

**INDIANA ENROLLMENT BROKER
(IN EB)**

**Business Continuity / Disaster Recovery
(BCDR) Plan**

September 2020

CONFIDENTIALITY STATEMENT

This document contains confidential and proprietary information and is the sole property of Maximus. The document or its contents shall not be disclosed, distributed, or copied without the written permission of Maximus

Applicability

This policy applies to the the Maximus IN EB project, located at 429 North Pennsylvania, Suite 301, Indianapolis, Indiana 46204

Policy

All Maximus project sites are required to develop, document, exercise, and maintain a Business Continuity / Disaster Recovery (BCDR) Plan. The BCDR Plan provides strategies and capabilities to safeguard and resume business functions within pre-determined timeframes established either by the contractual requirements of the program or Maximus. The DR Plan will integrate with and support the business objectives of Maximus.

Purpose

The purpose of this policy is to ensure quick and effective recovery of Maximus sites at the time of a business interruption or disaster regardless of the type of event (i.e., accidental, man-made, or natural.)

Scope

The BCDR plan is to be executed only after any immediate life-safety issues are addressed. Although no plan can be written to address every possible type of disaster, this plan is intended to be used as a procedural resource during a disaster.

Objective

Maximus recognizes the need to establish comprehensive BCDR policies to protect employees, customers, assets, and information as well as to minimize the time it will take to restore critical operations, functions, products, and services after an emergency is declared. The plan facilitates the identification of resources required to resume business operations at a survivable level. The following list includes the main objectives of the plan:

- Define prioritized critical processes using a Business Impact Analysis
- Define critical internal resources
- Define critical vendor and suppliers
- Define the infrastructure and dependencies
- Establish comprehensive procedures to plan for and respond to business disruptions

APPROVAL, EXERCISE, AND REVISION HISTORY

Approval

The Business Continuity / Disaster Recovery (BCDR) plan for each site must be approved annually by the IN EB Business Owner.

Maintenance

A maintenance program is instituted for regular updates of all Maximus BCDR plans no less than every twelve months. This maintenance program is crucial to ensuring that the documentation is up-to-date and that management is familiar with the strategy and solution.

Exercises

Conducting exercises are vital to train staff and identify gaps within the existing documentation so in the unlikely event of a business interruption/disaster, the staff will know what to do and follow the documentation to ensure a smooth transition into recovery. Exercises will be conducted annually in graduated complexity to include notification drills, tabletop exercises, disaster recovery failover exercises, and physical relocation events. Based on the specific goals/objectives of the exercise, the Senior Site Manager in conjunction with Maximus ISO-BCDR department will determine the most appropriate BCDR exercise. The IN EB Project Manager in combination with the Maximus BCDR team will facilitate annual exercises as required.

Distribution

Through our tried and tested methodology, Maximus's BCDR plans are created to prepare staff for the unlikely event of a business interruption. Naturally, site-specific plans include staff personal and company proprietary information. It is our desire to uphold this privacy and not distribute these plans. If distributed outside of Maximus, all plans will be sanitized.

Document Approval

Business Owner	Title	Date
Jennifer Haas	Vice President	9/1/2020

Revision History

Revision Number	Date	Revised By	Summary of Changes
1.1	07/01/2019	ISO-BCDR Team	BCDR Foundational Template
	09/10/2018	John DeLury	Initial plan creation
	08/26/2019	John DeLury	Migrated plan to latest template
	09/01/2019	Natalie Smith	Review & Update
	03/09/2020	Daniel Duzenbury	Review & Update
	09/01/2020	Jennifer Haas	Review & Update

Exercise History

Exercise Type	Date	Exercise Results/Comments
Tabletop	09/18/2018	Successful
Tabletop	09/09/2019	Successful

Authority to Activate BCDR Plan

Primary	NaKeita Boyd
Secondary	Jennifer Haas
Tertiary	Debbie Van Meter

Table of Contents

IN EB	Error! Bookmark not defined.
Applicability	ii
Policy	ii
Purpose	ii
Scope	ii
Objective	ii
Approval, Exercise, and Revision History	iii
Approval	iii
Maintenance	iii
Exercises	iii
Distribution	iii
Section 1 – Overview	2
Executive Overview	2
Definition of a Disaster	3
Business Continuity Assumptions	4
Training, Maintenance, and Exercises	4
BCDR Plan Testing	5
Exercise Description	5
Recovery Timeframe Definitions	6
Data Backup	6
Data Retention	6
Section 2 – Site Information / Mitigation	7
Site Summary	7
Summary of Services	7
Contractual Requirements/Service Level Agreement	7
Roles and Responsibilities	8
Delegation of Authority	14
Section 3 – RESPONSE	10
Corporate Crisis Management	10
Gather Employee Information	10
Notify Employee	10
Disaster Declaration Criteria	11
Maximus IT Notification and Escalation Process	12
Emergency Information Line	12
Recovery Personnel Contacts	13
Damage Assessment Procedures	13
Incident Response Tracker	13
Recovery Status Report	13
Media Protocol	13
Maximus Pandemic Plan	13
Section 4 – Recovery	17
Disaster Declaration Procedures	17
Business Process Recovery Steps	Error! Bookmark not defined.
Information Technology Incident Management	18

Telecom	21
Telephone Script	21
Offsite Storage	21
Section 5 – Reconstitution	22
System Functionality Validation	22
Data Validation	22
Backlog Processing	22
Attaining Normal Operations	23
Terminating Contingency Operations	23
Section 6 – Appendix	24
Glossary and Acronyms	24
Appendix A: Staff Contact Information	28
Appendix B: Client / Vendor Contact Information	29
Appendix C: Site Floor Plan	30
Appendix D: Site Aerial Maps and Driving Directions	30
Appendix E: Bomb Threat Checklist	32
Appendix F: Active Aggressor / Active Shooter	34
Appendix G: Disaster Recovery Box Inventory List	36
Appendix H: Third Party or IN EB related Business Continuity / Disaster Recovery Plans	37
Appendix I: Associated Documentation	38
Appendix J: Procedures Change Form	39
Appendix K: Recovery Notes	40
Appendix L: Incident Response Tracker	41
Appendix M: Recovery Status Report	43
Appendix N: Damage Assessment	44

SECTION 1 – OVERVIEW

Executive Overview

Maximus understands the importance of a comprehensive Business Continuity / Disaster Recovery Plan (BCDR) to address the specific recovery needs of each of our sites. We continually look for ways to team with our clients on BCDR as any type of disruption in service impacts Maximus, our clients, and their customers. Furthermore, we have standardized our BCDR approach and assigned team members that represent all aspects of operations (i.e., human resources, technology).

Together, the plans address restoration of business operations and technological functionality. These plans are designed to assist sites in educating, preparing, testing, and implementing disaster recovery in the event of a business interruption. In addition, Maximus's Business Continuity Disaster Recovery (BCDR) team members provide direction in the creation, training, maintenance, and exercising of the site-specific BCDR plan for each facility.

This plan is divided into six (6) Sections which will be described in further detail. When the Plan is updated, the Business Owners are responsible for notifying and/or distributing the updated Plan to key stakeholders.

