial market, and in the insurance sales segment, respectively.

MCS, a leading company in Puerto Rico's healthcare industry, provides a wide range of products and services backed by a comprehensive network comprised of 13,000 providers participating in its various programs. The company contracts and holds strong business relationships with medical groups, primary care physicians, specialists, ancillary providers, and hospitals. With over 35 years' worth of experience, the company currently has a client portfolio of over 500,000 members and is among the island's largest private-sector employers with a workforce of more than 2,200 active employees.

Organizational Structure

- Medical Card System, Inc. – The parent company of MCS.
- MCS - The parent company of MCS Life, MCS Advantage and MCS GIA that provides third-party administration services to its subsidiaries.
- MCS Life - Offers group and individual health and life insurance plans on the commercial segment.
- MCS Advantage - Through its MCS Classicare brand, this subsidiary offers Medicare Advantage products to the Medicare population plans pursuant to a contract with the Centers for Medicare and Medicaid Services (CMS).
- MCS GIA – Offers for sale a variety of life, health and disability insurance and other insurance products in the market.

MCS Advantage, Inc. (MCS Advantage)

MCS Advantage, Inc. was incorporated and authorized by the Insurance Commissioner of Puerto Rico as a Health Maintenance Organization (HMO) in 2004. In 2007, CMS authorized MCS Advantage to become a Medicare Advantage contractor/plan provider. The contracts MCS Life

had with CMS were transferred to MCS Advantage, effective January 1, 2007, through a Novation Agreement approved by CMS. MCS Advantage currently operates a Medicare Advantage plan for all 78 Puerto Rico municipalities and has over 275,000 members.

MCS Life Insurance Company (MCS Life)

MCS Life is focused on the commercial market segment, servicing this market through MCS Life. MCS Life is a duly incorporated and risk-bearing entity authorized by the Insurance Commissioner of Puerto Rico since 1994. MCS Life has a large commercial client base featuring large multinational employers, many of whom have longstanding relationships with the company. MCS Life divides its commercial business into three sub-segments: Group, Individual, and Life Insurance - determined by both the type of customer and the product marketed. Group customers can provide their employees with a choice of Preferred Provider Organization (PPO) networks ("at risk") or elect to hire the company to provide the claims and administrative support, while the customer elects to self-insure ("cost-plus"). MCS Life also has a variety of healthcare insurance products aimed at the individual market. Currently, MCS Life has over 240,000 members.

In addition, MCS Life was approved by the United States Department of Health and Human Services' (HHS) Centers for Medicare and Medicaid Services to be a Medicare Advantage contractor. A Novation Agreement, effective on January 1, 2007, transferred the CMS contracts to MCS Advantage.

Section 1 – CLIMATE RELATED FINANCIAL DISCLOSURES (TCFD) REPORT

GOVERNANCE

1. *Disclose the insurer's governance around climate-related risks and opportunities.*

In disclosing the insurer's governance around climate-related risks and opportunities insurers should consider including the following:

- Identify and include any publicly stated goals on climate-related risks and opportunities.
- Describe where climate-related disclosure is handled within the insurer's structure, e.g., at a group level, entity level, or a combination. If handled at the group level, describe what activities are undertaken at the company level.

A. *Describe the board and/or committee responsible for the oversight of climate-related risks and opportunities.*

- MCS's Board of Directors oversees MCS's business strategy. Our Board works with management to consider specific issues relevant to the overall conduct of our businesses, including strategy, emerging challenges and enterprise risks, safety, sustainability, culture, financial performance, and other strategic alliances. Our Board and company are focused on corporate responsibility efforts and meeting the needs of all our stakeholders– our employees, our customers and suppliers, our communities, and our shareholders.
- The Board convenes at least four times per year, but unscheduled meetings may be called at any time to address specific needs of MCS. Additionally, a yearly strategy meeting occurs where climate-related risks and opportunities may be part of the discussion. Committee structures are created to facilitate and assist in the execution of the Board's responsibilities. At each regular meeting of the Board, the committees are required to report significant matters reviewed by the committee and matters considered and acted upon.
- MCS has an Emergency Management Committee, whose members oversee the development and implementation of strategic decisions and the management of everything related to the approval, request, and discharge of the logistical, administrative, and financial resources during an emergency. The Committee is comprised by the Chief Operating Officer, Chief Administrative Officer, Senior VP of Information and Technology, Human Resources VP, Facilities Director, VP of Corporate Communications, and Controller.

In describing the position on the board and/or committee responsible for the oversight of managing the climate-related financial risks, insurers should consider including the following:

- Describe the position on the board and/or committee responsible for the oversight of managing the climate-related financial risks.

B. *Describe management's role in assessing and managing climate-related risks and opportunities.*

Refer to Question 1A.

STRATEGY

2. *Disclose the actual and potential impacts of climate-related risks and opportunities on the insurer's businesses, strategy, and financial planning where such information is material.*

In disclosing the actual and potential impacts of climate-related risks and opportunities on the insurer's businesses, strategy and financial planning, insurers should consider including the following:

- Describe the steps the insurer has taken to engage key constituencies on the topic of climate risk and resiliency.
- Describe the insurer's plan to assess, reduce, or mitigate its greenhouse gas emissions in its operations or organizations.
 - Working in partnership with our landlords and vendors evaluating potential energy consumption reduction initiatives that implies less use of energy derive from fossil fuels and to promote renewable energy use.

A. Describe the climate-related risks and opportunities the insurer has identified over the short, medium, and long term.

MCS invests in business continuity efforts that contribute to mitigating the potential for risk of loss and promote business continuity in the event a climate-related risk materializes.

- Short Term, Acute Physical - Increased severity and frequency of extreme weather events (i.e., cyclones, hurricanes, or floods). Although the sites are not in areas of high direct physical risk, fires may cause business disruption associated with power outages and smoke. MCS offices are in Puerto Rico, where there is an increased risk of stronger hurricanes. This could result in business disruption, as well as decreased asset value or asset useful life, leading to write-offs or asset impairments. In addition to impacting to our leased facilities, acute climate-related physical risks may cause business disruption through our supply chain and logistics functions.
- Medium Term, Emerging Regulation – Carbon Pricing Mechanisms: Potential regulations on energy, in particular carbon, may result in increased cost of energy used to support our operations and increased cost if we are not successful at limiting the associated emissions.
- Long Term, Chronic Physical – Rising Sea Levels: Though MCS has facilities in coastal regions, the sites are not in areas where there is high direct physical risk.

In describing the climate-related risks and opportunities the insurer has identified over the short, medium, and longer term, insurers should consider including the following:

- Define short, medium, and long-term, if different than 1-5years as short term, 5-10years as medium term, and 10-30 years as long term.

B. Describe the impact of climate-related risks and opportunities on the insurer's business, strategy, and financial planning.

- The climate-related risks that have been identified would not alter that mission for the benefit of both current and future members. Climate-related risks, however, inform how we evaluate our operations and supply chains for potential disruptions in connection with climate changes, implement contingency plans, and advance our preparedness. MCS has invested in business continuity efforts aimed at mitigating the potential for risk of loss and promoting business continuity in the event a climate-related risk materializes. The financial impact of these activities is evaluated within our annual and long-range financial planning cycles.

In describing the impact of climate-related risks and opportunities on the insurer's business, strategy, and financial planning, insurers should consider including the following:

- Discuss if and how the insurer provides products or services to support the transition to a low carbon economy or helps customers adapt to climate-related risk.
- Discuss if and how the insurer makes investments to support the transition to a low carbon economy.
 - Working in partnership with vendors that help us provide solutions to reduce carbon emissions. MCS is currently part of a local leading operator of electric vehicle charger station around the island. With MCS investing through this local supplier by installing vehicle chargers in our Service Center. With this partnership, MCS is part of a network that is currently support in a cumulative (since 2021) reduction of 411,855 pounds of Carbon Dioxide.

C. Describe the resilience of the insurer's strategy, taking into consideration different climate-related scenarios, including a 2 degree Celsius or lower scenario.

- MCS have a better understanding of short-, medium- and long-term risks associated with climate-related risks. MCS identified the increased severity of climate-related weather events as having the potential to impact operations and supply chain. Our strategy has been influenced by climate-related risks informing the increased importance to tracking and monitoring severe weather events in real-time, to maintain business continuity. Weather events may not only impact MCS, but also the partners we rely on within MCS's supply chain. To mitigate climate-related disruptions to MCS's supply chain, MCS works with its supply chain partners to ensure they have robust continuity plans and makes investments itself in assurance of supply activities. This investment includes, but is not limited to, obtaining redundant suppliers for raw materials.

RISK MANAGEMENT

3. Disclose how the insurer identifies, assesses, and manages climate-related risks. In disclosing how the insurer identifies, assesses, and manages climate-related risks, insurers should consider including the following:

- Describe how the insurer considers the impact of climate related risks on its underwriting portfolio, and how the company is managing its underwriting exposure with respect to physical, transition and liability risk.
- Describe any steps the insurer has taken to encourage policyholders to manage their potential physical and transition climate related risks, if applicable.
- Describe how the insurer has considered the impact of climate-related risks on its investment portfolio, including what investment classes have been considered.

A. Describe the insurers' processes for identifying and assessing climate-related risks.

In describing the insurers' processes for identifying and assessing climate-related risks, insurers should consider including the following:

- Discuss whether the process includes an assessment of financial implications and how frequently the process is completed.

Climate risks are integrated within the broader risk management framework. Some potential risks are identified through the development of the Emergency Response Plan (ERP). See **Exhibit 1**. The ERP is revised annually.

MCS' strategy has been influenced by climate-related risks informing the increase importance to tracking and monitoring severe climate-related events in real-time to maintain business continuity. Risks relating to emerging federal and state regulations around climate related risks are also considered.

B. Describe the insurer's processes for managing climate-related risks.

The potentially most significant risks for the Company are prioritized for mitigation through EMC strategic planning efforts. We have enterprise-wide risk mitigation protocols for physical climate-related risks from extreme weather, including with critical vendors and suppliers. During active situations, risks and threats are tracked in real time. Through business continuity measures, our resources are quickly shifted to alternative hubs to reduce the risk and impact of business interruptions and manage climate-related physical risks.

C. Describe how processes for identifying, assessing, and managing climate-related risks are integrated into the insurer's overall risk management.

Our EMC regularly evaluates risks to our operational footprint, including our physical assets and colleagues, as well as risks within our supply chain. We prioritize mitigation efforts based on the importance of the issue to the business, stakeholders, and the potential financial impact on the Company. Other major considerations include number of assets, employees, and customers potentially affected.

In describing how processes for identifying, assessing, and managing climate-related risks are integrated into the insurer's overall risk management, insurers should consider including the following:

- Discuss whether climate-related risks are addressed through the insurer's general enterprise-risk management process or a separate process and how frequently the process is completed.
- Discuss the climate scenarios utilized by the insurer to analyze its underwriting risks, including which risk factors the scenarios consider, what types of scenarios are used, and what timeframes are considered.
- Discuss the climate scenarios utilized by the insurer to analyze risks on its investments, including which risk factors are utilized, what types of scenarios are used, and what timeframes are considered.

METRICS AND TARGETS

- 4. Disclose the metrics and targets used to assess and manage relevant collateralized risks and opportunities where such information is material.*

In disclosing the metrics and targets used to assess and manage relevant collateralized risks and opportunities where such information is material, insurers should consider including the following:

- Discuss how the insurer uses catastrophe modeling to manage the climate-related risks to your business. Please specify for which climate-related risks the insurer uses catastrophe models to assess, if any. In order to measure and manage risk of write-offs and early retirement of existing assets (e.g., damage to property and assets in “high-risk” locations) the following metrics are tracked:
- Number and proportion of high-risk sites (critical infrastructure and retail sites) with exposure to hurricanes, flooding.
- Proportion of square footage of high-risk sites ((critical infrastructure and retail sites) with exposure to hurricanes, flooding

A. Disclose the metrics used by the insurer to assess climate-related risks and opportunities in line with its strategy and risk management process.

In disclosing the metrics used by the insurer to assess climate-related risks and opportunities in line with its strategy and risk management process, insurers should consider including the following:

- In describing the metrics used by the insurer to assess and monitor climate risks, consider the amount of exposure to business lines, sectors, and geographies vulnerable to climate-related physical risks [answer in absolute amounts and percentages if possible], alignment with climate scenarios, [1 in 100 years probable maximum loss, Climate VaR, carbon intensity], and the amount of financed or underwritten carbon emissions)

Water

To evaluate our exposure to water-related risks we track:

- Number of critical infrastructure sites with high risk of severe hurricanes or flooding
- Number of retail sites with high risk of severe hurricanes or flooding

Energy

To evaluate our exposure to energy-related risks we track:

- Total energy consumption
- % Grid electricity: 100%
- Cost per kWh, Rate of change

B. Disclose Scope 1, Scope 2, and if appropriate, Scope 3 greenhouse gas (GHG) emissions, and the related risks.

No Applicable

C. Describe the targets used by the insurer to manage climate-related risks and opportunities and performance against targets.

Our goal is to mitigate potential asset impairment due to hurricane-induced flooding. We do this through adequate insurance coverage for all Company sites with a reasonable deductible. Risks are currently well mitigated through insurance, resulting in estimated residual risk.

Section 2 – Close-Ended Questions

Closed-ended questions directly correspond to the narrative above, allowing for explanation and qualification of the yes/no answers. Closed-ended questions are voluntary for reporting year 2024 and individual states may elect not to request them.

Governance

- Does the insurer have publicly stated goals on climate-related risks and opportunities? (Y/N)
 - No
- Does your board have a member, members, a committee, or committees responsible for the oversight of managing the climate-related financial risk? (Y/N)
 - Not Applicable
- Does management have a role in assessing climate-related risks and opportunities? (Y/N)
 - Not Applicable
- Does management have a role in managing climate-related risks and opportunities? (Y/N)
 - Not Applicable

Strategy

- Has the insurer taken steps to engage key constituencies on the topic of climate risk and resiliency? (Y/N)
 - Not Applicable
- Does the insurer provide products or services to support the transition to a low carbon economy or help customers adapt to climate risk? (Y/N)
 - Not Applicable
- Does the insurer make investments to support the transition to a low carbon economy? (Y/N)
 - Not Applicable
- Does the insurer have a plan to assess, reduce or mitigate its greenhouse gas emissions in its operations or organizations? (Y/N)
 - Not Applicable

Risk Management

- Does the insurer have a process for identifying climate-related risks? (Y/N)
 - Yes
 - If yes, are climate-related risks addressed through the insurer's general enterprise-risk management process? (Y/N)
 - Yes, MCS Emergency Management Committee
- Does the insurer have a process for assessing climate-related risks? (Y/N)
 - Yes
 - If yes, does the process include an assessment of financial implications? (Y/N)
 - See, Exhibit 1. The Emergency Response Plan is revised annually.