- ♦ SECTION 1 – Overview
- ♦ SECTION 2 – Site Specific Operations
- ♦ SECTION 3 – Checklists and Scripts
- ♦ SECTION 4 – Recovery
- ♦ SECTION 5 – Reconstitution
- ♦ SECTION 6 – Appendix

Definition of a Disaster

A disaster is defined as a loss of the facility or business processing due to a catastrophic event, which causes vital business processes to stop for an extended period of time (i.e., more than 24 hours). This includes:

- Any incident that may endanger the lives and safety of the employees
- Loss of the building due to fire, water damage, hurricanes, etc.
- Regional threat due to severe weather conditions, civil disruption, etc.
- A situation that may be catastrophic for the business
- Loss or delay of providing mission-critical functions for an extended period of time
- An event that results in significant loss of assets or revenue flow
- An event resulting in the inability to meet important customer commitments and contractual obligations or to protect the interests of the program, customers, business partners and Maximus and its employees

Maximus may declare a disaster situation when a disruption occurs affecting daily operational services and/or network and telephony systems beyond acceptable limits.

A disaster may originate from an external or internal source and may involve one or more events. These may include, but are not limited to:

Level I: Logical or Outside Support Services Outage: This includes the destruction of data from a computerized or digital format (PCs, LAN, and communication systems) as a result of corrupted data or system backups, software errors, hardware failure, computer viruses, or intentional acts of sabotage. Also included are facility outages (i.e. HVAC; Heating, Ventilation, and Air Conditioning). Critical Support Services not within the scope of Maximus operation or control, such as voice and data telephony, electric, gas, and water services are also listed in this category.

Level II: Site is Not Available: This includes the destruction or denied access to the facility. A fire that affects any or all of the building is an example. Localized problems may also result from a power failure, water damage, or sabotage, and affect the facility or services.

Level III: Regional Disaster: This includes destruction or hindered access to a larger area wherein the facility is located (i.e., hurricane, winter storm, building fire, freeway closures, hazardous materials incident). This level includes major business interruption/disasters where resources in or near the impacted area are overwhelmed and extensive state and/or federal resources are required.

Business Continuity Assumptions

The successful execution of Maximus's Business Continuity / Disaster Recovery plan will depend upon:

- The availability of staff members to assist with the recovery
- The cooperation and assistance from other Maximus locations when necessary
- The timely declaration of a business interruption/disaster and activation of the Command Center
- Availability of alternate facilities
- Availability of identified critical resources
- Availability of critical vendors
- Availability of communication vehicles such as newspapers, radio, and local television to notify clients of the situation
- Current and applicable recovery procedures
- Availability of management staff to assist with legal and procurement procedures as outlined in the Maximus Authority Matrix and Project Manager Manual

Training, Maintenance, and Exercises

Maximus will work to develop a comprehensive Business Continuity / Disaster Recovery (BCDR) awareness program for all Maximus employees throughout the life of the contract term. The program will explain the importance of BCDR for the Maximus operation and what non-key employees should do in the event of a disaster. This training will help ensure that all staff associated with the Maximus are trained and prepared to respond in the event of a disaster.

Supervisors and managers will be given annual emergency preparedness training to site staff. All staff will receive additional instructions on their particular role in employee and property safety. This training is included in all new hire training classes. The chart below presents highlights of our planned training, exercises, and plan maintenance on a calendar year basis, which is based on the FEMA Emergency Management Guide's suggested training drill and exercise chart.

Annual Training and Exercise Chart

	January	February	March	April	May	June	July	August	September	October	November	December
Employee Awareness Training												
BC/DR Exercise									X			
Plan Maintenance								X				
Evacuation Drill												

BCDR Plan Testing

The IN EB Business Continuity / Disaster Recovery plan will be tested in accordance with the contract requirements using either a tabletop scenario or IT disaster recovery failover. It is the policy of Maximus that the BCDR plan for the IN EB Program is developed, documented, exercised, and maintained based on contract requirements. The plan is designed to assure the continuation of services in the event that a natural disaster or other disruption occurs and thereby protect the interests of the customers, employees and the IN EB Program.

Exercise Description

Following is an explanation of the various types of BCDR exercises. Based on the specific goals/objectives of the exercise, the Project Manager along with the BCDR team will choose the most appropriate BCDR exercise. The Business Continuity Disaster Recovery (BCDR) team will assist with leading and facilitating the exercise process. Recovery exercises are used to train staff and identify gaps within the existing documentation so in the unlikely event of a business interruption/disaster, the staff will know what to do and follow the documentation to ensure a smooth transition into recovery.

Notification Drill: A notification drill (manual call tree) is a telephone exercise to contact individuals on a call tree. This drill is initiated by a member of the IN EB Core Recovery Team. A notification log is completed and includes the following:

- Date and time of drill
- Staff contacted or attempted to be contacted
- Results/Documentation required (i.e., number of personnel contacted, number of no answers, number of answering machines, wrong numbers, busy, left message, if contacted—how long to get family in order and return to work.)

Tabletop Exercise: This type of exercise is a staged event where business unit management, staff, and vendors (if appropriate), meet in an open forum to discuss actions for response to a specific business interruption scenario. A tabletop exercise is an informal, low-stress method of exercising business continuity / disaster recovery (BCDR) plans in which participants review and discuss the actions they would take without actually performing the actions. The three primary objectives to this type of exercise are:

- Familiarize new project staff with their role in business continuity planning
- Provide business continuity planning training and awareness to project recovery staff
- Advance staff readiness in the recovery of their critical functions

IT Disaster Recovery Exercise: Typically, a test of only technology is included in an IT Instantiation exercise. Many times, this type of exercise is performed prior to a physical relocation—to prove a specific design or theory of how a recovery process should work. This may or may not include business staff, but always includes technology staff. This test will also confirm data has been correctly restored to accounts.

Physical Relocation: This is the most complex of exercises where the scenario prevents staff from working within their site. This exercise involves staff relocating to their recovery location or backup staff from another location taking over the work of the affected site. Based on the objectives of the specific exercise, this can be announced, unannounced, weekday, or weekend, or any combination. Detailed planning and use of existing BCDR plans allows for identification of gaps within the documentation.

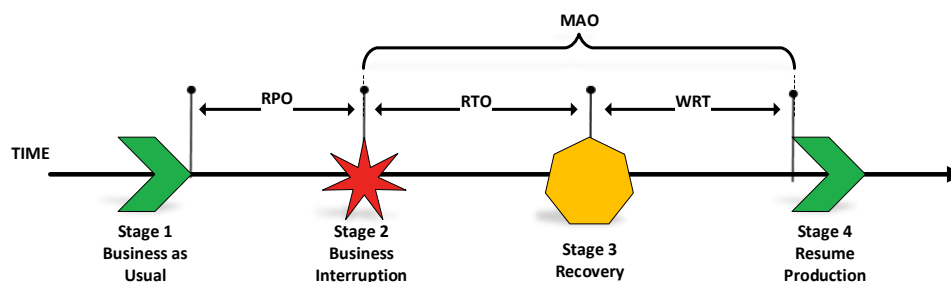
Recovery Timeframe Definitions

Recovery Point Objective (RPO): The RPO is the maximum targeted period in terms of hours, that data can be lost without causing serious damage to a function.

Recovery Time Objective (RTO): The maximum targeted period in terms of hours, in which an affected business unit must recover in order to not adversely affect financial or functional objectives.

Work Recovery Time (WRT): The time it takes to get critical business functions back up-and-running once the systems (hardware, software, and configuration) are restored to the RPO; this includes the manual processes necessary to verify that the system has been restored to the RPO, and all necessary processes have been completed to address the remaining lost, or out-of-synch, data or business processes.