- Does the insurer have a process for managing climate-related risks? (Y/N)
 - Yes
- Has the insurer considered the impact of climate-related risks on its underwriting portfolio? (Y/N/Not Applicable)
 - Not Applicable
- Has the insurer taken steps to encourage policyholders to manage their potential climate-related risks? (Y/N)
 - Not Applicable
- Has the insurer considered the impact of climate-related risks on its investment portfolio? (Y/N)
 - Not Applicable
- Has the insurer utilized climate scenarios to analyze their underwriting risk? (Y/N)
 - Not Applicable
- Has the insurer utilized climate scenarios to analyze their investment risk? (Y/N)
 - Not Applicable

Metrics and Targets

- Does the insurer use catastrophe modeling to manage your climate-related risks? (Y/N)
 - Not Applicable
- Does the insurer use metrics to assess and monitor climate-related risks? (Y/N)
 - Not Applicable
- Does the insurer have targets to manage climate-related risks and opportunities? (Y/N)
 - Not Applicable
- Does the insurer have targets to manage climate-related performance? (Y/N)
 - Not Applicable

MCS Attachment

- a. Emergency Response Plan - Exhibit 1



Emergency Response Plan

Prepared by:



June 18, 2024

REVISION HISTORY:

Date	Version	Description	Author
08/31/2022	1.0	Initial Plan	JL.Navedo, C.Solis
03/07/2023	1.1	Plan Revision	JL.Navedo, C.Solis
03/12/2024	1.2	Plan Revision	JL. Navedo, R. Jordan
06/18/2024	1.3	Contacts update	Jose Serrant, Javier Santiago

APPROVALS:


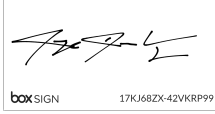

MCS Management			
		 <div style="text-align: right;">Jun 21, 2024</div>	
Gannett Ramos Arzuaga		Signature	Date
Chief Information Officer Incident Commander			
		 <div style="text-align: right;">Jun 21, 2024</div>	
Jorge Torres Vargas		Signature	Date
Business Continuity Officer			
Business Continuity Professionals, Inc			
		 <div style="text-align: right;">Jun 21, 2024</div>	
José Luis Navedo, CBCP		Signature	Date
President & CEO Certified Business Continuity Profesional			

Table of Contents

1.0 INTRODUCTION	5
1.1. Scope	5
1.2. Objectives	5
1.3. Methodology	5
1.4. Policy	6
1.4.1. Definitions:	6
1.4.2 Responsibilities:	6
1.5. MCS - Business Continuity Structure	7
2.0 INCIDENT MANAGEMENT TEAM (IMT)	8
2.1. Purpose	8
2.5. Initial Incident Management Team Activation and Notification Procedures	11
2.5.1 Notification and Escalation Process	11
2.6 Event Severities	13
3.0 EMERGENCY RESPONSE PROCEDURES & DISASTER DECLARATION	15
3.1. Emergency Action Teams and Their Responsibilities	15
3.1.1. Organization and Planning	15
3.1.2 Facilities - Team Members – Contact Information	15
3.1.3 Business Continuity Coordinator – Facilities Team	15
3.2. Notification of The Facilities Team	18
3.3. Initial Readiness Procedures	18
4.0 FACILITY CONTROLS	19
4.1. INTRUSION DETECTION EQUIPMENT AND SECURITY DEVICES	19
4.2. Closed Circuit TV (CCTV) Operations and Surveillance Cameras	19
4.3. Access Controls	19
4.3.1. Access Control Systems	20
4.4.2. Vendors/Contractors/Maintenance Personnel	21
4.4.3. Visitors	21
4.4.4. Search Inspections	22
5.0 KEY AND LOCK CONTROL	22
5.1. Key Control and Inventory	22
5.1.1. Master Inventory	24
5.1.2. Duplicate Keys	24
5.2. Cipher Lock Operations	24
5.2.1. Cipher Lock Code Security	24
5.2.2. Special Use	24
6.0 FIRE PREVENTION AND DETECTION	25
6.1. Fire Prevention	25
6.2. Fire Detection	25
6.3 Fire Emergency Response	26
7.0 GUARD FORCE OPERATIONS	26
7.1. General Guard Force Responsibilities	27

7.2. Communications Protocol	27
7.3. Responding to Alarms or Incidents	27
7.4. Use of Force	27
8.0 SECURITY SITUATIONS UNDER EMERGENCY	27
8.1. Operations	27
9.0 MAINTENANCE RECORD.....	29
9.1 Equipment Maintenance	29
9.2 Cipher door release mechanism	29
10. RECOVERY BY SCENARIOS	29
10.1. During Each Incident	30
10.2. After Each Incident	30
10.3. Business Unit Plans	31
10.3.1. Building Premises Evacuation Plan	31
10.4. Loss of Workplace Scenario.....	38
10.5. Major Regional Event and/or Loss of Utilities Scenario	40
10.6. Pandemic Scenario.....	43
11.0 Checklist	45
11.1. Earthquakes	45
11.2. Fire.....	48
11.3. Floods	51
11.4. Hurricanes	52
11.5. Bomb Threat.....	55
11.6. Hazardous Materials.....	56
11.7. Power Outages.....	58
11.8. Vital Records Storage	60
11.9. Incident Response Checklist.....	62
11.10. Event Log.....	62
11.11. Incident Notification Form	63
11.12. Damage Assessment Checklist	64
Appendix A. Associated Sites	65
Appendix B. Checklists & Forms	65
Appendix C. Alternate Site Protocol & Facility Inspection sheet	65
Appendix D. Associated Relationships.....	65
Appendix E. Electrical and Mechanical Drawings.....	66
Appendix F. Glossary	67

1.0 INTRODUCTION

Medical Card Systems (MCS) is committed to its customers, employees, stakeholders, and suppliers. To ensure people's adequate safety and the availability of essential products and services, MCS establishes this Business Continuity Management Governance to support a comprehensive program for incident response, business continuity, disaster recovery, and business recovery.

The MCS's Emergency Recovery Plan is designed to provide immediate response and subsequent recovery from unplanned emergency interruption that affects the safety of employees or any of the physical facilities of MCS. A centralized team called the Incident Management Team would oversee response and recovery activities and support the recovery at the facility affected. This Emergency Recovery Plan provides the strategies, resources, and procedures required to recover short- or long-term facility interruption. Emergency response personnel should refer to their Standard Operating Procedures for specific response procedures.

1.1. Scope

This Emergency Response plan has been developed to ensure an orderly and effective response to any incident that significantly disrupts any MCS operating facilities. An incident may include one or a combination of any of the following:

- Any major regional event, like natural disasters (e.g., earthquake, storm, tsunami, flood, hurricane, among others);
- Loss of Workplace or lack of critical resources (e.g., power, water, office facilities, supplies).
- Loss of Telecommunications

Any other scenario will be responded to by adapting the procedures for the above scenarios. The plan documents the emergency response procedures MCS's Incident Management Team followed when preparing for, responding to, and recovering from such incidents.

1.2. Objectives

The specific objectives of this emergency response plan are to:

- Establish responsibilities, policies, and procedures for safeguarding personnel, materials, and facilities from natural and environmental hazards and unauthorized intrusion within the facilities of Medical Card System, Inc., as well as compliance with HIPAA Security Standards.

1.3. Methodology

The Emergency Response Plan was developed following the professional practices of the Disaster Recovery Institute International (DRII).

1.4. Policy

MCS shall assign resources with specific roles and responsibilities to develop and oversee the emergency response plan in compliance with the business continuity management program.

1.4.1. Definitions:

- **Business Continuity Planning (BCP):** An organization's risk management strategy for threats that may terminate or significantly disrupt core business. It involves mitigation activities and contingency planning for response and recovery actions. (Note: BC planning necessarily embraces disaster recovery and incident management planning.)
- **Business Continuity Program:** An ongoing funded process supported by senior management, comprising all business continuity planning, plans, arrangements, practices, and processes to achieve required business continuity outcomes in compliance with business continuity aims and agreed expectations.
- **Emergency Response Plan:** An emergency response plan is a documented series of steps an organization will take during a critical event to ensure employees' safety and minimize the impact on critical operations. Every emergency management professional will tell you that the best time to prepare for an emergency is well before it occurs.

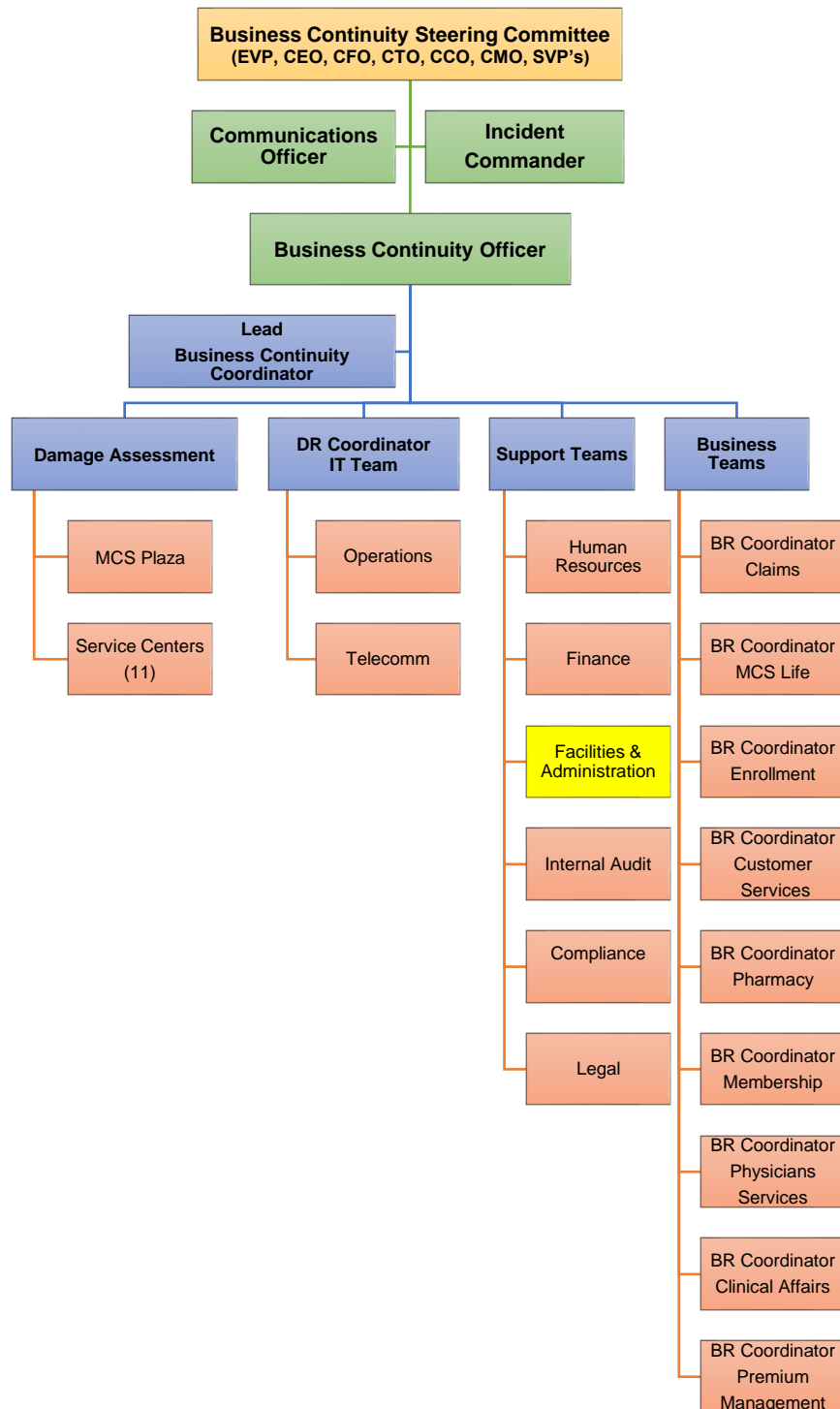
1.4.2 Responsibilities:

MCS has defined the Incident Management Team (IMT) as the person responsible for executing the Incident Management process for MCS.

MCS responds promptly to emergencies or events threatening its business continuity and communicates effectively with employees, customers, and the media, if necessary, through various communication devices and methods. All employees, volunteers, trainees, and temporary workers must comply with this policy.

1.5. MCS - Business Continuity Structure

The following diagram presents the structure of MCS Business Continuity to address corporate incidents.



This Business Continuity Structure should be reviewed and updated once any positions change. The Business Continuity Officer will be responsible for making the changes.

All Business Continuity Coordinators must adjust their Business Unit Incident Management Structure to the Corporates Incident Management Structure.

The Business Continuity Steering Committee includes the following members:

Business Continuity Steering Committee	
Executives	Contact Number
Jim O'Drobinak	(813) 766-1083
Gannett Ramos	(787) 642-2721
Roberto Torres	(787) 645-7221
Jose Aponte	(787) 231-5767
Ines Hernandez	(787) 646-7832
Jorge Torres	(787) 600-7580
Jose Serrant	(787) 903-3417
Maite Morales	(787) 667-1063

2.0 INCIDENT MANAGEMENT TEAM (IMT)

An Incident Management Team (IMT) is a designated group of senior executives responsible for managing a potentially disastrous event (also known as a Crisis Management Team). The Incident Management Team establishes lines of supervisory authority and formal reporting relationships. Direction and supervision always follow selected organizational lines.

2.1. Purpose

The purpose of the Incident Management Process is to simplify the decision-making process by defining the following:

- The incident management structure;
- Potential consequences of different crisis 'scenarios';
- Available options for responding to the different scenarios;
- Any predetermined 'deadlines' for crucial decisions.

2.2. MCS - Incident Management Structure

This Incident Management structure will become operational in the event of an incident that could affect the operations of MCS.



The Business Continuity and Incident Management Structure should be reviewed and updated once positions change. The Business Continuity Coordinator will be responsible for updating their Incident Management Structure.

2.3. Incident Command Center

An Incident Command Center is established in a significant disaster, where all communications and activities will be directed. The Incident Command Center is used to coordinate the management of recovery procedures. It will center all interactions among the Incident Commander, Business Continuity Officer, the Action Teams, and other personnel. The administration of the Incident Command Center is the responsibility of the Business Continuity Officer.

1. The Incident Command Center is activated when a significant disaster has occurred, significantly when employees' safety or property is jeopardized. The Business Continuity Officer's responsibility and the management of activities and communications from the Incident Command Center are the Incident Command Center's readiness and activation.
2. This center will provide centralized and coordinated communications control during emergencies. When the Incident Command Center is in operation, the Incident Commander, Business Continuity Coordinators, and Action Team Leaders will coordinate their activities through the center and keep informed of their status and progress.
3. If conditions warrant the MCS Main Office Building's closing, the Incident Command Center will communicate the closing notice through the management chain to all employees.

Of an incident that requires the activation of the Incident Management Team, the team members, as needed, report to the assigned command center.

It has established an **MCS Incident Hotline (787) 522-8300**, in which the MCS official releases will be issued in the event of an incident that disrupts the operations for a term of more than three (3) hours. The following locations have been established as command centers for incidents:

Designated Command Centers / WorkPlace:

Centro de Comando	Localización	Capacidad	Contacto	Teléfono
Vivela Main Room	Lobby MCS Plaza	45	Javier Santiago	787-396-8929
Vivela 5	Lobby MCS Plaza	10	Javier Santiago	787-396-8929
Happy Room	MCS Plaza – 2 nd Floor	32	Javier Santiago	787-396-8929
C S Bayamón	Bayamon	38	Joan Panel	787-370-4105
C S Carolina	Carolina	40	Orlando Irizarry	787-504-2214
C S Caguas	Caguas	18	Yanira Lopez	787-397-0158
Academia	Anexo – 2 nd Floor	30	Javier Santiago	787-396-8929

2.4. Corporate Business Continuity Strategies

MCS has developed various strategies to ensure recovery from any major disaster. The Disaster Recovery (IT) Plan establishes the framework to be followed if a major disaster strikes the data center operations. The Emergency Response Plan sets the structure to be followed if a major catastrophe strikes any physical location.

MCS's Incident Commander will issue a disaster recovery declaration if a disaster occurs. The Incident Management Team will agree with the strategy of the relocation of operations at a local level.

Move to an Alternate Location

Regarding functions that could be performed by staff working from an alternate location, the Facilities developed a protocol to determine the relocation of operations to alternative facilities to provide continuity to the business lines. Exceptions would be considered achieved by each Business Recovery Team.

The purpose of this protocol is to maintain the operations of the corporate group's business lines if atmospheric events, disasters, or other causes do not allow services in a particular MCS location. Different MCS locations were identified as alternatives to transfer and give continuity to the business lines' operations.

These alternative facilities must have a generator, water tank, communications infrastructure, and safety systems. Also, they must be located at strategic points throughout the island. The following Service Centers have been identified as alternate locations.

Physical Address – Service Centers

MCS Central Plaza	Ave. Ponce de Leon 1st floor
<i>Aguadilla</i>	Aguadilla Mall, State Rd. #2 Km. 126.5,
<i>Arecibo</i>	Galería Pacífico, Bo. Tanamá Carr. 10
<i>Bayamón</i>	San Miguel Plaza Building 2 Las Rosas
<i>Caguas</i>	Calle Marginal Carr. 1 Km. 33.3 Bo.
<i>Carolina</i>	Escorial Office Building I. Parque Escorial
<i>Fajardo</i>	Local I Ralph Food Warehouse, Carr.3,
<i>Guayama</i>	Condominio Commerce Plaza #1 Carr. 3,
<i>Manatí</i>	Centro Plaza Carr. 2, Local 6
<i>Mayagüez</i>	Santander Securities Plaza Bldg., #349
<i>Ponce</i>	Ave. Tito Castro 601 Carr. 14 Km. 4.2, Ste.
<i>Plaza Las Americas</i>	Second Floor Suite 511-513

Service Centers – Contact Information

Service Centers	Manager	Contact Number	Ext.	Fax	Cell Phone Number
Hato Rey	Maricelly Cruz	787-758-2500	5100/5101	787-620-0980	787-396-0355
Aguadilla	Migdalia Hernández	787-758-2500	5470/5471	787-882-6844	787-436-3562
Mayaguez	Daliana Santaliz	787-758-2500	5768/5712	787-805-6415 787-805-3815	787-402-4492
Carolina	Orlando Irizarry	787-758-2500	5630/5635	787-620-6340	787-504-2214
Ponce	Jorge Maldonado	787-758-2500	5550/5551	787-290-1730	787-378-9349
Arecibo	Roberto Vega	787-758-2500	5500/5513	787-200-2863	787-685-4738
Caguas	Yanira López	787-758-2500	5402/5427		787-397-0158
Fajardo	Abimael Cepeda	787-758-2500	5670/5671	787-622-2464	787-664-0389
Bayamon	Hector Vazquez	787-758-2500	5308/5112	787-200-2874	787-628-8876
Manatí	Yolanda Ruiz Diaz	787-758-2500	5600/5601	787-200-2864	787-502-1056
Guayama	Ana Morales Velez	787-758-2500	5706/5707	787-864-1225	787-664-0365

AVP & General Managers - Customer Services	Contact Number	Ext.	Cell Phone Number
Rosadaliz Berrios Colon	787-758-2500	5240	787-221-0661
Rebecca Melendez (General Manager)	787-758-2500	5602	787-565-3121
Ibis Echevarria (General Manager)	787-758-2500	5767	787-216-2391

In addition to the alternate locations mentioned above, MCS may use any other internal facility to access the Internet for its operations. The Facilities Team will determine team member relocation from the primary to an alternate location.

2.5. Initial Incident Management Team Activation and Notification Procedures

2.5.1 Notification and Escalation Process

The following individuals can contact the Incident Commander to activate the Incident Management Plan:

1. Incident Management Team (IMT) Members – Any IMT Member can contact the Incident Commander to request activation.
2. Business Continuity Officer (BCO) – Will contact the Incident Commander to alert any IT events interrupting any critical business process's regular operation.
3. Facilities AVP – Will notify the Incident Commander of any events that impact any MCS locations (leading site & service center), causing the loss of resources and services.

Notification Procedures:

The initial contact will be made with the Business Continuity Coordinator. The Business Continuity Coordinator may contact the Incident Commander for additional consultation. Activation will occur for all events that impact MCS's primary site, service centers, and IT Platforms that exceed the recovery time objective of any critical business processes.

The notification messages must be consistent. It is recommended that a script is written before the team is notified containing:

- Type of incident / Area Affected
- Outage start time / Current status if known / Teams Activated
- Incident Response Activation / Numbers

2.5.1.2 Activation Criteria

When considering IMT activation criteria, it is impossible to predict all possible scenarios that may occur. Many events occur with associated measures, levels, or categories that assist local authorities in determining severity. IMT Criteria to use to determine the severity should be:

- Safety of Building
- Technology Events outside the normal operation scope
- The impact on infrastructure and Personnel

The Incident Management Team (IMT) will review the current events, impact, and assessment details. Alternate team members will be activated in the absence of the primary representatives.

2.5.1.3 Activation – Incident Management Team

The Incident Management Team (IMT) provides immediate support before, during, and after events. The IMT activation is managed through the Incident Commander. IMT activations will occur during any threat to staff, operations, or environmental emergencies within any MCS location.

This IMT will be responsible for the staff and visitors' safe evacuation, assessing damage to the site, and communicating with supporting departments after all restoration activities are coordinated through the IMT members. The IMT must be notified and activated to oversee incidents in significant incidents. The IMT manages disaster response, recovery, restoration, provisioning support, and funding requirements.

All Business Units will provide updates to the IMT as requested. The IMT Membership includes the following:

Incident Management Team

Name	Position	Contact Numbers
Maite Morales	Chief Administration Officer	(787) 667-1063
Jose Aponte	CFO	(787) 231-5767
Roberto Torres	COO	(787) 645-7221
Gannett Ramos	CIO, Incident Commander	(787) 642-2721
Jorge Torres	Business Continuity Officer	(787) 600-7580
Jose Serrant	Facilities AVP	(787) 903-3417
Lourdes Perez	Corporate Communications Officer	(787) 758-2500 ext 3881
Briseida Torres	Human Resources VP	(787) 955-4599

2.6 Event Severities

Event Severities – Level 1- Level 4.

The following are the severity levels defined by the MCS Incident Management Structure to estimate the impact on MCS following an incident. The MCS Business Continuity program will take different actions depending on the Incident Severity Level. There are 4 Incident Severity Levels:

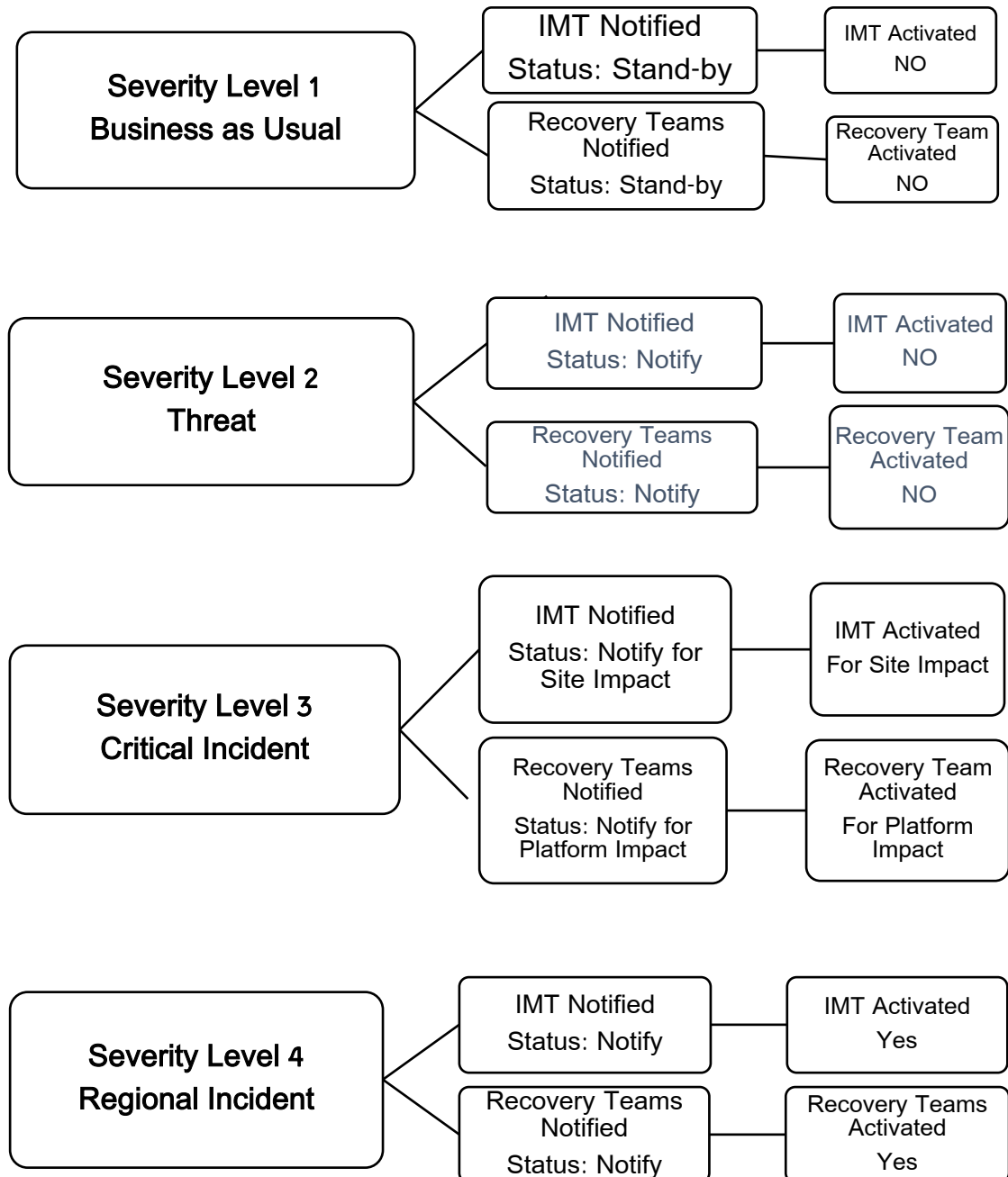
1. **Level 1 – Business as Usual (BAU)** – Within acceptable operational parameters, permitting outages to occur during the ordinary course of business - BAU. MCS regularly operates at Level 1 unless circumstances dictate a change to an escalated level.
2. **Level 2 –Threat:** An escalation of the standard operating procedures resulting from identifying a potential threat to MCS personnel, operations, community, and national security. Impending threats typically have forewarning and require close monitoring and communications by the IMT until the threat either subsides or occurs; in this case, it will be assigned an increased Incident Severity Level.
3. **Level 3 – Critical Incident (0 - 24 Hours):** An incident disrupting IT platforms or impacting multiple MCS locations requires immediate support resources, and incident management ensures the timely resumption of normal operations. These local events usually cause interruption of normal operations with the potential of additional impact.
4. **Level 4 – Regional Incident (More than 24 hours):** An incident of such magnitude as to cause a severe impact to (a) human life/safety of many MCS employees; (b) national security; (c) MCS's ability to continue doing business as an ongoing concern.

The IMT activates the Incident Management Structure following the MCS's declaration of a Level 4 incident. (Examples: Major Hurricane, loss of operational site, major transportation issues impacting staff, multiple areas affected by one or more events simultaneously, National or Global crisis, corporate-wide systems virus, Human infectious outbreak, etc.)

Severity Team Activations

Other Recovery Teams will operate independently of this plan. The status of activations, deployments, and actual recovery should be maintained with the IMT.

Recovery Teams Activation / Notification by Severity Level



3.0 EMERGENCY RESPONSE PROCEDURES & DISASTER DECLARATION

3.1. Emergency Action Teams and Their Responsibilities

Emergency Response Plan

An Emergency Response Plan (ERP) is developing procedures in advance that enable an organization to respond to a disaster. This process would include actions such as warnings, command and control, evacuation, and shutdown.

We have incorporated essential emergency response procedures into this Business Recovery Plan.

3.1.1. Organization and Planning

The Business Continuity Team comprises a Business Continuity Coordinator, an Alternate Business Continuity Coordinator, and other designated individuals.

The responsibilities of individuals assigned to the Business Recovery Team included their regular assignments and were made by familiarity and competence in their respective areas or specialties.

The Emergency Response Plan facilitates the response to various types of emergencies. We discussed the Business Continuity Coordinators' responsibilities and the Incident Management Team's functions in the following sub-sections.

3.1.2 Facilities - Team Members – Contact Information

Name	Position	Contact Numbers
Jose Serrant	Facilities AVP	(787) 903-3417
Javier Santiago	Facilities Manager	(787) 396-8929
Nitza Camacho	Team Member	(787) 233-2188
Richard Luquis	Team Member	(787) 396-4655

Any problem related to MCS Plaza facilities will be handled through the Facilities Team. Below is the contact information for the MCS Plaza administration.

MCS Plaza – Administration Contact Information

Name	Position	Contact Numbers
Jose Dubon	Executive Vice President D Group Equities Management Corp.	(787) 553-9020
Carlos Salico	Facilities Engineer/Superintendent Bldg D Group Equities Management Corp.	(787) 553-9025
Ramon Maldonado	Electrical Supervisor D Group Equities Management Corp.	(787) 553-9044

3.1.3 Business Continuity Coordinator – Facilities Team

The Business Continuity Coordinator of the Facilities Team is responsible for developing and coordinating its Business Recovery Plan. During an incident, the

Business Continuity Coordinator will activate and direct all activities until the incident is under control. Additionally, the Business Continuity Coordinator is responsible for the following:

1. Reviewing, evaluating, and updating the Business Recovery Plan in RPX. At least every year, the Facilities Team assures that all emergencies have been adequately considered and that appropriate contingency plans have been prepared.
2. Ensure the business recovery teams and other employees receive proper emergency plan and procedure training. This will routinely be done as a part of the periodic tests of the Business Continuity Plan. The Business Continuity Coordinator will also ensure that new employees in their Business Unit have the proper training and that specific emergency procedures are reviewed as frequently as necessary.
3. Conduct meetings with the Alternate Business Continuity Coordinator and the Incident Management Team as necessary.
4. Keeping all members of the Incident Management Team fully briefed on all aspects of the Business Recovery Plan.
5. Monitoring all tests of their Business Recovery Plan and recording the progress, problems, and successes.
6. Evaluate the appropriateness of each Business Recovery Team's readiness, proficiency, and assignments.
7. Keeping the Business Continuity Officer informed of the Business Recovery Team's status and business recovery plan.
8. Communicate the status of emergencies to senior management promptly and efficiently.
9. Maintain active communication with local fire and police agencies, other MCS locations, and parties involved.

In the event of a hurricane or any other event that can be anticipated, the Business Continuity Coordinator will ascertain that all preparation tasks and activities are coordinated based on the occasion.

Facilities Team

Purpose

The Facilities Team will establish and direct plans of action to follow during an interruption or cessation of services caused by a disaster emergency. As the name implies, the Facilities Team maintains emergency readiness through the BCP. The Facilities Team is also responsible for managing the business recovery activities following a disaster and can be considered the “emergency management team.” Through the emergency plans, the Facilities Team will provide for the following:

- The safety of personnel,
- The protection of property,
- The continuation of the business.

Responsibilities

- Maintain current facility configurations as an Appendix to the Plan or as part of supporting documentation. The arrangements should include spacious layouts, a list of all facilities such as air conditioning, power distribution, specifications of model numbers, capacities, electrical requirements, etc.
- In the event of a disaster, assess the damage and recoverability of the facilities. If the facility is usable, proceed to organize immediate repairs.
- If the facilities are destroyed and unusable, locate replacement facilities that can be acquired quickly and are usable for a reasonably long period, if not permanently. Again, facilities include requisite square footage in a building and cabling, air conditioning, power, etc.
- Coordinate with property owners to provide necessary facilities - buildup equipment, installation, and permits on an incident basis. As much as possible, negotiate contingency plans.
- Coordinate with finance, insurance, and other departments to order new equipment, contract space and buildup, make insurance claims, and finance the new facilities.