Maximum Allowable Outage / Maximum Tolerable Downtime (MAO/MTD): The maximum amount of time mission / business process can be disrupted without causing significant harm to the organization's mission.



Data Backup

Maximus backup procedures require all servers be backed up and the media or data stored at an off-site facility. Tape backups are executed on a daily, weekly, and monthly schedule, with each version being retained in the active tape library for a pre-determined period of time. The current versions of the daily backups are retained at off-site facilities until a weekly backup has been executed and delivered to the off-site location. Weekly backup tapes remain at the off-site facility until a monthly backup has been created and delivered to off-site storage. The backup tapes are sent to the off-site storage facility the following morning in secured, environmentally controlled vehicles. Access to the off-site facility, or retrieval of tapes from the off-site facility, are limited to those individuals granted authorization by the data center management.

Backups occurs locally at each data center. The primary location for all data that is backed up will be online on separate media in the data center where it is backed up (Culpepper and Englewood). A secondary copy will be duplicated to tape on a daily basis. Monthly backup data will be residing on site for one month, and duplicated and kept off-site at a nearby Iron Mountain facility for 2-year retention and disaster recovery. The yearly backups that occur at the beginning of the year are written to encrypted tape media and stored at an Iron Mountain facility for 10 years.

Data Retention

Daily Differentials (Monday – Friday 6:00 PM – 6:00 AM) data resides on disk for one week. Daily tapes are sent offsite for two weeks. The tapes are placed back into the rotation cycle after the two-week period has passed.

Weekly Full Backups (every Friday 6:00 PM – Monday 6:00 AM) data resides on disk for two and weekly tapes are sent offsite five weeks. Tapes that are sent offsite for a five-week period and placed back in the rotation cycle once returned.

Monthly (First Friday of every month 6:00 PM – Monday 6:00 AM) data resides on disk for two and monthly tapes are sent to offsite for two years. Tapes that are sent offsite for a two-year period and placed back in the rotation cycle once returned.

Yearly (First week, first Friday 6:00 PM – Monday 6:00 AM) data resides on disk for two weeks and yearly tapes are sent to offsite storage for ten years.

SECTION 2 – SITE INFORMATION / MITIGATION

Site Summary

Main Facility:
429 North Pennsylvania
Suite 301
Indianapolis, IN 46204

Location Description

We are located on the 3rd floor, North Pennsylvania across from the Indiana World War Memorial, we staff 26 employees and share our floor with another Maximus project.

In the event of a pandemic or other emergency, services will be shifted to work from home using established policies and procedures.

Summary of Services

IN EB provides live voice services for inbound and outbound calls supporting enrollment, disenrollment, plan changes, and general questions for the following Indiana Medicaid programs: HIP, Hoosier Healthwise, and Hoosier Care Connect.

Additionally Indiana provides live chat services for general questions through the FSSA website.

Contractual Requirements/Service Level Agreement

90% of new eligibles contacted w/in 14 days	100% of after-hours calls returned next business day.
Relevant information entered into CORE w/in three business days.	85% of all issues resolved on line.
Relevant information entered into CORE with 98% accuracy.	100% of unresolved issues followed-up w/in one business day.
98% of all written provider/recipient inquiries answered w/in 10 business days.	Data Reporting and Monitoring
100% of correspondence responded to w/in 15 business days of receipt.	Status Report 1 working day prior to each status meeting
15% Auto-assignment rate for Care Connect	Program Data Report w/in 10 business days of the end of the previous month.
Helpline	Usage Report (submitted with invoice)
97% calls reach the helpline menu w/in 30 Seconds	Member Education and Outreach Plan submitted (November 30)
Average Speed of Answer Less than or Equal to 60 Seconds	QMIP Plan w/in thirty (30) calendar days after the end of each calendar year (January 29, 2016)
0% busy rate.	QMIP quarterly updates within 30 calendar days after the end of each quarter.
Abandon rate less than or equal to 7%	

Roles and Responsibilities

The following table describes each team and role responsible for executing or supporting system recovery and reconstitution. Designation of key planning personnel may need to be modified at the time of the event for enhanced situation response. Additionally, any personnel assigned directly or indirectly to any of the below positions, groups or teams are considered essential for purposes of dismissal and recall.

Business Owners / Project Managers
<ul style="list-style-type: none"> • Lead IN EB BCDR plan development, exercises, maintenance, activation, and recovery efforts. • Reviews the BCDR plan at least once every 365 days or whenever there is a significant change to the system or operating environment; • Ensures the BCDR plan is tested at least annually; • Ensures a technical test for each system is conducted at least every other year; • Reviews and corrects plan deficiencies in a timely manner; • Investigates and implements the most cost effective, efficient and available recovery strategies; • Ensures the annual plan review includes an analysis of the identified recovery strategies to ensure recovery strategies take full advantage of all possible cost savings and efficiencies; • Obtains appropriate resourcing to include funding and staffing, for recovery planning requirements; • Ensures all personnel with recovery responsibilities are trained to consider recovery preparedness part of their normal duties; • Determines and manages information system and data backup storage and alternate processing facility agreements; • Ensures the Contingency plan is distributed to all personnel who are assigned recovery responsibilities and maintained in current status; • Ensures a copy of the most current BCDR plan is maintained at the alternate processing location; • Ensures stringent change control is maintained over the application/system and the BCDR plan; • Should an event occur, contacts recovery team members or escalates to senior management depending upon the severity of the event; and • Delegates recovery responsibility as necessary during an actual event to ensure expeditious and accurate information system recovery
Management Team
<ul style="list-style-type: none"> • Ensuring a thorough and rapid failure assessment is conducted to accurately declare a disaster and fast enough to ensure recovery within the established Recovery Time Objectives (RTOs); • Declaring a disaster when a specific event warrants such action; • Adjusting the RTO as necessary to accommodate cyclical operational peaks and ebbs; • Ensuring effective implementation of the BCDR plan when necessary; • Coordinating with client throughout the recovery process; • Tracking the status of all recovery efforts within the scope of the BCDR plan; • Coordinating all travel and lodging requirements for relocating recovery team personnel; • Coordinating and obtaining approval for all recovery-related procurement actions; and • Coordinating and authorizing the migration back to the primary facility.

Disaster Recovery Coordinators (DRC)
<ul style="list-style-type: none"> • Assist the business owner in conducting all phases of Contingency planning; • Assist the business owner in recovery strategies development and implementation; • Oversee and coordinate the recovery-related training and awareness program for all personnel
IT Recovery Team
<ul style="list-style-type: none"> • Conduct failure assessment and recommending disaster declaration status to the business owner; • Implementing mitigation actions for impact reduction; • Recovering a VPG (Virtual Protection Group) • Coordinating repair and salvation action; • Recovering application/system functionality at the alternate processing facility in RTO order. • Coordinating with the alternate facility and the BCDR Management Team to resolve any telecommunications connectivity issues to include extending the system to the users; • Ensuring all required system cyber security controls are in place throughout the recovery and reconstitution phases; • Stopping operations at the alternate facility when directed and replenishing any expended supplies; • Ensuring the most current data is shared with the primary facility so the restored system is up to date; • Ensuring all systems are transitioned to backup mode1 when directed to do so by the BCDR Management Team.
Business Continuity Disaster Recovery (BCDR) Team
<ul style="list-style-type: none"> • Provide Business Continuity Disaster Recovery (BCDR) program governance and oversight in project and enterprise continuity and recovery planning efforts. • Promote best practices in project recovery planning through Business Impact Analysis (BIA) and Risk Analysis (RA). • Provide support and direction in BCDR plan development, documentation, maintenance, and testing. • Establish BCDR project guidance and oversight for recovery plan exercise requirements. • Assist project with declaring a disaster and invoking plan activation as needed. • Assist project with coordinating Corporate IT resources as needed during an event. • Provide project with guidance during relocation and recovery efforts as needed during an event. • After event post mortem / lessons learned review.