3.2. Notification of The Facilities Team

A critical aspect of disaster recovery is the quick reaction of the Facilities Team. This requires immediate notification of appropriate personnel to initiate the Business Continuity Plan (Disaster Recovery + Business Recovery Plans) as quickly as possible.

The Business Continuity Coordinator has established and will maintain an Incident Notification List and ensure all essential personnel is available. In the event of a disaster, the following notification procedures will be followed:

Procedures

- If the disaster occurs while the personnel is on duty, they should initiate the notification process immediately. Operations staff are required to have updated the list of emergency telephone numbers in RPX. Nevertheless, all emergency telephone numbers should be posted in a visible location through the Intranet. If the personnel are off duty, then the building security provided with a proper procedure should notify them.
- The Business Continuity Coordinator is at the top of the Notification List.
- The first member of the Facilities Team notified is responsible for informing all other critical members and initiating action. The initial response will be to assemble the team at the Incident Command Centers, depending on the disaster's nature and extent.

3.3. Initial Readiness Procedures

Once the Facilities Team has been notified, they must immediately assess the situation and initiate appropriate actions.

Procedures

Suppose the Business Continuity Coordinator has yet to be reached. In that case, the Alternate persons listed next on the Incident Notification List will assume the Business Continuity Coordinator's full responsibilities until they arrive and have been fully briefed. The Business Continuity Coordinator or Acting Coordinator will implement the contingency plans.

The team should assess the situation directly at the scene or based on reported information from the notification sources. Based on the evaluation of the case, determine the severity of the problem and decide on the appropriate action. If the Facilities Team judges the incident to be a significant disaster, proceed to do the following:

- Activate the Incident Command Center
- Notify the proper Incident Management Team
- Notify the Business Continuity Steering Committee
- Notify the Alternate Site or Sites

These steps constitute the activation of the contingency plans for a major disaster. Additional procedures for these tasks are provided on the following pages. The appropriate correction or contingency plans will be implemented if the incident is not considered a major disaster. In such a case, if required, notify the selected Recovery Teams.

Activation of the Incident Command Center

The Business Continuity Officer's first task is establishing an Incident Command Center. The Incident Command Center should be near the Main Office Building. It can be in another office or another building in your complex. A nearby hotel may provide excellent accommodations if something is not available or usable.

During that period, the Command Center should be close to other departments in your organization for maximum communication.

The **MCS Incident Hotline (787) 522-8300** should be available to all departments and users to channel all information through the center.

Notification of Alternate Site

Activating business recovery plans will require retrieving documentation and supplies and establishing operations at alternate sites. However, to expedite the initial recovery process, the Facilities Team will notify the alternate sites of a disaster and activate the Business Recovery Plans.

Procedures

The Alternate Sites have been provided with written procedures to follow when notified that Business Recovery Plans for an emergency have been implemented.

Notify the Alternate Sites that a disaster has occurred, which requires activation of contingency operations. The standing contingency procedures should specify the alternate sites expected to take before the Business Recovery Teams' arrival.

3.4. Facilities Salvage or Replacement by Facilities Team

These procedures cover the salvage or replacement of the Main Office Building facilities under the Facilities Team's jurisdiction.

- Immediate contact with the Facilities AVP is necessary to establish new site arrangements.

4.0 FACILITY CONTROLS

This section defines standard security devices and procedures that Medical Card System, Inc. employs to protect its employees, customers, and other people, facilities, assets, and records.

Any suggested improvement and/or addition of security devices shall be informed to the Facilities AVP for study and recommendation. The IT Senior VP will be involved if security devices pertain to information systems.

4.1. INTRUSION DETECTION EQUIPMENT AND SECURITY DEVICES

System Description

The building alarm will be activated when a physical threat is imminent, in progress, or if a scheduled drill is taking place. Protecting cash or other assets, such as a vault, safe, or secure space, will be required. These devices shall meet the minimum standards outlined in all applicable regulations.

All work areas are separated from customer areas, and all walk-through doors between these areas shall be secured during business hours. These devices shall meet the minimum standards outlined in all applicable regulations.

The Building Administration will have a surveillance system for all areas open to the public and other common areas considered appropriate. It will raise any proper action in case of an attempted or completed crime or unauthorized entry. Alarms, intrusion detection systems, and CCTV systems are located, controlled, and monitored by the building's Administration.

A copy of the Access Register Report (generated by the alarm system Contractor) will be forwarded to the Facilities Specialist for auditing purposes in regional offices. In case of any intrusion or access violation, the Human Resources Department will be alerted along with the Chief Administrative Officer and any other proper authority. Every regional office defines a predefined escalation notification and emergency response alert.

All incidents will be documented. Refer to Reporting and Recording Requirements – Section 1.9.

An Alarm/Intrusion Detection Record will be completed and forwarded with information regarding the Intrusion Detection Equipment operation status available in the Computer Room area. It will include the following information:

- Date of the spot check
- Time of the spot check
- Person performing a spot check
- Area being verified
- Remarks

The Project Engineer manages the hardware system maintenance.

4.2 Closed Circuit TV (CCTV) Operations and Surveillance Cameras

Closed-circuit television cameras can be used as a part of the facility security system by Building's Administration.

4.3 Access Controls

The following section describes the existing al and administrative security mechanism controls to prevent unauthorized entry into restricted areas of the facilities, data storage, and other support areas in Medical Card System, Inc.

4.3.1. Access Control Systems

Key/ID/Access Card controls are implemented to delineate which personnel can access specific areas.

Formal guidelines for computer security should be in place for all Medical Card System, Inc. facilities. All file servers are in a locked room denominated as the Data Center.

All information technology systems and devices will be located inside restricted areas, and only authorized personnel will have access to this equipment. Locks, locking devices, and key control systems should be inspected continuously, and malfunctioning equipment repaired or replaced. All employees/vendors/contractors/maintenance employees must always wear a proper ID.

4.4. Facility Access

4.4.1 Employees

- Medical Card System, Inc. must establish and implement appropriate procedures to control and validate employees' access to all facilities that store electronically protected health information (EPHI) systems.
- All employees should always wear their employee photo ID when performing duties for Medical Card System, Inc.
- Employees will be responsible for verifying that no office door is left or propped open, especially after hours. Any employee who finds them available should close them immediately. Employees who have been issued keys to permit access after-hours should never duplicate these keys nor give these keys to non-employee or non-authorized personnel.
- Failure to comply with this statement will result in disciplinary actions based on policies and procedures established by the Human Resources Department.

4.4.2. Vendors/Contractors/Maintenance Personnel

- Medical Card System, Inc. will always provide tags and will be required to wear them. Vendors' and contractors' visits should be scheduled in advance. All vendors and contractors must always be escorted.
- Access lists that preauthorize regular contractors and vendors to enter are permitted in charge of the daily schedule requirements. Policy ADM _ COMPRAS - 008

4.4.3. Visitors

- Medical Card System, Inc. must establish and implement mechanisms to control, validate, and document visitor access to any facility that houses electronically protected health information (EPHI) systems.
- All visitors who request access to facilities containing electronically protected health information (EPHI) systems must sign in to the log and provide information regarding their identity and the purpose of their visit. The Logs are safeguarded and stored with the Dead File Administration Company for five years.
- All visitors must be provided with a visitor's badge. While in the facility, all visitors must always place this ID in a visible location on their clothes.

- All visitors must be escorted to and from their destination. Visitors should be scheduled in advance. If not, the entry should be denied until proper authorization.
- All visitors after work hours will not be allowed unless proper authorization is provided before the visit.

4.4.4. Search Inspections

- All search inspections are performed to prevent unauthorized possession of equipment, materials, or any other Medical Card System, Inc. property by employees or outside personnel.
- All cubicles, desks, offices, vehicles, file cabinets, and exempt and non-exempt personnel packages could be subject to search inspections. All search inspections will be made randomly and/or based on probable cause. The employee/visitor/contractor must be present whenever possible during the examination.
- All personnel will give their full cooperation during these searches. Any employee refusing to cooperate will be subject to disciplinary actions, including employment termination. For additional information, refer to the MCS Employee Policy and Procedure Manual.

5.0 KEY AND LOCK CONTROL

This section aims to establish security controls and logistics over the Medical Card System, Inc.'s keys to prevent unauthorized personnel from accessing restricted areas, data storage, and other support areas throughout the building.

5.1. Key Control and Inventory

All activity keys and locks will be stringently always controlled and accounted for. The minimum standard measures described herein are to be applied in every case. Specific procedures include:

- The facilities' specialties will generate a key inventory.
- Specific keys to secure Medical Card System, Inc. property accessible only to authorized individuals will remain locked in the activity key depository and properly signed out as needed to authorize personnel.
- Combinations of padlocks and safe locks will be strictly controlled and protected to prevent loss or compromise. Specific procedures are as follows.
- The combined information will be available inside the key depository out of direct view whenever the key repository is open.

- Combinations will be changed annually or when necessary; this includes but is not limited to compromise of the combination or whenever an individual with access to the container is no longer assigned to the activity.
- A recorded copy of the Padlocks and Safe Locks Combination Registry will be sealed in an envelope in such a manner as to allow easy detection of any attempt to open the envelope. The sealed envelope containing combinations to padlocks will be secured with the key control Facilities Specialties or at the next higher activity.
- Master keys will have Facilities Specialties, Facilities Technician, Facilities Manager, and Facilities AVP. There will be only four (4) sets of Master keys. A spare master key will be in a combination box for emergencies outside our everyday work. This combination box number will only have the Facilities Department and any time it is divulged, this combination will automatically change within 24 hours.
- Office locks will be used to secure or protect Medical Card System, Inc.'s property. The Department Manager will only retain and distribute such keys to authorized personnel as needed.
- Custodians and alternates shall be responsible for the proper accounting and security of all keys for the activity. Individuals appointed as key Custodians or alternates and those authorized to issue or receipt keys shall have access to all keys and associated secured areas within the movement. Therefore, the reliability and trustworthiness of appointed and qualified individuals must be considered.
- Under no circumstances will personnel who have been relieved of employment or are subject to or pending disciplinary action be assigned duties with unaccompanied access to an activity or unit keys and property.
- The number of personnel authorized to possess (personally retained keys) and use keys will be limited to employees with an absolute need, as determined by the Department Supervisor/Manager/Director responsible for the activity. Persons designated to access a key system, or separate keys, will be identified in writing.
- When not in use, all keys will be secured by the person to whom they were assigned or attached to the key storage. Keys shall not be left in the keyway of the locking device or in any fashion to permit easy access from unauthorized use. The key storage will be in a room kept under surveillance around the clock or in a room that can be securely locked during work and non-working hours.

5.1.1. Master Inventory

All keys to locking devices used to secure or protect Medical Card System, Inc. will always be accounted for. A complete written inventory of all keys by assigned number and location will be maintained on the Key Inventory Registry.

5.1.2. Duplicate Keys

All keys (offices, doors, etc.) will be allowed to be duplicated with the prior written authorization of the Facilities AVP. All keys should be marked with a "Do Not Copy" sign.

5.2. Cipher Lock Operations

The locking mechanism is one of the essential safeguards to protect employees, customers, and other people, as well as facilities, assets, and records.

Cipher (push button) locks should be limited to controlling access in secure areas and should not be considered for use as security locks. Cipher locks can be used with electric release latches. Doors utilizing this type of lock should have an automatic door-closing mechanism. The electrical cipher lock should also be fitted with a keyed bypass lock to allow access in the event of power failure.

Medical Card System, Inc. should provide this type of security to sensitive areas identified by the Facilities AVP and the Chief Administrative Officer.

5.2.1. Cipher Lock Code Security

Medical Card System, Inc. uses cipher locks on doors to control access to various entry points to the office and other access points within the facility. This cipher lock security mechanism will be administered by the Administration & Facilities Department, and only authorized personnel will access the cipher code. A list of all authorized users will be maintained and updated as needed. The Facilities AVP will have copies of cipher lock codes whenever they are changed.

5.2.2. Special Use

Cipher locks will be permitted as a convenience item and approved on a case-by-case basis by the Facilities AVP; in those cases where information systems are involved, the IT Senior VP will be contacted for approval.

Cipher locks will be allowed when it is necessary to isolate significant visitors waiting for areas from administrative areas that require separation due to sensitive material or mobility processing activities and temporary facilities. Cipher locks on exterior doors must include a timeout tamper function that delays the code entry after an incorrect code. Requests for cipher systems will be submitted to the Project Engineer/Facilities Supervisor; when information systems are involved, the IT Senior VP will be contacted for approval before installation on any facility.

6.0 FIRE PREVENTION AND DETECTION

This section aims to ensure that the appropriate safeguards are implemented to prevent, detect, and suppress fires and protect Medical Card System, Inc. assets in the event of a fire.

Medical Card System, Inc. is committed to preventing fire occurrences or any other situation that may promote a fire at the facility. Fire prevention is the responsibility of all Medical Card System, Inc. personnel.

Employees should follow safe practices to minimize fire hazards, and Supervisors must ensure that safe practices are tracked daily, and will inspect their work areas daily as a fire prevention initiative and report any situation promptly to the Health and Occupational Safety Committee and the Facilities AVP for corrective action.

The Health and Occupational Safety Committee is an established committee with delegates in all Medical Card System, Inc. departments. The committee and the Project Engineer/Facilities Supervisor will address all fire incidents accordingly.

6.1. Fire Prevention

Take preventive measures to minimize the threat of fires, such as keeping all equipment rooms clear of trash and unnecessary supplies and enforcing a prohibition on smoking.

All fire protection equipment will be inspected annually by the Facilities AVP. When Fire Department inspections occur, the Building Administration Representative will coordinate these inspections with the Facilities AVP and Specialist to ensure proper facility access and controls.

The Facilities AVP will provide a copy of the certification and maintain a secure location.

No unusual fire hazards exist at this Medical Card System, Inc., and its regional offices. Particular emphasis is placed on housekeeping and storage practices.

Listed below are specific procedures that shall be addressed by the facility to minimize the occurrence and impact of a fire emergency.

1. There is a no-smoking policy in the facilities. Candles or any other flammable substance are prohibited within the facilities.
2. The facility is committed to preventing fires and situations that may promote a fire at the premises.
3. Fire prevention is the responsibility of all facility personnel.
4. Employees should follow safe practices to minimize fire hazards, and Supervisors must ensure that safe practices are followed daily.
5. An authorized agent will inspect all fire protection equipment annually. The results of these inspections will be provided to the Facilities AVP.

6.2 Fire Detection

Smoker fire detection equipment is installed in the main office building to ensure early detection of fires. All alarms are connected to a central alarm station or fire station. The Building's Administrator manages this system.

In case of fire detection, pursue the following steps:

1. Always be aware of the locations of all fire extinguishers.
2. Any person discovering a fire will contact its immediate Supervisor, Facilities Specialist, Facilities AVP, Building Administration, and Health and Occupational Safety Committee member.
3. All employees should evacuate the building and follow pre-established procedures from the Health and Occupational Safety Program and the Evacuation Plan.
4. Avoid panic, remain calm, and move with assurance.
5. Proceed with the procedure stated in the Emergency Management Procedure.

6.3 Fire Emergency Response

Identify equipment for emergency power shutdown and air conditioning during a fire or other emergencies and ensure that overhead lighting is not shut down. Provide covers or other protective measures for emergency power controls and fire alarm switches to prevent accidental activations. The Emergency Management Procedure and the Evacuation Plan must be activated.

To provide for the safety of employees and visitors, it is essential that early warning of emergencies be made so that evacuation procedures can be implemented and emergency response organizations are notified of the situation.

Evacuation of employees and visitors from the facility is of the utmost importance.

Most emergencies will require the evacuation of all or part of the facility. To achieve a safe and timely evacuation, it is critical that an early warning of the emergency be communicated to personnel and that action be implemented to remove personnel from the hazard area, as well as continuous drill or exercise practices.

7.0 GUARD FORCE OPERATIONS

This section aims to design a secure physical environment to prevent unauthorized intrusion, damage, and interference to business premises and ensure that the appropriate safeguards are implemented to protect Medical Card System, Inc. personnel, visitors, material, and facilities.

Physical protection measures, physical barriers, and intrusion detectors ultimately depend on human intervention.

7.1. General Guard Force Responsibilities

The Building's Administrator is responsible for providing and administering contract guard services at MCS Plaza's main office building to supplement security systems and/or law

enforcement personnel. This service is at the Administrator's discretion and for general building security. Medical Card System, Inc. administers additional contracted security services for satellite offices.

The Facilities AVP will receive communication if an illegal entry or security incident is suspected in any of the Medical Card System, Inc. areas. When an employee is involved, the Human Resources Department will be contacted and proceed with the procedures.

7.2. Communications Protocol

- A Security Communication Flowchart between the Administrator and Medical Card
- The systems are in place and become active should an emergency occur.

7.3. Responding to Alarms or Incidents

An Evacuation Plan is provided to all employees upon hiring. Medical Card System, Inc. identified a Security Committee with defined strategies by the building's security plan for responding to major emergencies and/or disasters.

7.4. Use of Force

Medical Card System, Inc. does not promote using force within its premises. This statement also includes the private official guards contracted for specific sites. In those cases where human life, property, or any reasonable doubts deserve this kind of intervention, notification to the proper authorities as the "Policía de Puerto Rico" may be placed.

8.0 SECURITY SITUATIONS UNDER EMERGENCY

The purpose of this section is to demonstrate the most common guidelines used in security under emergencies. For this reason, it is essential to follow these guidelines:

8.1. Operations

The facilities specialist will oversee the emergency at the Medical Card System, Inc.'s central and regional offices. Without the facilities specialist, the emergency management responsibilities are delegated to the Facility's AVP. Each Department needs a Committee Member in charge of emergency management responsibilities and designated backup staff.

The Evacuation Plan ("Plan de Desalojo") shall be reviewed periodically for modifications to the procedures, changes of key personnel or other resources, and additions of new emergency management information.

The Human Resources Leader shall control the Evacuation Plan ("Plan de Desalojo") to ensure appropriate updates, changes, and reviews are incorporated in all distributed

copies of this plan. A copy of the plan shall be maintained and posted in the following areas:

- Document Number - Position
- FSP-1 Chief Executive Officer
- FSP-2 Facilities AVP
- FSP-3 IT Senior VP
- FSP-4 MCS Life & MCS HMO President
- FSP-5 Chief Operational Officer
- FSP-6 Human Resources Leader.

In an emergency, the Facilities AVP and/or the Health and Occupational Safety Committee shall declare an emergency and institute the appropriate response actions. If the Facilities AVP is unavailable, the next person in authority shall assume the responsibilities.

- Work with the building's Administration and local emergency agencies to arrange evacuation locations and transportation away from the building.
- Familiarize all staff with the crisis/emergency response Evacuation Plan and ensure effective implementation.
- Ensure that the building's practice drill program is implemented at least once a year and documented.
- Ensure supplies and equipment are present and checked at least monthly.
- Review each crisis/emergency to ensure accurate reports are completed, and appropriate action is taken to prevent the repetition of ineffective efforts.
- Act as Team Leader in a crisis/emergency. Identify the emergency and determine the course of action.
- Try to remain calm. Follow pre-define evacuation instructions and help any disabled person during an evacuation.
- Contact the buildings and/or other local authorities to inform the main office building of potential or existing crises/emergencies.

All lobbies and common areas should have the floor/plan diagram outlining the primary and secondary evacuation routes from that location and denoting the location of all fire extinguishers (red dots) and pull stations (blue squares). Also, a narrative description of the emergency plans is to be posted.

The emergency shut-off for the HVAC system, water supply, and electric service shall have a sign placed by the control identifying it as the primary disconnecting/shutoff means. This information will be available in the Building's Administration office.

Refer to the Standard Operating Procedures listed in Coordination with Local Enforcement and Emergency Management Officials - Section 1.8 for additional information related to security incidents.

9.0 MAINTENANCE RECORD

This section demonstrates that the building's and MCS equipment are inspected and certified.

9.1 Equipment Maintenance

Yearly equipment maintenance will be required to be inspected and certified by the Building's Administrator, Third Party Companies, and MCS Facilities Technician. The Facilities AVP will keep a record of such certifications on file.

1. Equipment Maintained by the Building's Administrator on common areas at MCS Plaza, Main Lobbies on each floor, Emergency Stairs, Hallways, Elevators, and Restrooms will include but are not limited to the following:
 - a. Fire Extinguishers
 - b. Smoke Detectors
 - c. Fire Alarm System
 - d. Emergency Lights
 - e. Emergency Generators
 - f. Air Conditioning System at MCS Plaza
2. Equipment Maintained by Third Party Companies on the premises, usable areas of Medical Card System, Inc. will include, but are not limited to, the following:
 - a. Fire Extinguishers
 - b. Emergency Lights
 - c. Air Conditioning System at Annex, 11th & 16th floor and Computer Room
 - d. Automated External Defibrillators
3. MCS Facilities Technician or Project Engineer will inspect all areas in the facility to check the following unsafe conditions:
 - a. Blocked or locked fire exits
 - b. Poor housekeeping procedures
 - c. Obstructed access to electrical rooms and panels

9.2 Cipher door release mechanism

Third-Party Company provides services on-premises, usable areas of Medical Card System, Inc upon request.

10. RECOVERY BY SCENARIOS

10.1. During Each Incident

At all stages, keep any affected business unit or person jointly advised of progress – even negative development. Do not hesitate to notify any member of the Incident Management Team of the incident and progress.

The following table contains a list of the Business Recovery Scenarios that could be executed in the event of an incident.

Incidents	<i>Business Recovery Scenarios</i>				
	<i>Loss of IT</i>	<i>Loss of Workplace</i>	<i>Regional Event</i>	<i>Loss of Workforce</i>	<i>Pandemic</i>
Earthquake	X	X	X	X	
Fire	X	X	X	X	
Hurricane	X	X	X	X	
Bomb Threat		X	X		
Hazardous Materials		X	X		
Power Outages	X	X	X		
Vital Records		X	X		
Operational Deficiency	X	X		X	X

10.2. After Each Incident

After every incident, a standard set of tasks must be done. These have not been repeated under each risk, but they must still be done:

- Return all operations and services to their original form.
- Contact all affected business units and suppliers to advise them that the incident is over and back to normal.
- Thank everyone involved, preferably by a personal phone call or email.
- Review how the incident was managed and consider any necessary changes; if so, they must be documented.

10.3. Business Unit Plans

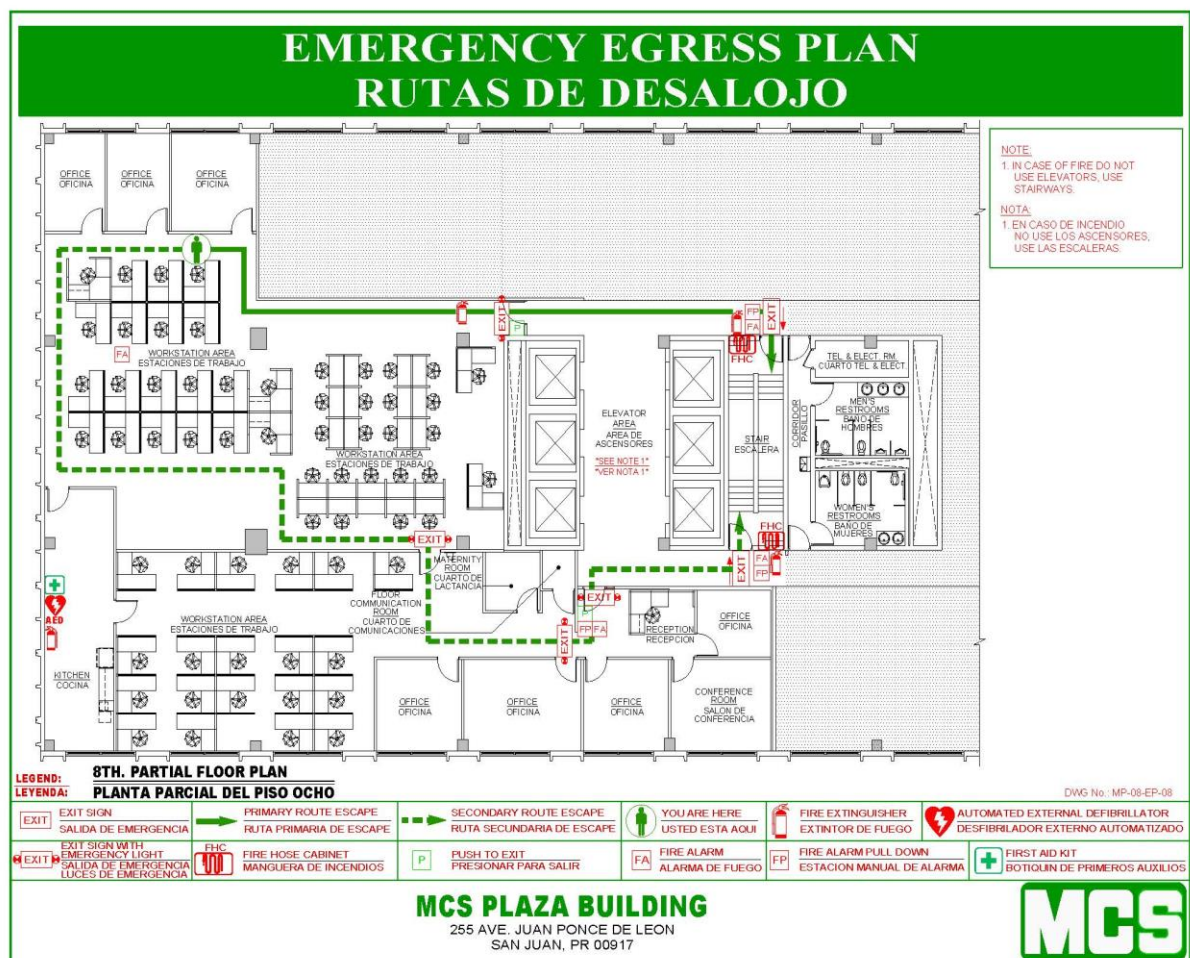
10.3.1. Building Premises Evacuation Plan

A workplace emergency is an unforeseen situation that threatens employees, customers, or the public, disrupts or shuts down MCS operations, or causes physical or environmental damage. The evacuation plan includes procedures that could be activated due to a disaster that obliges us to abandon the building premises. It could be any disaster like fire, bomb threat, or earthquake. Its purpose is to ensure that human life is our main priority. The best way is to prepare to respond to an emergency before it happens. Few people can think clearly and logically in a crisis, so it is crucial to advance when you have time to be thorough.

Building Premises

Building premises must be prepared to facilitate the evacuation of all personnel and access to all emergency agencies to perform their duties.

8TH Floor Emergency Evacuation Map:



Building Premises Readiness:

	TASK	Responsible	Task Performed (Y\N) Date
1	<p>Physical Areas</p> <ul style="list-style-type: none"> a. All lobbies, stairs, and floor access must be free of any object impeding personnel access to the emergency exits. b. All emergency exit doors have to be functional, identified, and labeled. c. All floors must have a floor plan indicating all emergency exits. d. All stairs must be well-illuminated with bright lights. e. All exits will have emergency lights and batteries connected to the building power plant. 	Facilities Team	
2	<p>Emergency Equipment</p> <ul style="list-style-type: none"> a. The facilities department will coordinate all emergency equipment maintenance, including fire extinguishers, tools, windshields, and flashlights. b. The Human Resources department will maintain the medicine inventory complete and up-to-date. c. IT Dept. will maintain the available and ready-to-use telecommunications. d. Building owners will be responsible for maintaining the building premise's access to cleaning without any objects impeding personnel evacuation. They will also preserve the building's power plant, water hoses, cistern, and emergency exits, which are fully operational. 	IT Team Facilities Team	

Personnel Preparedness:

1	<p>Personnel</p> <ul style="list-style-type: none"> a. The Emergency team will be responsible for the execution of this plan. b. Each floor will have two to four Emergency Team members. These team members will ensure personnel evacuation and security, whether they are the departments' supervisors or managers. c. Emergency Team and Human Resources will have an up-to-date list of all personnel from each department. This list will include the person's information and any physical impediments needing special attention during the evacuation. 	<p>Emergency Team Business Unit Members Human Resources Facilities Team</p>	
---	---	---	--

	<ul style="list-style-type: none"> d. Emergency Team leaders will present and discuss the evacuation plan with all Emergency Team members and understand their responsibilities. e. The Facilities Team will coordinate with supervisors and managers to present the Evacuation Plan to each business unit personnel to ensure everyone knows what to do during the process. 		
--	--	--	--

Evacuation Plan Activation:

Evacuation Plan Activation will vary depending on the emergency call. Steps could differ depending on the emergency occurring at a time. If the Evacuation Plan had been activated, the emergency would have been dangerous for the personnel, and they needed to abandon the building.

The Incident Commander or the Facilities AVP is the only one authorized to activate the Evacuation Plan.