Delegation of Authority

The table below identifies the delegation of authority for key positions in the event that those employees are not available during an incident or business disruption.

Position Title	Primary	Secondary	Tertiary
Business Owner	Jennifer Haas	Robin LaFrance	Ilene Baylinson
Project Manager	NaKeita Boyd	Jennifer Haas	
Supervisors / Team Leads	Debbie Van Meter	Tierra Pinkins	Robin Gomez-Olvera

SECTION 3 – RESPONSE

The Alert and Notification phase of the Business Continuity Disaster Recovery (BCDR) plan defines the initial actions to take in order to ensure effective communication, provide for adequate staffing, and to conduct a damage assessment for the purposes of determining response scope.

Corporate Crisis Management

If IN EB has been involved in a significant business disruption that may impact corporate matters or may be publicized negatively in the media, such as; branding, reputation, corporate officers, cyber-attack, etc., you must contact the Maximus General Council at 703-251-8602.

Gather Employee Information

- Have all employees, visitors, etc., been counted?
- Which employees are missing, and have their names and descriptions been communicated to local authorities?
- Do any employees need medical assistance or did any employees go to the hospital?
- Do any employees have special needs that need to be accommodated during the emergency?
- Can the employees be sent home or should shelter arrangements be made?
- Do employees need any type of transportation?

Notify Employee

Below is an example notification script for notifying staff after a business interruption/disaster impedes critical business functions. Contact the staff to inform them of work expectations.

This is _____
(Your Name – i.e., program manager)

The date is _____, and the time is _____.
(Today's Date) (Current Time and Time Zone)

I am calling to inform you that IN EB _____
(Location, Street address, city and state)

has been affected by a _____
(Give Situation- business interruption/disaster, crisis, or emergency)

I need you to:

- 1) Stay home and wait for instructions
- 2) Go to _____
(Complete Recovery Site's name)
- 3) Call your staff and let them know to either:
 - a) Stay home and wait for instructions
 - b) Go to _____
(Complete Recovery Site's name)
- 4) Call the 800 number for updates

Disaster Declaration Criteria

Activation is the means by which the procedures contained in the BCDR plan are initiated and executed. An impacting event occurs and pre-planned steps are taken. Inter-related processes must address multiple needs and requirements, accounting for life safety, chain of command, escalation, and effective communication. The significance of the event, the level of disruption, and the cost of activating the business continuity recovery plan should be taken into account before making the decision to declare a disaster.

Business Continuity (BC) recovery plan activation is to be made by the project Incident Commander (IC), usually the project business owner (BO) or project manager (PM) after consulting with the Core Recovery Team (Project Operations, Security, Facilities, SME's).

Activation criteria must focus on triggering events and conditions, such as event; Type, Severity, Impact, and Duration to clearly analyze and evaluate current circumstances.

Damage Assessment

Activate the business continuity plan if the damage assessment report indicates the activation criterion has been met.

- Life Safety
- Facilities
- Power Distribution

Recovery Timeframes

Activate the business continuity plan if the restoral time for critical functions significantly exceed recovery time objectives.

- Recovery Point Objective
- Recovery Time Objective
- Maximum Allowable Outage

Once the decision is made to activate the BCDR plan. Implement with Urgency!

Notification

Declaration of a disaster is to be made by the Incident Commander, after consulting with the Core Recovery Team.

The Incident Commander will notify the 24/7 Maximus IT Enterprise Operations Center (EOC) at: 1-888-349-7762 –or- 1-800-321-0701. Advise the EOC staff that IN EB is declaring a disaster and invoking their business continuity recovery plan procedures.

Let IN EB staff know your expectations of them (go home, work from home, call Emergency Information Line for updates, etc.).

Notify IN EB client, appropriate vendors and key stakeholders of your situation and that recovery status updates will follow.

Communication

Updated manual call tree information needs to be available on print out as well as cell phones to those making calls and updating staff.

Ensure that your staff knows the Emergency Information Line number to receive recovery status updates.

Schedule regular update meetings with all stakeholders, assign a scribe to document all decisions made.

Activate Command Center (when appropriate) for off-site Recovery Command & Control.

Activate Alternate Recovery Site Solution for off-site critical function recovery.

Maximus IT Notification and Escalation Process

When a system/service outage or facility disaster occurs, please first ensure all safety procedures are met, and then follow these IT alert / escalation procedures:

1. Call the 24/7 Maximus IT Enterprise Operations Center (EOC) at: 1-888-349-7762 –or- 1-800-321-0701
2. Report the issue or request to the on-call representative, who will then open a service ticket on your behalf.
3. Contact ISO-IR@Maximus.com if there is a suspicion that the BCDR event might have been caused by or might be the cause of an Information Security Incident.
4. Depending on the criticality and complexity of the situation, the service representative may escalate to EOC management.
5. As needed, EOC management will then involve specific on-call IT staff and management to assist. The EOC will also be responsible for further escalations and on-going communication with appropriate upper level management.
6. The EOC will coordinate all necessary conference bridges and email correspondence throughout the outage / disaster.

In order for this process to work efficiently and effectively, we ask that you refrain from directly contacting individual IT staff members and IT management.

Emergency Information Phone Tree

Communication and notification processes are a key element to a viable business recovery solution. An Emergency Information phone tree has been established for our location to provide updates to staff during a significant business disruption.

During weather or emergency events, assigned staff members would call through the phone tree per their assigned responsibilities.

Recovery Personnel Contacts

In the event a system or application in a IN EB facility is operating in an anomalous fashion, the appropriate personnel in [Appendix A: Personnel Contact Information](#) will be called. They will determine the nature of the anomaly and if any additional personnel must be notified.

Damage Assessment Procedures

Operational assessment is made on all applicable hardware, software, and data at IN EB facility. The detailed Damage Assessment steps and checklist are documented in [Appendix C: Damage Assessment](#).

Incident Response Tracker

A high level guide for initial response is located in [Appendix B](#)

Recovery Status Report

In the event of a business disruption go to [Appendix C](#) and complete the Recovery Status Report form.

Media Protocol

A clear, concise, repeatable media protocol helps us best meet the needs of our state agency clients and the families we serve. Please follow the protocol highlighted below when contacted by any person from the media.







Do not answer any media questions!



IN EB will notify Media Relations at media@Maximus.com immediately to let them know that reporters are inquiring about the situation.

Maximus Pandemic Plan

A pandemic is described as a global disease outbreak that will affect an undetermined number of individuals. A pandemic flu occurs when a new virus emerges for which people have little or no immunity, and for which there is no vaccine. The disease spreads easily from person to person, causing serious illness or fatality. The World Health Organization (WHO) estimates that international air travel may cause the flu virus to infect all countries within three months of its emergence, regardless of where it originates.

A pandemic is another type of business interruption/disaster in which procedures must be followed. Maximus Pandemic Flu Plan will be used in conjunction with this BCDR plan, which includes moving the team to the Command Center and supported by the Corporate Command Center teams. Please refer to the Pandemic Flu Plan for specific step by step procedures.

Incident	Summary of Initial Action Steps
Power Outage 	<ul style="list-style-type: none"> Stay calm and communicate with others Continue operations normally, if safe to do so, under emergency battery power Retrieve and use flashlights or navigate by emergency lighting Wait until the situation can be fully assessed for cause and duration, at which point, act accordingly or as told to do so by local authorities or building management Obtain news and weather reports and emergency instructions through the use of an emergency radio or other battery-operated device in the event of a power outage
Fire 	<ul style="list-style-type: none"> Attempt to extinguish if small and safe to do so Notify others and evacuate the area or building Call 911 and/or pull fire alarm Account for all staff and visitors at pre-determined check-in sites in parking lot or nearby meeting place using staff list and visitor sign-in sheet
Virus, Cyberattack, or Sabotage 	<ul style="list-style-type: none"> Immediately unplug infected device and contact Maximus IT Security and Audit Department Contact ISO-IR@Maximus.com if there is a suspicion that the BCDR event might have been caused by or might be the cause of an Information Security Incident. Follow instructions to eradicate virus and then test equipment Follow up with preventative measures for future protection and obtain Maximus IT approval before re-connecting the device
Pandemic / Biohazards 	<ul style="list-style-type: none"> Follow advice of local health authorities and project best practices Work with fully operational secondary site to augment call center staff If feasible, allow staff to work from home to accomplish assigned activities Institute liberal leave policies as appropriate to encourage people to stay home if sick
Flood 	<ul style="list-style-type: none"> Notify others and move to higher ground if flash flood occurs Work from home and communicate with staff to stay home, if appropriate Obtain news and weather reports and emergency instructions through the use of an emergency radio or other battery-operated device in the event of a power outage
Inclement Weather 	<ul style="list-style-type: none"> Move to safe area as appropriate to the situation: <ul style="list-style-type: none"> Basement or lower level or inside room for tornado, away from windows Inside and away from windows and electrical equipment for a storm with lightning Heed hurricane warnings and stay home or evacuate as advised by local authorities Obtain news and weather reports and emergency instructions through the use of an emergency radio or other battery-operated device in the event of a power outage

Incident	Summary of Initial Action Steps
Earthquake 	<ul style="list-style-type: none"> ■ Move to safe area under doorways, inside, under heavy furniture to protect from falling ceilings or glass ■ Exit the building when safe to do so ■ Evacuate following the event until the building has been deemed safe to re-enter ■ Obtain news and weather reports and emergency instructions through the use of an emergency radio or other battery-operated device in the event of a power outage
Terrorist Attack 	<ul style="list-style-type: none"> ■ Notify authorities or emergency coordinator immediately. Call 911 when you are safe ■ Quickly determine the most reasonable way to protect your own life and the lives of others ■ Lock doors or evacuate the building if possible (help others evacuate if you can) ■ Run or escape (if possible), hide (if escape is not possible), fight (only as a last resort)

Evacuation

IN EB evacuation procedures are as follows:

- Evacuation graphics are on each floor in the elevator lobby ("YOU ARE HERE").
- Notify 911 of the location of mobility challenged persons during an emergency.
- Evacuation of the building occurs through the building stairwells located
 - Through front lobby, past the double glass door, immediately to the left
 - Through employee entrance, towards the restrooms, around the corner to the left across from male restroom
- All employees must check in with their Fire Warden or designated representative at their assigned safe assembly area.
- Once all persons are accounted for, the Tenant/Fire Warden or designated representative should report this to the fire department and to the IN EB Command Center.
- You must wait for an "all-clear" announcement from the fire department or building management prior to re-entering the building.
- During an evacuation, mobility challenged individuals should stay with their "buddy" near the stairwell entrance until emergency personnel arrive.

NO ONE SHOULD LEAVE THE PROPERTY DURING AN EMERGENCY UNTIL GIVEN PERMISSION BY EMERGENCY PERSONNEL.

Evacuating Mobility Challenged Occupants

The following procedures are to assist mobility challenged persons in this building:

NOTE: Mobility challenged conditions include pregnancy, broken appendages, epilepsy, and/or any other physical or medical condition.

- Supply a list of all mobility challenged persons to Fire Wardens and the IN EB Command Center. This list should include: 1) the person's name; 2) the floor on which he/she works; 3) the name of the "buddy" responsible; and, 4) the nature of the challenge.
- Fire Wardens should assign at least two people to be the mobility challenged person's "buddy". In this way, someone is able to be with and stay with the mobility challenged person at all times.
- In the event of an emergency, never leave the mobility challenged person alone. The "buddy" should always take the mobility challenged person to inside the nearest stairwell on his or her floor when there is smoke or fire; or if the Fire Department instructs everyone to leave the area.
- If the Fire Warden relocates mobility challenged persons, they must notify 911 and Core Recovery Team (Command Center) of the mobility challenged person's new location for evacuation out of the building.

Identified Safe Assembly Areas

Reference Safe Assembly Area locations in the IN EB Emergency Preparedness Guide.

Shelter-In-Place

Shelter-In-Place is a procedure where the entire building population is moved to a single or multiple location(s) in a building. Most commonly used during weather emergencies or when an extremely hazardous substance is released into the outside atmosphere.

Procedures

- Stay inside your building, or immediately go into the nearest building.
- Close all windows.
- Immediately go to your designated shelter area.
- Await further instructions from emergency personnel or your Emergency Team Member.
- DO NOT evacuate the building until you receive an "all clear" from emergency personnel.

Identified Shelter-In-Place Locations

Reference Shelter-In-Place procedures and locations in the IN EB Emergency Preparedness Guide.

Lockdown

A Lockdown of a floor, building, or group of buildings, is a procedure used when there is an immediate threat to the locations occupants. In the event of a lockdown, staff are instructed to secure themselves in the room they are in and not to leave until the situation has been curtailed. This allows emergency responders to secure the staff in place, address the immediate threat and remove any innocent bystanders from immediate danger to an area of safe refuge.