Evacuation Plan procedures will be executed as follows:

1	<p>Fire</p> <ul style="list-style-type: none"> a. The plan was activated based on the fire because it was out of control, and the Emergency Team reported the situation to the Human Resources area. b. Human Resources will call all affected areas to inform them that the Evacuation Plan has been activated. They will also contact the Fire and Police Departments to report the incident. c. Human Resources will call the designated elevator operator to immediately take control of the elevator and be prepared to go to the affected floor if needed. d. Each Emergency Team member will inform the person that the Evacuation Plan has been activated, so they must leave the premises. e. Personnel will stop doing their duties and will form a line. The woman will take out their high heels (if applicable). All staff will be prepared to leave the premises when requested. f. The Emergency Team Leader will inform if personnel has to leave immediately or if there is enough time to pick up their belongings, turn off all electrical equipment, and/or carry out essential documents. g. An Emergency Team member will be at the beginning of the line and another at the end. They will count on all personnel to be evacuated. h. When the Emergency Team member is ordered, the personnel will leave the premises using the emergency stairs. They will 	<p>Emergency Team Business Unit Members Human Resources</p>	
---	---	---	--

	move to park lots XX to XX using the right side of the stairs in order and quietly.		
	<ul style="list-style-type: none"> i. If people are identified as handicapped or cannot walk, an emergency team member will use the elevator and move out of them from the floor. This is the only situation where the elevator will be used under a fire incident. j. Emergency Team members will ensure nobody else is still in the fire area. They will turn off all equipment, lights, and air conditioners if possible. k. Emergency Team members will ensure that all doors remain closed but not locked. l. Supervisors and Emergency Team floor members will recount personnel in the Emergency area (XX to XX) to ensure they are present. m. Depending on the fire's magnitude, the Emergency Team leaders and Incident Commander will decide if we must evacuate the floors above and below the fire. If they have to, Human Resources will call the Emergency Team members of each floor to report that their floor's Evacuation Plan has been activated and to prepare the personnel to be evacuated when the order is given. They will perform the same procedures detailed from e to l. n. If the floors above or below are not part of MCS, they will report the situation to the company management official. It will not be MCS's responsibility to evacuate personnel from these companies. We can assist if they ask for it. o. The Emergency Team leader, Incident Commander, and Human Resources manager will be available and waiting for the Fire and Police dept. I will report the situation to them and assist in any duty they are needed. They will also ask if there are personnel in the Emergency Area that require medical attention. p. Personnel will wait patiently and quietly in the emergency areas until the Emergency Team leader gives any other instructions. 	Emergency Team Business Unit Members Human Resources	

2	<p>Bomb Threat</p> <ul style="list-style-type: none"> a. If the plan has been activated based on a bomb threat, the Business Continuity Steering Committee and Emergency Team leaders have determined it is an authentic call and a dangerous situation. b. The Incident Commander will call all Managers of the affected area to inform the activated evacuation plan. They will also contact the Fire and Police Departments to report the incident. c. Emergency Team leaders will locate any artifact, box, purse, thermos, or object that does not belong to the area. If they discover it, they will not touch or remove the thing. They will 	Emergency Team Business Unit Members Human Resources	
---	---	---	--

	<p>immediately report the location when the Fire and Police dept. Arrives.</p> <p>d. The Incident Commander will call the designated elevator operator, who will immediately take control of the elevator and prepare to go to the affected floor if needed.</p> <p>e. Each Emergency Team member will inform the employees that the Evacuation Plan has been activated, so they must leave the premises.</p> <p>f. Personnel will stop doing their duties and will form a line. All staff will be prepared to leave the premises when requested.</p> <p>g. The Emergency Team Leader will inform if personnel has to leave immediately or if there is enough time to pick up their belongings, turn off all electrical equipment, and/or carry out essential documents.</p> <p>h. An Emergency team member will be at the beginning of the line and another at the end. They will count on all personnel to be evacuated.</p> <p>i. When the Emergency Team member is ordered, the personnel will leave the premises using the emergency stairs. They will move to park lots XX to XX using the right side of the stairs in order and quietly.</p>		
	<p>j. If people are identified as handicapped or cannot walk, an Emergency team member will use the elevator and move out of them from the floor.</p> <p>k. Emergency Team members will ensure nobody else remains in the affected area.</p> <p>l. Supervisors and Emergency Team floor members will recount personnel in the Emergency area (XX to XX) to ensure they are present.</p> <p>m. Depending on the Government Agencies' instructions, Emergency Team leaders and the Incident Commander will evacuate the floors above and below. The Incident Commander will call the Emergency Team members of each floor to report that the Evacuation Plan has been activated and to prepare the personnel to be evacuated when the order is given.</p> <p>n. If the floors above or below are not of MCS, they will report the situation to the MCS Plaza Administration. MCS will not be responsible for evacuating personnel from other tenants, although we can assist if they ask.</p> <p>o. Personnel will wait patiently and quietly in the emergency areas until the Emergency Team leader gives any other instructions.</p>	<p>Emergency Team Business Unit Members Human Resources</p>	
3	<p>Earthquake</p> <p>a. This plan has been activated based on the damages caused by an earthquake to the building premises and the danger it represents to the personnel security.</p>	<p>Emergency Team Business Unit Members Human Resources</p>	

	<ul style="list-style-type: none"> b. Once the shaking is over, the Facilities AVP will call Emergency Team leaders of all areas to inform them that the Evacuation Plan has been activated. c. Emergency Team members will assess the situation on their floor to verify injured personnel and their readiness to evacuate the area. They will report to the Incident Commander or Human Resources how many injured persons are and the situation's gravity. d. Emergency Team members will also verify the damages caused to the floor premises that could impede personnel from abandoning the area. They will try to clear access to the emergency exits without risking any lives. e. Based on the reports, the Emergency Team will organize the evacuation of each floor and the medical aid that has to be offered to the injured personnel. f. Emergency Team Leaders will inform the Emergency Team floor members of their turn to leave the premises and where they will move. g. When the Emergency Team member is ordered, the personnel will leave the premises using the emergency stairs. They will move to the assigned area using the right side of the stairs in order and quietly. 	Facilities Team	
	<ul style="list-style-type: none"> h. Suppose there are people identified as handicapped or anyone who cannot walk. In that case, an Emergency team member will use the elevator (if functional) and move out of them from the floor if possible. They will inform the Call Center and wait for professional assistance if they cannot move them out. i. Emergency Team members will ensure nobody else remains in the affected area. j. Managers and Emergency Team floor members will recount personnel in the Emergency area to ensure they are all present. k. The emergency team will have all reports ready to be used by any government agency to arrive at the premises and help us. l. Personnel will wait patiently and quietly in the emergency areas until the Emergency Team leader gives any other instructions. 	Emergency Team Business Unit Members Human Resources Facilities Team	

Resuming Business Operations:

1	<p>a. The Emergency Team will wait until Government Agencies permit us to return to business premises.</p> <p>b. Emergency Team members will coordinate the employees' return to working areas.</p> <p>c. If the area is not reusable, the Management Team will activate the necessary Contingency and Recovery Plans to ensure business operations.</p> <p>d. If the area is re-usable, Emergency Team floor leaders will instruct the personnel to be prepared to return to their floor.</p> <p>e. They will form a line and use the emergency stairs' right area to return to their floor. If the elevators are functional, the Emergency Team will coordinate with the guards on their utilization. Handicapped personnel and people identified by Human Resources will use the elevators first. Afterward, the remaining persons could use the elevators in an orderly and organized manner.</p> <p>f. After personnel return, Supervisors and Recovery Teams will ensure and encourage personnel to resume business operations.</p>	<p>Emergency Team Business Unit Members Human Resources Facilities Team</p>	
---	---	---	--

10.4. Loss of Workplace Scenario

Response Procedures

1. If the incident requires evacuation to ensure personnel safety and security, have all staff report to the designated meeting place and account for all building staff during the event. Notify the Facilities Team. Refer to the Evacuation Plan provided by the Facilities Team.
2. When instructed by the Incident Management Team, activate the response activities.
3. Prepare and submit the Damage Assessment report. Prioritize the order of the damages identified in the report. Take detailed photographs of all damages for use in insurance claims (if applicable).
4. Request the Facilities Team to ascertain whether the building/workplace is safe and available for re-entry. If it is unreliable or unavailable for re-entry, proceed with this Response phase. Otherwise, return to the workplace and continue normal operations.
5. If relocation is required, communicate with the Incident Management Team regarding the schedule.
6. Meet with the Business Continuity Coordinator, evaluate the event, and estimate the expected duration.
7. Share the information with the Facilities Team.

Recovery Procedures

1. Meet with business unit team members at the alternate site location and identify and prioritize work-in-progress.
2. Assign critical staff to designated alternate locations.
3. Collect, review, and approve all completed incident log sheets. Tracking the time expended for recovery-related activities such as record reconstruction is essential.
4. Initiate business processes as soon as possible.
5. Using the Critical Business Functions list, initiate and coordinate critical operations recovery, set priorities and staffing requirements, and start work.
6. If access to the alternate site is allowed, ascertain which documents and items are salvageable and required.
7. Working with the IT Recovery Team, request telephone redirection processes to start based on an agreed priority list. Consider providing additional telephone operator/reception assistance at the location receiving the redirected calls. Notify the call center of the new number so they can turn the call (if applicable).
8. Initiate the Call Tree for critical staff. According to need, reassure “On Call” employees

that they will be brought in as soon as possible.

9. Review the status and execute the recovery strategies and implementation schedule. Share this information with the Incident Management Team.
10. Ensure visitors/clients expected to visit the primary premises are informed of any changes to meeting venues.
11. Transport appropriate employees to their designated alternate site (if applicable).
12. Work with The IT Recovery and Facilities teams to prepare the alternate site.
13. Report the status to the Business Continuity Coordinator or Business Unit Head.

Resumption Procedures

1. If IT services were interrupted, refer to the Loss of IT Services scenario and follow the recovery and resumption tasks.
2. Otherwise, proceed with the Critical Business Functions validation and resume normal activities at the alternate location.
3. Generate an internal test call (If applicable).
4. Contact key clients to ensure they have the most current communication methods with your office.
5. Report any problems encountered during the validation process to the Business Continuity Coordinator.
6. When the recovered systems are updated, validated, and ready to resume normal (or contingency mode) operations, obtain the Business Unit Head (or designated alternate) approval to proceed to the next phase (normal operations or restoration phase in contingency mode).

Restoration Procedures

1. When the Business Unit Head or alternate approves, begin normal operations (full functionality). Start the restoration phase if operating in contingency mode (with less than full functionality).
2. Continue processing work backlog (if any).
3. Monitor operations and notify the Business Continuity Coordinator of restoration-related incidents.
4. Proceed to notify clients and vendors of the resumption of operations at either whole or contingency level (if applicable)
5. When notified that IT services have been restored (to their primary site), the Incident Management Team refers to the Resumption phase for tasks related to data validation, full system functionality, and user accessibility of the restored system.
6. When the IT systems have been validated, obtain the Business Unit Head's approval to return to normal operations.
7. Return to normal operations.
8. Report the return to normal operations to the Incident Management and IT Recovery teams.

10.5. Major Regional Event and/or Loss of Utilities Scenario

Response Procedures

1. Monitor bulletins from the Incident Management Team indicating what action to take: activate Business Recovery Plans, standby for further instructions, or take no action.
2. Refer to detailed checklists and plans if the Regional Incident is a hurricane or tropical storm.
3. Business Continuity Coordinator: Meet with the Incident Management Team to evaluate the event and estimate its expected duration.
4. If the main facility is impacted and is unavailable, refer to the Loss of Workplace scenario for tasks related to the relocation to an alternate site.
5. If the IT systems are impacted and unavailable, refer to the Loss of IT Services scenario for tasks related to the potential need to begin manual operations.
6. Collect, review, and approve all completed response tasks. It is particularly crucial for recovery-related tasks such as backlog processing.

7. Prepare and submit the Damage Assessment report. Prioritize the order of the damages identified in the report. Assist Facilities personnel in completing assessments as needed. Take detailed photographs of all damage: record the date, times, and location.
8. Report the status to the Business Continuity Coordinator, the Incident Management Team, and/or the Business Unit Head. Monitor bulletins issued by the Incident Management Team. If activation is required, proceed to the recovery phase tasks.

Recovery Procedures

1. Assign key staff to appropriate alternate locations if primary facilities are unavailable. Consider family commitments, travel difficulties, and business requirements.
2. Maintain thorough and complete written records throughout the recovery process.
3. At the Command Center, the Site Business Continuity Team will meet to initiate the recovery of critical business processes.
4. Using the list of Critical Business Functions, initiate and coordinate critical operations recovery, set priorities and staffing requirements, and begin work.
5. If access to the alternate site is permitted, ascertain which documents and items must be salvaged.
6. Working with the IT Recovery Team, request telephone redirection processes to start based on an agreed priority list. Consider providing additional telephone operator/reception assistance at the location receiving the redirected calls. Notify the call center of the new number so they can turn the call (if applicable).
7. Initiate the Call Tree for critical staff. According to need, reassure “On Call” employees that they will be brought in as soon as possible.
8. Report status updates to the Incident Management Team.
9. Ensure that all visitors/clients expected to visit the primary premises are informed of any changes to meeting venues.
10. Conduct status and progress meetings. Agree on the next steps and next team meeting, and ensure that the team meets at the start and end of the day while the incident is critical, then as necessary.
11. Transport appropriate employees to their alternate recovery sites (If applicable).
12. Phase in additional technical provisioning as it becomes available.

13. Maintain contact with key clients to ensure they have the most current communication methods with your office.
14. If IT services were interrupted, assist the IT Recovery Team in validating restored processing facilities. Refer to the Loss of IT Services Scenario (Appendix X).
15. If IT services were interrupted, establish whether any work in progress has been lost and how to recreate lost data.
16. If IT services were interrupted, enter data collected via manual processes following the disaster/outage.
17. Report the status to the Business Continuity Coordinator and/or Business Unit Head.

Resumption Procedures

1. If IT services were interrupted, refer to the Resumption phase of the Loss of IT Services scenario.
2. Report recovery status updates to the Business Continuity Coordinator and the Incident Management Team.

Restoration Procedures

1. If IT services were interrupted, refer to the Restoration phase of the Loss of IT Services scenario.
2. Ensure that all operational requirements are functionally available to support normal operations.
3. Validate the operational resumption process at the primary site.
4. Notify the Incident Management Team of any inconvenience in the operational restoration process.
5. Once the operational resumption process has been completed, notify the Incident Management Team.
6. Notify clients and vendors of the normalization of operations.
7. Report status to the Incident Management Team, the Business Continuity Coordinator, and/or the Business Unit Head.

10.6. Pandemic Scenario

Response Procedures

1. Alert the Business Unit's Incident Management Team Member and the Human Resources Department of any event or situation that has resulted in or could result in a loss of workforce availability (medical causes, civil unrest, weather-related causes).
2. If the cause is health-related (10%), refer to the Pandemic scenario section for appropriate actions.
3. Refer to the Regional Disaster scenario for appropriate actions if the cause is weather-related and widespread (such as a hurricane, storm, or flooding).
4. If the cause is civil unrest (public protests, blockage of access routes), meet with the Business Continuity Coordinator to determine the best course of action (VPN remote access, suspend operations, or provide escorted transportation to the workplace, among others).
5. Notify the Human Resources Department and the Incident Management Team of any injury or fatality.
6. Meet with the Business Continuity Coordinator to evaluate the event's impact, estimate the expected duration, and determine the course of action.
7. If the workforce's loss prevents MCS from performing critical business functions for an intolerable duration, determine the course of action, such as re-assigning personnel or notifying the Human Resources Department to contract additional temporary help.

Recovery Procedures

1. Notify personnel impacted by the event and provide instructions.
2. Coordinate with local emergency services and authorities (if necessary) to provide essential services such as security or escorts for transportation.
3. Request the Human Resources Department for extra staff/volunteers (if applicable).
4. Notify impacted clients, vendors, and third parties of the disruptive event and provide instructions (if applicable).

5. Report accountability to the Human Resources Department regarding employees who do not report to work due to the disruptive event.
6. Deploy re-assigned staff and/or contract temporary help to critical business functions.
7. Report status daily (or when significantly changed) to the Business Continuity Coordinator and Business Unit Head.

Resumption Procedures

1. When the recovery process is completed, notify the Business Unit Head to begin the resumption phase and continue normal operations.
2. Notify personnel impacted by the event and provide instructions on returning to the workplace.
3. Monitor the work backlog accumulated because of the disruption.
4. Ensure that the minimum workforce is available.
5. Notify impacted clients, vendors, and third parties that they are returning to normal operations (if applicable).
6. Report status to the Business Continuity Coordinator, Business Unit's IM Team member, Business Unit Head, and Human Resources Department.

Restoration Procedures

1. Conduct and document lessons learned exercises.

11.0 Checklist

11.1. Earthquakes

Earthquakes cause extensive structural damage. Transportation routes such as highways, bridges, and airport runways are typically damaged. Damage to buried utilities and communications systems, including water, sewage, and gas pipelines; telephone lines; electrical lines; and above-ground radio and television towers, can interrupt the operations within buildings that survived the earthquake.

They occur suddenly and without warning. They can trigger landslides, avalanches, flash floods, fires, or substantial ocean waves called tsunamis.

Planning considerations

- Consider the following when preparing for an earthquake.
- Assess the facility's vulnerability to earthquakes. Ask local agencies for seismic information for your area.
- Has a structural engineer inspected the facility? Develop and prioritize strengthening measures. These may include:
 - Adding steel bracing to frames
 - Adding sheer walls to structures
 - Strengthening columns and building foundations
 - Replacing un-reinforced brick filler walls.
- Follow safety codes when constructing a facility or making renovations.
- Inspect non-structural systems such as air conditioning, communications, and pollution control. Assess the potential for damage. Prioritize measures to prevent damages.
- Inspect facilities for earthquake-related items that can fall, spill, break, or move. Take steps to reduce these hazards:
- Move large and heavy objects to lower shelves or the floor. Hang heavy items away from where people work.
- Secure shelves, filing cabinets, tall furniture, desktop equipment, computers, printers, copiers, and light fixtures.
- Securely fixed equipment and heavy machinery to the floor. Larger equipment can be placed on casters and attached to harnesses, which attach to the wall.
- Add bracing to suspended ceilings, if necessary.
- Install safety glass where appropriate.