Procedures

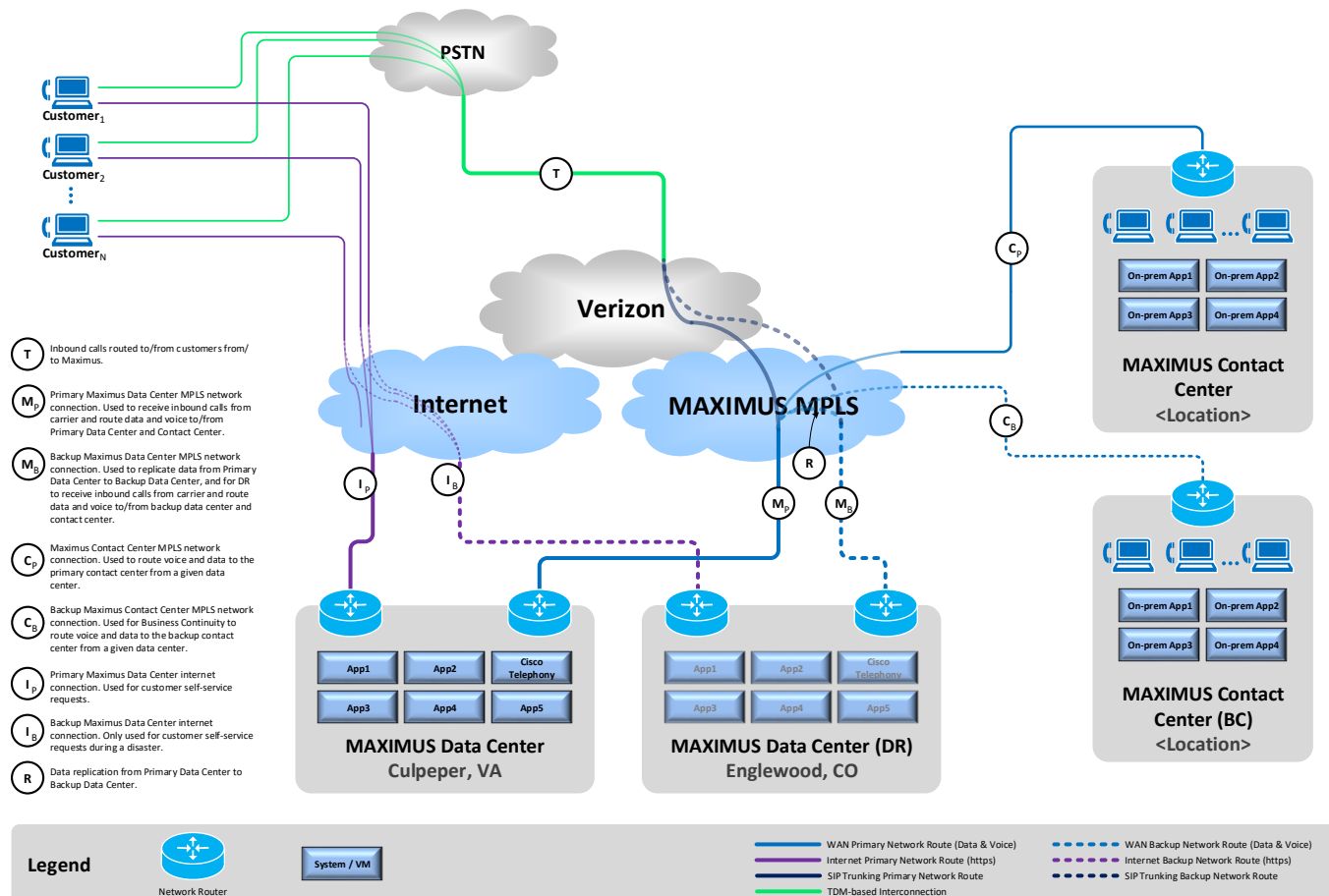
- Stay in your room or office and barricade the door.
- Remain quiet.
- Do not attempt to leave the building or room.
- Wait until emergency personnel give you an "all clear!"

SECTION 4 – RECOVERY

Disaster Declaration Procedures

Once a disaster has been confirmed via the Disaster Declaration Criteria noted above, and declared via the IT Escalation Process, the Project Manager will attend a Conference Bridge for status meetings with recovery personnel that has been set up by the IT Enterprise Operations Center (EOC) (IMT).

Network Diagram



	Network Topology View: <Program Name> BCDR	Created by: K. Erickson	Created: 06/22/16
		Updated by:	Last Updated:
		Approved by:	Approved:
		Category: Confidential *	Version: 1.0

View Template Version: NTV-011

* Contains proprietary and confidential trade secret information belonging to Maximus. Unauthorized distribution will be prosecuted under applicable civil and criminal laws.

Information Technology Incident Management

The IT Incident Management process administers all network related incidents. An incident is an unplanned interruption to an IT service or reduction in the quality of an IT Service. A Major Incident is a Priority P1 or P2 affecting production systems (service degradation or outage). The Service Desk provides Tier 1 and Tier 2 support for all IT Incidents. The Enterprise Operations Center (EOC) provides support on Major Incidents (Priority 1 and Priority 2), and any other incidents escalated by the Service Desk. The purpose of Incident Management is to restore normal service operation as soon as possible within the specified Service Level Agreements (SLA) and Operating Level Agreements (OLA).

The following process table will provide an overview of all the activities involved with Incident Management. The description column provides a brief explanation of the activity and calls out the name of the team or team member's role, in bold text, responsible for the step.

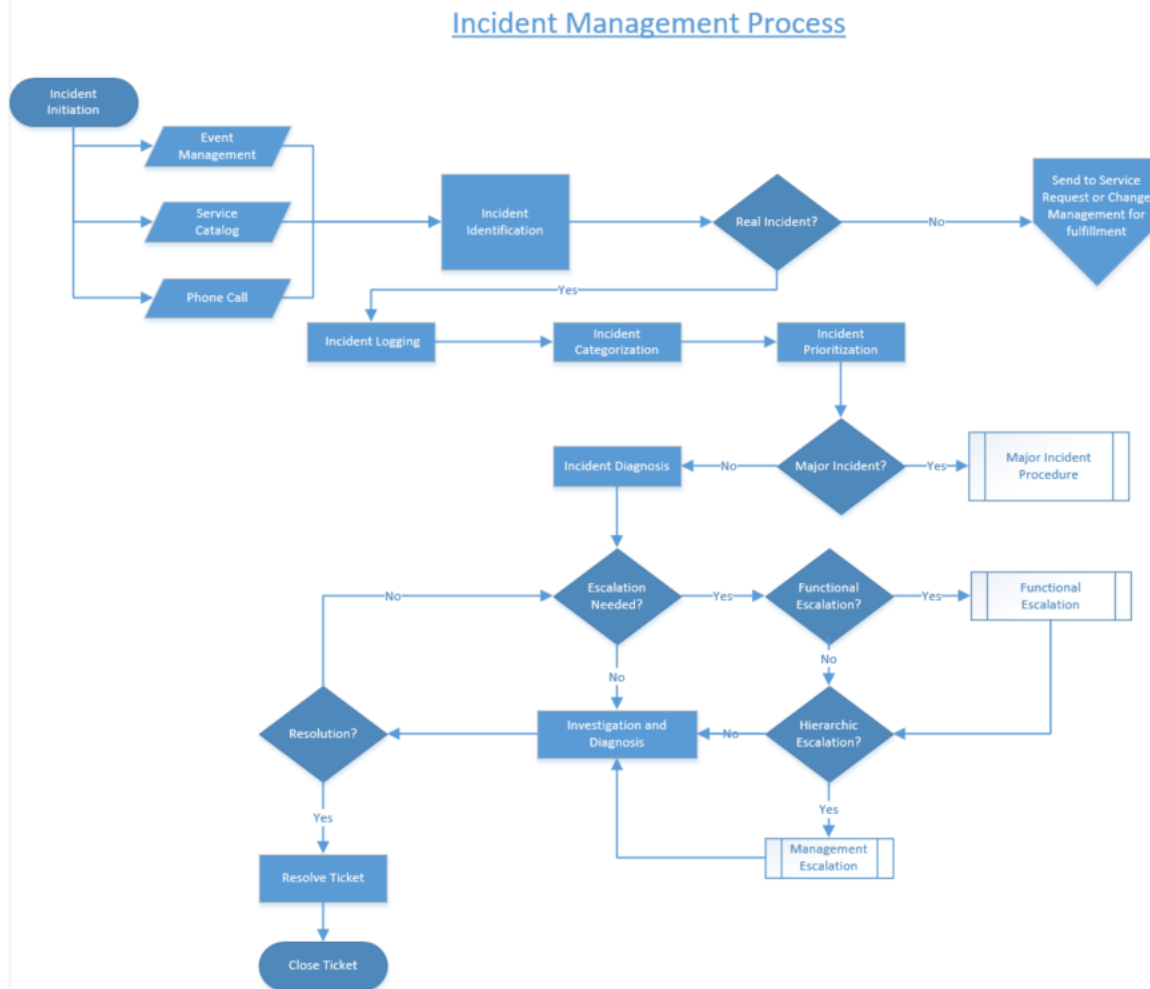


Table 1 Information Technology Incident Management Process Table

Incident Management Process

Step	Activity	Description
1	Identification	Incident reported by phone call to Service Desk (1-888-349-7762), self-service portal (https://itservicedesk.Maximus.com) or e-mail to itservicedesk@Maximus.com
2	Logging	Incident record is created in ticketing system
3	Categorization	Incident details, type, status, impact, urgency, etc. captured
4	Prioritization	Determined by support staff (Service Desk, Enterprise Operations Center)
5	Initial Diagnosis	Discover symptoms of incident and compare against similar incidents for quick resolution
6	Escalation (2 Types)	
6.1	By Scope	Enterprise Operations Center and on-call technical resources are engaged due to the scope and impact (see Major Incident Process)
6.2	By Access / Skill	Internal support escalation by the Service Desk
7	Investigation and Diagnosis	If no known solution, further investigation is required
8	Resolution and Recovery	Solution to incident found and service has been restored
9	Closure	Validation solution resolved incident

IT Major Incident Procedures

- An Incident is reported by phone call to Service Desk (1-888-349-7762).
- Requestor asks the Service Desk to escalate the Incident to Major Incident.

The general process includes:

- Troubleshooting the Major Incident
- Communicating with stakeholders
- Resolving the incident
- Creating a Root Cause Analysis (RCA), which communicates the analysis of the outage

STEP 1—Service Desk Tier 1

1. Assess the scope and impact of the outage.
2. Create a Cherwell ticket.
 - The ticket captures customer name, telephone number, Incident details, type, status, impact, urgency, Project(s) affected, Incident numbers for similar Incidents, Problem tickets, etc.
3. Escalate to Tier 2 via a warm handoff.

STEP 2—Service Desk Tier 2

1. Ensure the ticket information is complete.
2. If multiple Major Incidents are reported and are related, group the tickets by:
 - Adding a child link to parent tickets
 - Adding requestors and any other stakeholders to the communication tab of the parent ticket
 - Consult with Director, IT Resources if you are not sure if a new ticket is related.
3. Escalate to the EOC via warm handoff via Skype EOC group chat.

STEP 3—EOC

1. Take ownership of the ticket, set ticket status to “In Progress,” and engage the responsible BCM/IM following the process.
2. Discover symptoms of the incident and compare against similar, historic incidents and known errors in the Problem records, for quicker resolution.
Use the search function in Cherwell to look for similar incidents. Searches examples: server name, requestor, notes in prior tickets, etc. Also, look at recent incidents to see if this is a recently-occurred issue.
3. Begin Skype conferencing session, which is an invitation-only Skype bridge with the technicians and BCM/IM and Executive Manager that are troubleshooting.
 - Priority 1 Tickets:
 - Audio is required for all P1 Incidents.
 - Notify technicians and BCM/IM of the Incident details and provide instructions on how to join the Skype bridge call. Notifications must be sent to the on-call BCM/IM, VP Information Security, the VP’s managers, and Executive Manager all via MIR3.
 - If end users request additional distribution lists (DL) or people to be added to the business communication, the EOC (ticket owner) receives an email with the request. The EOC must inform the BCM/IM to add the DL or individuals or DLs on the business communication tab.
 - Priority 2 Tickets: EOC must open a dedicated Skype chat for every ticket.
 - EOC can change to Skype audio bridge, if determined it is needed.
 - Notify the on-call BCM/IM via MIR3.
 - If end users request additional distribution lists (DL) or people to be added to the business communication, the EOC (ticket owner) receives an email with the request. The EOC must inform the BCM/IM to add the DLs or individuals on the business communication tab.
4. Begin engaging the on-call SMEs as appropriate, depending on the scope and impact.
To engage SMEs, use the MIR3 BCM/IM Engagement Notification procedure. For instructions, see MIR3 Intelligent Notification in the Appendix.
5. As the EOC adds other SMEs/Tier 3 (such as Applications Administration, Networking), the EOC must create separate task tickets for each team to track their time and capture any corrective actions taken during the incident.
If necessary, the BCM/IM can set up a business-only Skype bridge to maintain communications with the appropriate business members.
6. Search Problem tickets for related incidents and link the Major Incident that is being resolved to an existing Problem ticket.

Notification

The EOC sets up notifications using the MIR3 notification tool. See MIR3 Intelligent Notification in the Appendix for instructions.

When the EOC sets the ticket to “In Progress,” this enables the Business Communication and engages the BCM /IM and SMEs. All business communications are generated from Cherwell for all P1 and P2 tickets.

The Executive Manager determines if Corporate Communications will be used on a P1 ticket.

Business Communication continues per the Service Level Agreement (SLA) as described in section **Error! Reference source not found.** Communication until normal service is restored.

Investigation and Diagnosis

1. EOC along with SMEs if engaged, troubleshoots and works towards restoration of service as quickly as possible.
EOC documents activities as described in the following list. Customers have complete transparency into the ticket work log through the IT Service Desk Self-Service Portal.
 - Update information in the ticket system Work Log and/or in emails from the ticket system.
 - Capture chat room transcripts and attach them as Work Log entries, or as new journal entries to the ticket.
 - Document any remediation or corrective actions into the bridge chat.

Resolution and Recovery

When the solution to the Major Incident is found, service has been restored, and the Requestor has verified Restoration, follow these steps:

1. EOC ensures all tasks are closed. Follow up with SMEs as needed.
2. EOC writes a detailed summary in the Resolution Details field and saves it. Summary may include, but is not limited to:
 - EOC documents troubleshooting steps and any corrective action taken in the ticket(s).
 - If sufficient evidence is gathered to provide a root cause for the incident, the EOC provides a summary of the evidence.
If a root cause is not determined, open a Problem ticket and set the Major Incident ticket to 'resolved'.
3. BCM/IM sends a Restoration message to the Major Incident DLs and appropriate stakeholders as specified in BCM field in the tickets.
4. EOC sets the ticket as resolved.
5. EOC completes a Root Cause Analysis (RCA) of the Major Incident (P1 required and P2 as requested) using the Cherwell RCA generating process. Refer to Creating an RCA in the Appendix.
 - EOC reviews and verifies the RCA content for accuracy and completeness
 - EOC creates a ticket for KM to review and puts a link to the RCA Tracker in the KM ticket.
 - KM reviews the RCA and approves it.
 - EOC in RCA Tracker prints the RCA to generate an Adobe Acrobat file (PDF) of the RCA.
 - EOC sends the PDF to management for review and approval.
 - EOC attaches the approved RCA PDF to the ticket and notifies the BCM/IM.
 - BCM/IM (or EOC if BCM was not assigned) sends the RCA as BCC to stakeholders in addition to the DL Maximus IT – RCA Delivery

Telecom

In the box below, is your site's current phone number and Direct Inward Dial (DID) number or 800 number—where your current phone number would be rerouted.

Facility Name and Existing Phone Number	Required Rerouting Action: No Rerouting Necessary, Auto Reroute, and Reroute to	DID Phone Number (List the Number where Calls Will be Rerouted)
IN EB Contact Center Local Number: Toll Free Numbers: Fax Number:	No Rerouting Necessary	No Rerouting Necessary

Telephone Script

We are sorry, but due to circumstances beyond our control, our call center is closed. You may still visit our website at <WEB ADDRESS> or press 1 to request a callback.