- Secure large utility and process piping.
- Keep copies of the facility's design drawings to assess the facility's safety after an earthquake.
- Review processes for handling and storage of hazardous materials. Have incompatible chemicals stored separately?
- Ask your insurance carrier about earthquake insurance.
- Establish procedures to determine whether an evacuation is necessary after an earthquake.
- Designate areas in the facility away from exterior walls and windows where occupants should gather after an earthquake if an evacuation is unnecessary.
- Conduct earthquake drills. Provide personnel with the following information:
 - In an earthquake, if indoors, stay there. Cover under a sturdy piece of furniture or counter, or brace yourself against an inside wall. Protect your head and neck.
 - If outdoors, move into the open, away from buildings, streetlights, and utility wires.
 - After an earthquake, avoid windows, skylights, and items that could fall. Do not use the elevators.
 - Use stairways to leave the building if it is determined that a building evacuation is necessary.

Earthquake Checklist

Date: _____

Completed by: _____

Tasks	S	U	N/A
Develop and practice an earthquake response plan. Include provisions for responding to medical emergencies, loss of power, fire, water, sprinkler system leakage, natural gas leakage, and chemical spills.			
Design new buildings and modify existing facilities to conform to local and federal building codes.			
Regularly inspect buildings for structural deterioration. Promptly repair all structural problems (i.e., cracked beams, broken masonry, mortar, dry rot, etc.)			
Situate newly constructed buildings on firm foundation materials, bedrock, cohesive soil, etc.			
Anchor all structures, tanks, and machinery to foundations.			
Anchor or brace top-heavy contents, industrial racks, bookshelves, etc.			
Equip all incoming natural gas and fuel lines with automatic shut-off valves.			
Equip buildings with a backup power supply, diesel generator, or long-term battery backup system.			
Maintain a minimum 72-hour water supply, non-perishable foods, and sanitation materials.			
Maintain a first aid kit along with search and rescue equipment.			
Provide embankment for all large liquid containers.			

S=Satisfactory

U=Unsatisfactory

N/A=Not Applicable

Identify corrective action for all Unsatisfactory responses.

Action Needed	Completed	Date

11.2. Fire

Fire is the most common of all hazards. Fires cause thousands of deaths, injuries, and billions of dollars in property damage worldwide.

Planning considerations

Consider the following when planning for a fire:

- Meet with the fire department to discuss the community's fire response capabilities. Talk about your operations. Identify processes and materials that could cause or fuel a fire or contaminate the environment in a fire.
- Has your facility been inspected for fire hazards? Ask about fire codes and regulations.
- Ask your insurance carrier to recommend fire prevention and protection measures. Your carrier may also offer training.
- Distribute fire safety information to employees: how to prevent fires in the workplace, how to contain a fire, how to evacuate the facility, and where to report a fire.
- Instruct personnel to use the stairs, not the elevators, in a fire. Instruct them to crawl on their hands and knees when escaping a hot or smoke-filled area.
- Conduct evacuation drills. Post maps of evacuation routes in prominent places keep evacuation routes clear of debris, including stairways and doorways.
- Assign fire wardens for each area to monitor shutdown and evacuation procedures.
- Establish procedures for safely handling and storing flammable liquids and gases. Establish procedures to prevent the accumulation of combustible materials.
- Provide for the safe disposal of smoking materials.
- Establish a preventive maintenance schedule to keep equipment operating safely.
- Place fire extinguishers in appropriate locations — train employees in using fire extinguishers.
- Install smoke detectors. Check smoke detectors monthly and change batteries at least once a year.
- Establish a system for warning personnel of a fire. Consider installing a fire alarm with automatic notification to the fire department.
- Consider installing a sprinkler system, fire hoses, and fire-resistant walls and doors.
- Ensure that key personnel are familiar with all fire safety systems.

- Identify and mark all utility shutoffs so fire wardens or responding personnel can quickly shut off electrical power, gas, or water.
- Determine the level of response your facility will take if a fire occurs. Among the options are:
 1. Immediate evacuation of all personnel on the alarm.
 2. All personnel are trained in fire extinguisher use. Staff in the immediate area of a firing attempt to control it. If they cannot, the fire alarm sounds, and all personnel evacuate.
 3. Only designated personnel are trained in fire extinguisher use.
 4. A fire team is trained to fight incipient-stage fires controlled without protective equipment or breathing apparatus. Beyond this level of fire, the team evacuates.
 5. A fire team is trained and equipped to fight structural fires using protective equipment and breathing apparatus.

Fire Checklist

Date: _____

Completed by: _____

Tasks	S	U	N/A
Develop and practice a fire emergency response plan. Include provisions for building evacuation, equipment shutdown, protection, electrical systems shutdown, stored documents, and response to medical emergencies.			
Meet with the fire department to discuss the community's fire response capabilities. Develop a fire plan with the local fire department.			
Establish business contingencies with suppliers.			
Post emergency phone numbers to activate the fire response plan.			
Distribute fire safety information to employees: how to prevent fires in the workplace, how to contain the fire, how to evacuate the facility, and where to report a fire.			
Ensure key personnel are familiar with all fire safety systems.			
Establish procedures for the safe handling and storage of flammable liquids and gases.			
Place fire extinguishers in appropriate locations — train employees in using fire extinguishers.			
Install automatic fire detection. Check alarms and detectors monthly.			
Establish a preventive maintenance schedule to keep equipment operating safely. Test fire protection equipment such as fire pumps regularly.			
Equip all incoming natural gas and fuel lines with automatic shut-off valves.			
Provide embankment for all large liquid containers.			

S=Satisfactory

U=Unsatisfactory

N/A=Not Applicable

Identify corrective action for all Unsatisfactory responses.

Action Needed	Completed	Date

11.3. Floods

Floods are the most widespread of all-natural disasters. Floods can be caused by numerous situations: intense storms, dam failures, sprinkler failures, broken pipes, etc.

Planning considerations

Consider the following when planning for floods:

- Review the community's emergency plan.
- Establish warning and evacuation procedures for the facility.
- Inspect areas in your facility that are subject to flooding. Identify records and equipment that can be moved to a higher location. Make plans to transfer files and equipment in case of a flood.
- Consider the need for backup systems:
 1. Portable pumps to remove floodwater.
 2. Alternate power sources such as portable generators or gasoline-powered pumps.
 3. Battery-powered emergency lighting.

Flood Checklist

Date: _____

Completed by: _____

Tasks	S	U	N/A
Develop and practice a flood emergency response plan. Include provisions for building evacuation, equipment shutdown, protection, electrical systems shutdown, stored documents, and response to medical emergencies.			
Regularly inspect buildings for structural deterioration, as well as for open entries for water. Promptly repair all structural problems and cover open gates.			
Locate all-important equipment and business records above ground level. If this is not possible, it is suggested that watertight walls or rooms be constructed around these items.			
Locate as many electrical system components as possible above ground level.			
Equip basement and ground-level areas with water pumps.			
Equip the plumbing system with back-flow valves.			
Cover and secure all liquid containers, especially those containing toxic chemicals.			
Maintain a first aid kit.			

S=Satisfactory

U=Unsatisfactory

N/A=Not Applicable

Identify corrective action for all Unsatisfactory responses.

Action Needed	Completed	Date

11.4. Hurricanes

Hurricanes are severe tropical storms with 74 miles per hour or higher winds. Hurricane winds can reach 160 miles per hour.

Hurricanes bring torrential rains and a storm surge of ocean water that crashes into the land as the storm approaches. Hurricanes also spawn tornadoes.

The National Weather Service issues hurricane advisories when a hurricane appears to be a threat. The hurricane season lasts from June through November.

Planning considerations

The following are considerations when preparing for hurricanes:

- Establish facility shutdown procedures. Establish warning and evacuation procedures for the facility.
- Make plans for communicating with employees' families before and after a hurricane.
- Take inventory and restock emergency items such as canned food, clothing/blankets, water, duct tape, flashlights with working batteries, first aid supplies, etc.
- Purchase a NOAA (National Oceanic and Atmospheric Administration, which provides National Weather Service Broadcasts) Weather Radio with a warning alarm tone and battery backup. Listen to hurricane watches and warnings.
- Hurricane Watch: A hurricane is possible within 24-36 hours. Stay tuned for additional advisories. Tune in to local radio stations for further information.
- Hurricane Warning: A hurricane will hit land within 24 hours. Take precautions at once.
 - Survey your facility. Make plans to protect external equipment and structures.
 - Make plans to protect windows. Permanent storm shutters offer the best protection. Covering windows with 5/8" marine plywood is a second option.
 - Consider the need for backup systems:
 - Portable pumps to remove floodwater.
 - Alternate power sources such as generators or gasoline-powered pumps.
 - Battery-operated emergency lighting.
 - Prepare to move records, computers, paints, and other items within your facility to another secure site.
 - Participate in community hurricane control projects.

Hurricane Wind Velocity Categories

Category	Wind Speed (MPH)	Storm Surge (Ft)	Probable Property Damage
1	74 – 95	4 – 5	<ul style="list-style-type: none"> • Damage primarily to shrubbery, trees, foliage, and unanchored mobile homes. • Some damage to poorly constructed signs.
2	96 – 110	6 – 8	<ul style="list-style-type: none"> • Considerable damage to shrubbery, trees, and foliage. • Some trees were blown down. • Major damage to mobile homes. • Extensive damage to poorly constructed signs. • Some damage to the roofing materials of buildings. • No significant damage to buildings.
3	111 – 130	9 – 12	<ul style="list-style-type: none"> • Foliage torn from trees. • Large trees were blown down. • Poorly constructed signs down. • Some damage to the roofing materials of buildings. • Some windows and doors were damaged. • Some structural damage to small buildings
4	131 – 155	13 – 18	<ul style="list-style-type: none"> • Shrubs and trees were blown down • All signs down • Considerable damage to roofing materials and buildings, windows, and doors. • Destruction of roofs of many small residences. • Destruction of mobile homes.
5	> 155	> 18	<ul style="list-style-type: none"> • Shrubs and trees were blown down • Extensive damage to roofs • Roofs were destroyed in many residences and industrial buildings. • Severe damage to windows and doors. • Extensive shattering of glass in windows and doors. • Some complete building failures. • Destruction of mobile homes.

Hurricane Checklist

Date: _____

Completed by: _____

Tasks	S	U	N/A
Activate the emergency response plan.			
Communicate the proposed plan of action to employees.			
An emergency communications plan of action was established and tested.			
Move vulnerable equipment, records, and paintings away from doors and windows, and cover computers with water-resistant tarps.			
Fill the vehicle's fuel tanks.			
Fill the emergency power generator tank with diesel.			
Move equipment off the floor.			
Secure valuable papers in watertight containers and store them in a safe building area.			
Back up all computer files and store them off-premises at the secured storage facility.			
Secure building envelope. Place wood or metal covers over windows and doors to prevent glass breakage.			
Extra supplies of plastic rolls, mops, buckets, water vacuums, lubricants (like WD-40), portable generators, radios, batteries, bottled water, and canned foods are available for the disaster recovery team.			
Keep a list of all vendors' telephone numbers available and secured. Notify them of any changes in the situation that may affect them.			
Begin securing the building from the storm and potential theft in the aftermath. Protect and cover windows and doors.			
Notify security and local authorities of a pending closing and identify personnel permitted on the premises after the storm.			
Shut down the nonessential power supply to equipment in the building.			
Secure all roof-mounted HVAC, lights, signs, and any loose equipment.			
Maintain a first aid kit.			

S=Satisfactory

U=Unsatisfactory

N/A=Not Applicable

Identify corrective action for all Unsatisfactory responses.

Action Needed	Completed	Date

11.5. Bomb Threat

Consider the following before responding to bomb threats in your organization:

- Develop a company policy on how to handle bomb threats.
- Develop a media policy and designate a spokesperson if a bomb threat occurs.
- Inform employees of the company's action plan in case of a bomb threat.
- Train employees on how to handle these threatening situations.
- Increase internal security measures and state of readiness.
- Professionals (e.g., local police departments) should give training seminars to employees to improve their techniques for these problems. Consider all employees involved in such an event, such as receptionists, customer service, human resources, and managers.
- Make sure copies of a report form are available at the receptionist and others' desks. Government agencies, such as the Treasury Department Bomb Threat Checklist, produce some quality forms. Alternatively, use the following to record information:

Bomb Threat Incident Report

Department:			
Your Name:		Date:	
Telephone No.		Ext.	
What time was the call received?			
Record caller's statements:			
DO NOT INTERRUPT THE CALLER. IF THE CALLER SEEMS AGREEABLE TO FURTHER CONVERSATION, ASK THE FOLLOWING QUESTIONS:			
Where is the bomb hidden?			
What time will the bomb detonate?			
Why did you plant the bomb?			
What floor is the device on?			
What type of device is it?			
Is the caller familiar with your facility?			
Additional Information:			
Male		Female	
	Yes	No	Comments:
Does the person appear angry?			
Can you determine an accent?			
Is it foreign? What dialect?			
Are there any background noises?			
Does a person appear calm?			
Outside phone?			
Good Connection?			
Other:			

11.6. Hazardous Materials

- Hazardous materials are flammable, combustible, explosive, toxic, harmful, corrosive, oxidizable, irritating, or radioactive. A hazardous material spill or release can risk life, health, or property. An incident can result in a few people's evacuations, a section of a facility, or an entire neighborhood.
- Many Federal and Local laws regulate hazardous materials.
- Consider the following when planning for hazardous materials:
 - Identify and label all hazardous materials stored, handled, produced, or disposed of by your facility. Follow government regulations that apply to your facility. Obtain a material safety data sheet (MSDS) for all hazardous materials at your facility.
 - Ask the local fire department for assistance in developing appropriate response procedures.
 - Train employees to recognize and report hazardous material spills and releases.
 - Establish a hazardous material response plan:
 - Establish procedures to notify management and emergency response organizations of an incident.
 - Establish evacuation procedures.
 - Depending on your operations, organize and train the Facilities Team to confine and control hazardous material spills following applicable regulations.
 - Identify highways near your facility used for the transportation of hazardous materials. Determine how a transportation accident near your facility could affect your operations.

Hazardous Materials Checklist

Date: _____

Completed by: _____

Tasks	S	U	N/A
Develop and practice a hazardous emergency response plan. Include provisions for containment, building evacuation, and response to medical emergencies. Distribute procedures to all employees.			
Keep containment supplies and proper containment equipment on hand, such as absorbent materials, tarps, and off-the-shelf containment equipment.			
Have a proper hazard communication program, including the complete Material Safety Data Sheet on hazardous substances.			
Establish business contingencies with suppliers.			
Familiarize the fire department with the hazardous materials in your facility. Send them copies of MSDSs if they keep those records.			
Survey transportation routes (roads, highways) for possible hazardous materials incidents.			
Survey neighborhoods and other facilities for possible hazardous materials incidents.			
Maintain a hazardous incident emergency kit. Include containment materials (gloves, face shields, respirators, drums, etc.).			
Maintain a first aid kit.			

S=Satisfactory

U=Unsatisfactory

N/A=Not Applicable

Identify corrective action for all Unsatisfactory responses.

Action Needed	Completed	Date

11.7. Power Outages

Power outages or technical emergencies resulting from power outages include any interruption or loss of a utility service, power source, life support system, information system, or equipment needed to keep business.

Planning considerations

Consider the following when planning for power outages or technological emergencies:

- Identify all critical operations, including:
- Utilities include electric, power, gas, water, municipal and internal sewer systems, and wastewater treatment services.
- Security and alarm systems, elevators, lighting, life support systems, ventilation, air conditioning, and electrical distribution systems.
- Communication systems, both data and voice computer networks.
- Determine the impact of service disruption.
- Ensure that key safety and maintenance personnel know all building systems.
- Establish procedures for restoring systems. Determine the need for backup operations.
- Establish preventive maintenance schedules for all systems and equipment.

Power Outage Checklist

Date: _____

Completed by: _____

Tasks	S	U	N/A
Develop a formal company response plan for technological emergencies such as power outages.			
Review all departments' equipment and operations to determine critical equipment and applications.			
Ensure that all critical equipment has backup power and/or UPS systems.			
Ensure that all software applications and data have backups.			
Ensure backup computer and telecommunications equipment is available if necessary.			
Establish business contingencies with suppliers.			
Develop a security policy/program for both in-house and network computer operations.			
Establish preventive maintenance schedules for all equipment.			

S=Satisfactory

U=Unsatisfactory

N/A=Not Applicable

Identify corrective action for all Unsatisfactory responses.

Action Needed	Completed	Date

11.8. Vital Records Storage

Both vital records programs and corporate business continuation plans deal with information protection.

The loss of information on vital records can affect business continuity, stockholder equity, legal or regulatory compliance, and financial stability. The loss of such can result in business failures.

A vital records program aims to identify and classify critical records and valuable papers and determine the protection necessary against hazards such as fire, water, smoke, building collapse, etc. In business continuation plans, the security and availability of vital records are essential to the business's survival during the emergency response, recovery, and restoration phases.

Vital records are irreplaceable documents or contain information for which temporary unavailability could constitute a severe legal, regulatory, or business impairment. Typically, these types of documents would be considered vital:

- Records must be original and for which reproduction cannot be substituted.
- Records are needed promptly to sustain the business or recover monies with which to replace buildings, equipment, finished goods, and work in progress,
- Records required to avoid delay in restoration of business and services,
- Records of high intrinsic value; and,
- Records are essential to the reconstruction of other documents.

Vital Records Checklist

Date: _____

Completed by: _____

Tasks	S	U	N/A
Develop a formal, comprehensive Vital Records plan. Vital Records are identified, categorized, and labeled with handling procedures established, locations documented, access during an emergency defined, and backups made as operating procedures.			
A comprehensive filing system has been established to organize and locate vital records quickly.			
All vital records have been copied or backed up and stored offsite.			
A record retention vendor has been selected. Its facility has been surveyed for ambient storage conditions, storage practices, fire protection, and safety.			
The equipment necessary for running backup media has been identified and is in place.			
Employee access to critical documents is limited, and an authorization procedure is in place.			
Employees have been trained on proper vital record handling, storage, and backup procedures.			
A list of records restoration vendors has been developed for emergencies.			

S=Satisfactory

U=Unsatisfactory

N/A=Not Applicable

Identify corrective action for all Unsatisfactory responses.

Action Needed	Completed	Date

For use during an Incident

Tasks	Check
1- Start a log of actions taken:	
2- Communicate with the Facilities Team:	
3- Identify any damage:	
4- Identify Critical Business Functions disrupted:	
5- Assemble your Response / Recovery Team:	
6- Provide information to staff:	
7- Decide on a course of action:	
8- Communicate decisions to staff and business partners:	
9- Provide public information to maintain reputation and business:	
10 - Arrange a Debrief:	
11- Review Business Continuity Plan:	

The Incident Commander should ensure a log is maintained at the beginning of an event and continued until the event's conclusion. Recording the chain of events throughout the disaster will help during the post-activity review. The Incident Management Team will collect these logs after the Exercise/Event.

[illegible]

11.11. Incident Notification Form

When notified by the Incident Management Team that the Business Recovery Plan (BRP) has been activated, the team leader or alternate should record the following information that will be passed along to department personnel:

The reporting individual must complete this form for all Disaster Events. During incident communications, the Business Continuity Coordinator will provide this information to the Incident Management Team. Advise the reporting individual that the information will be communicated to the IMT and other Teams as needed. Complete as much of the form as possible:

INCIDENT NOTIFICATION FORM

Incident Name: (i.e., Hurricane 20XX)		
Current Situation: (Who/What/When)		
Incident Start Date & Time: (mm/dd/yy & hh: mm AM/PM Time Zone)		
Area Affected: (Geographical area or site address - street, city, state)		
Reporting Person Name: (last, first)	Position/Title:	Company
Reporting Person's Contact Number: (Area code, phone number)		
Report Date/Time: (mm/dd/yy, hh: mm AM/PM)		
Site Situation: (i.e., building evacuated/open/closed; if reporting multiple addresses, list each)		
STATUS:		
<u>Employees</u> - Status, Communications, Relocation, Releasable, Relief		
<u>Customers</u> - Impact, Alternate Processing, Communications		
<u>Operations</u> - Impact, Shutdown, Defer, Relocation, Reductions, Shifts		
<u>Assets</u> - Damage, Loss, Replacement, Protection		

11.12. Damage Assessment Checklist

DAMAGE LOSS REPORT - PRELIMINARY DAMAGE ASSESSMENT

Location: _____ Completed By: _____

Date: _____ Time: _____

Area	OK?	Damaged?	Comments
Structural			
Utilities – Power, water, gas			
Elevator			
HVAC			
Generator – CPS/UPS			
Telecommunications- Phones, circuits			
Contents – Desk, chair, carpet			
Physical & Logical Security			
Property / Land Access, exits			
People			
IT Infrastructure – WAN, IP Voice, PCs			
Machine Room Equipment			
Environmental / Air / Health & Safety			
Other			

- If possible, estimate the time until damaged components can be repaired.
- If possible, estimate the resources required to repair damaged components.

Appendix A. Associated Sites

Appendix B. Checklists & Forms

Appendix C. Alternate Site Protocol & Facility Inspection sheet

Facility Inspection sheet:

Appendix D. Associated Relationships

MCS Plaza
One Line Diagrams
(Sheets E-1 + E-2 combined)



Appendix F. Glossary

This glossary contains the preferred definitions related to Business Continuity (BC), Disaster Recovery (DR), and Risk Management (RM) that are used in this document.

Acceptable Risk	A society or community considers the potential losses acceptable given existing social, economic, political, cultural, technical, and environmental conditions.
Activation	Implementing business continuity procedures, activities, and plans responds to a severe incident, emergency, event, or crisis. (BCI)
Alternate Facilities	Locations other than the primary facility are used to carry out essential functions, particularly in a continuity event. "Alternate facilities" refers to not only other sites but also non-traditional options such as working at home ("teleworking"), telecommuting, and mobile-office concepts.
Alternate Site	An alternate operating location to be used by business functions when the primary facilities are inaccessible. a. Another location, computer center, or work area designated for recovery. b. Location, besides the main facility, can be used to conduct business functions. c. A location other than the regular facility is used to process data and perform critical business functions in a disaster.
Application Recovery	The disaster recovery component deals with restoring business system software and data after the platform has been restored or replaced.
Business Continuity	An ongoing process ensures that the necessary steps are taken to identify the impact of potential losses and maintain viable recovery strategies, recovery plans, and continuity of services.
Business Continuity Management (BCM)	A holistic management process that identifies potential threats to an organization and the impacts on business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities. (ISO 22301)
Business Continuity Management Lifecycle	A series of business continuity activities collectively cover all aspects and phases of the BCM program. (BCI)
Business Continuity Management Program	Ongoing management and governance process supported by top management and appropriately resourced to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products and services through training, exercising, maintenance, and review. (BCI)
Business Continuity Steering Committee	A top management group gives direction, advice, guidance, and financial approval for the BCM programs undertaken by the BCM manager and various BC coordinators. (BCI)
Business Continuity Strategy	A strategic approach by an organization to ensure its recovery and continuity in the face of a disaster or other significant incidents or business disruptions. (BCI)
Business Continuity Team	The strategic, tactical, and operational units would respond to an incident and contribute significantly to the BC plans' writing and testing. (BCI)
Business Impact Analysis (BIA)	A method of identifying the effects of failing to perform a function or requirement.

Business Interruption	Whether anticipated (i.e., public service strike) or unanticipated (i.e., blackout), any event disrupts the ordinary business operations at an organization's location. (DRJ)
Business Interruption Costs	Different types of outages cause an impact on the business, usually measured by revenue lost. (DRJ)
Business Recovery	Steps were taken to resume the business within an acceptable timeframe following a disruption. (BCI)
Business Recovery Timeline	The approved sequence of activities is required to achieve stable operations following a business interruption. Depending upon the recovery requirements and methodology, this timeline may range from minutes to weeks. (DRJ)
Business Resumption	Following its recovery, a function's condition is when it is ready to take on tasks and activities to meet new business obligations.
Command Center	The location is local to the event but outside the immediately affected area, where tactical response, recovery, and restoration activities are managed. Each event could have multiple command centers, reporting to a single incident operations center. (DRJ)
Contingency Plan	An organization or business unit uses a plan to respond to a specific system failure or disruption of operations. (DRJ)
Data Recovery	The restoration of computer files from backup media to restore programs and production data to the state that existed at the last safe backup. (DRJ)
Declaration	A formal announcement by pre-authorized personnel that a disaster or severe outage is predicted or has occurred and triggers pre-arranged mitigating actions (e.g., a move to an alternate site). (DRJ)
Disaster	A sudden, unplanned, catastrophic event is causing unacceptable damage or loss. a. An event compromises an organization's ability to provide critical functions, processes, or services for some intolerable period. b. An event where an organization's management invokes its recovery plans. (DRJ)
Disaster Recovery (DR)	The technical aspect of business continuity. The collection of resources and activities to re-establish information technology services (including infrastructure, telecommunications, systems, applications, and data) at an alternate site following the disruption of IT services. Disaster recovery provides resumption and restoration of those operations at a more permanent site. (DRJ)
Disaster Recovery Exercise	A test of an institution's disaster recovery or BCP. (FFIEC)
Disaster Recovery Plan	A written plan for recovering one or more information systems at the alternate facility responds to a significant hardware or software failure or destruction of facilities. (NIST SP 800-34)
Disaster/Emergency Management	1. An ongoing process to prevent, mitigate, prepare for, respond to, maintain continuity during, and recover from an incident threatening life, property, operations, or the environment. (NFPA 1600) 2. A program that implements the program and organization's mission, vision, strategic goals, objectives, and management framework. (BCI)
Disruption	An event interrupts regular business, functions, operations, or processes, whether anticipated (e.g., hurricane, political unrest) or unanticipated (e.g., a blackout, terror attack, technology failure, or earthquake). <i>ASIS Editor's Note:</i> A disruption can be caused by positive or negative factors that disrupt normal functions, operations, or processes. (ASIS)

Downtime	A period in time when something is not in operation. <i>BCI Editor's Note:</i> This is often an outage regarding IT services and systems. (BCI)
IMT	Incident Management Team
Emergency	1. An unexpected or impending situation that may cause injury, loss of life, destruction of property, or cause the interference, damage, or disruption of an organization's regular business operations to such an extent that it poses a threat. (DRJ) 2. The sudden, urgent, usually unexpected occurrence or event requires immediate action. [ISO/PAS 22399 2007] <i>ASIS Editor's Note:</i> An emergency is usually a disruptive event or condition that can often be anticipated or prepared for but seldom precisely foreseen. (ASIS)
Emergency Response	The immediate reaction and response to an emergency commonly focus on ensuring life safety and reducing the incident's severity. (DRJ)
Emergency Response Plan	A documented plan usually addresses the immediate reaction and response to an emergency. (DRJ)
Essential Services	Infrastructure services without which a building or area would be considered disabled and unable to provide regular operating services typically include utilities (water, gas, electricity, telecommunications) and may also include standby power systems or environmental control systems. (BCI)
Hazard	A dangerous phenomenon, substance, human activity, or condition may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage.
Human Threats	As identified during the risk assessment, possible disruptions in operations result from human actions. (i.e., disgruntled employees, terrorism, blackmail, job actions, riots, etc.) (DRJ)
Impact	The effect, acceptable or unacceptable, of an event on an organization. The types of business impact are usually described as financial and non-financial and are further divided into specific types of impact. (DRJ)
Impact Analysis	Analyzing all operational functions and the effect an operational interruption might have upon them. <i>ASIS Editor's Note:</i> Impact analysis includes business impact analysis – the identification of critical business assets, functions, processes, and resources, as well as an evaluation of the potential damage or loss that may be caused to the organization resulting from a disruption (or a change in the business or operating environment). Impact analysis identifies: a. how the loss or damage will manifest itself b. How that degree of a potential escalation of damage or loss with time following an Incident; c. the minimum services and resources (human, physical, and financial) needed to enable business processes to continue to operate at a minimum acceptable level; and d. The timeframe and extent of the organization's activities, functions, and services should be recovered. (ASIS)
Incident Management	The process by which an organization responds to and controls an incident using emergency response procedures or plans. (DRJ)
Incident Response	An organization's response to a disaster or other significant event may significantly impact its people or ability to function productively. The incident response may include evacuating a facility, initiating a disaster

	recovery plan, performing a damage assessment, and other measures necessary to bring an organization to a more stable status. (DRJ)
Maximum Time Objective (MTO)	The amount of time the mission/business process can be disrupted without causing significant harm to the organization's mission. (NIST SP 800-34)
Offsite Location	A site is safe from the primary site where critical data (computerized or paper) and equipment are stored, and it can be recovered and used during a disruptive incident if original data, material, or equipment is unavailable. (BCI)
Pandemic	An epidemic of infectious disease that can have a worldwide impact.
Recovery Point Objective (RPO)	Point to which an activity's information must be restored to enable the activity to operate on resumption.
Recovery	Activities and programs are designed to return conditions to an acceptable level for the entity. (NFPA 1600)
Recovery Procedures	Actions necessary to restore data files of an information system and computational capability after a system failure.
Recovery Time Estimate (RTE)	After considering any uncertainties, the estimated period is required to restore a functionality level.
Recovery Time Objective (RTO)	The time goal is to restore and recover functions or resources based on acceptable downtime and an acceptable level of performance in case of a disruption of operations. (ASIS)
Response	<p>1. Immediate and ongoing activities, tasks, programs, and systems to manage an incident's effects that threaten life, property, operations, or the environment. (NFPA 1600)</p> <p>2. Providing emergency services and public assistance during or immediately after a disaster saves lives, reduces health impacts, ensures public safety, and meets the people's basic subsistence needs. <i>UNISDR Editor's Note:</i> Disaster response focuses on immediate and short-term needs, sometimes called "disaster relief." The division between this response stage and the subsequent recovery stage is unclear. Some response actions, such as the supply of temporary housing and water supplies, may extend well into the recovery stage. (UNISDR)</p>
Response Plan	Documented collection of procedures and information developed, compiled, and maintained in readiness for use in an incident. (ASIS)
Restoration	The process of planning for and implementing procedures for repairing hardware, relocation of the primary site and its contents, and returning to normal operations at the permanent operational location. (DRJ)
Resumption	The process of planning for and implementing the restarting of defined business functions and operations following a disaster. (ECB)
Risk Analysis	The quantification of organizational threats and the probability of them being realized. (BCI)
Risk Assessment/Analysis	The process of identifying the risks to an organization, assessing the critical functions necessary to continue business operations, defining the controls in place to reduce organization exposure, and evaluating the cost for such rules. Risk analysis often involves an evaluation of the probabilities of a particular event. (DRJ)