Offsite Storage

Required Resources	Location	Retention Period	Procedures for Retrieval
Data	Data is maintained in the Denver Primary Data Center. Backups are performed nightly and taken offsite weekly.	Ten (10) years	A request is sent via IT Help Desk to the offsite vendor for retrieval.
Paper	Paper documents are shredded after imaging		

SECTION 5 – RECONSTITUTION

Reconstitution is the process by which recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. A determination must be made on whether the systems have undergone significant change and will require a security reassessment and reauthorization. The Reconstitution Phase includes the detailed procedures for salvage operations, validating the system and data, normalizing operations, and terminating contingency operations. This phase consists of:

- Validating data at the alternate facility.
- Validating system functionality at the alternate facility.
- Validating full operational capabilities of the recovered critical functions.

Once the above activities have been completed, contingency operations are considered completed, and notification that the plan has been completed is sent to all affected parties.

System Functionality Validation

The system functionality must be verified by a System Developer/Maintainer or the System Administrator. System validation must ensure that the system can effectively and accurately process the data in the same manner as before the disaster.

Selected system users, project managers, network administrators and database administrator (if needed) will verify that infrastructure, system and application functionality has been tested and that the systems are ready to return to normal operations.

Data Validation

Data validation consists of comparing the pre-disaster data with the recovered data to ensure the available data in the recovered system is accurate, complete and effectively supports the reliant functions. Once the data has been restored from backups, and with any transactions processed during the Recovery Phase, backlogged transactions may be processed.

The following procedures will be used to determine that the data is complete and current to the last available backup:

- Validate timestamps on data files
- Review restoration report from data backup and recovery tool
- Compare a database audit log to the recovered database to ensure transactions were updated

Backlog Processing

As a result of the time elapsed from the point of the disaster, it is assumed that some amount of backlogged work will have been accumulated. A backlog may include:

- Accumulation of mailed documents that need to be scanned (onsite or on hold at local postal/parcel facilities);
- Mailed documents that were received and require processing, but cannot be salvaged due to the extent of the damage from the disaster;
- Voice mails that could not be accessed or retrieved, which require phone response;
- Electronic file submissions that were received but stored in a holding queue, and require routing; or
- Electronic file submissions that could not be received due to the impact of the disaster

Completing backlogs takes precedence over newer processing. In order to clear an accumulated backlog, the Business Owners will direct staff to begin processing accessible work. Stakeholders may be requested to resubmit specific collateral, which upon receipt is added to the accessible backlog. Once all backlogs have been cleared, the Business Owners are notified so that they can communicate to the user community or other stakeholders.

Attaining Normal Operations

Normalization is achieved when the system has been recovered, all data has been loaded and validated, and all backlogs have been processed. The Business Owner(s) are responsible for verifying normal operations. Upon successfully completing system testing and validation, the business owner (BO) or project manager (PM) will formally declare recovery efforts complete and that operations at the Maximus facility are functioning as normal. All BCDR Plan contact personnel will be notified of the declaration by the BO or PM (see [Appendix A: Personnel Contact Information](#)).

Terminating Contingency Operations

Once normal operations are achieved, contingency operations are terminated. When returning to the primary facility or pre-disaster state, the declaration authority will decide on the appropriate failback sequence that best serves the business. This includes:

- Failback in the same sequence which allows the longest time for all functions at the alternate processing facility before the second disruption; or
- Failback in reverse order, causing major disruption to the lesser critical processing but allowing additional opportunity for the most critical functions to continue processing before the second disruption; or
- Failback in a custom option that best benefits the organization.

Upon returning to normal system operations, Maximus Facility staff, customers and support contractors will be notified by the BO or PM using e-mail lists, subscriber lists or web page notifications as appropriate.

SECTION 6 – APPENDIX

Glossary and Acronyms

ACTIVATION: When all or a portion of the recovery plan has been put into motion.

ACD: Automatic Call Distributor

ARB: Advisory Review Board

ALERT: Notification that a disaster situation has occurred - stand by for possible activation of disaster recovery plan.

ATOD: At Time of Disaster

BUSINESS CONTINUITY MANAGEMENT (BCM): is defined in ISO 22301 as 'a holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

BUSINESS CONTINUITY PLANNING (BCP): A business continuity plan is a plan to continue operations if a place of business is affected by different levels of disaster which can be localized short term disasters, to days long building wide problems, to a permanent loss of a building.

BUSINESS CONTINUITY /

DISASTER RECOVERY PLAN: The document that defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals.

BCP CRITICAL: The highest rating of criticality. Applications \ Functions deemed BCP Critical will be recovered at the Recovery Vendor recovery site.

BUSINESS IMPACT ANALYSIS: The process of analyzing all business functions and the effect that a specific disaster may have upon them.

BUSINESS RECOVERY TEAM: A group of individuals responsible for maintaining and coordinating the recovery process.

CCC: Crisis Command Center

CERTIFIED BUSINESS CONTINUITY PROFESSIONAL): CBCP's are certified by the Disaster Recovery Institute, a not-for-profit corporation, which promotes credibility and professionalism in the DR industry.

CHECKLIST TEST: A method used to test a completed disaster recovery plan. This test is used to

determine if the information such as phone numbers, manuals, equipment, etc. in the plan is accurate and current.

CRISIS MANAGEMENT: The plans for and actions taken to protect and defend the reputation of the organization, its brand and its products/services.

CMS: Centers for Medicare & Medicaid Services

CMS: Call Management System

COLD SITE: An alternate facility that is void of any resources or equipment except air-conditioning and raised flooring. Equipment and resources must be installed in such a facility to duplicate the critical business functions of an organization. Cold-sites have many variations depending on their communication facilities, UPS systems, or mobility.

CONOPS: Concept of Operations

COMMAND AND/OR CONTROL CENTER: A centrally located facility having adequate phone lines to begin recovery operations. Typically, it is a temporary facility used by the management team to begin coordinating the recovery process and used until the alternate sites are functional.

CORPORATE GOVERNANCE: Corporate governance is a term

that refers broadly to the rules, processes, or laws by which businesses are operated, regulated, and controlled. Business Continuity Management is a key element in Corporate Governance, and may also include; Compliance, Risk, Vendor, Incident, and Audit management and controls.

CSR: Customer Service Representatives

DATA CENTER RECOVERY: The component of Disaster Recovery which deals with the restoration, at an alternate location, of data centers services and computer processing capabilities.

DATA CENTER RELOCATION: The relocation of an organization's entire data processing operation.

DATA GAURD: Oracle Data Guard ensures high availability, data protection, and disaster recovery for enterprise data.

DRC: Disaster Recovery Coordinator

DCS: Distributed Communications Services (clustered PBX network)

DDoS: Distributed Denial of Service

DECLARATION FEE: A one-time fee, charged by an Alternate Facility provider, to a customer who declares a disaster.

DISASTER: Any event that creates an inability on an organizations part to provide critical business

functions for some predetermined period of time.

DISASTER RECOVERY PLANNING: A process to recover and protect a business IT infrastructure in the event of a disaster.

DISASTER RECOVERY

COORDINATOR: The Disaster Recovery Coordinator may be responsible for overall recovery of an organization or unit(s). ALSO KNOWN AS CONTINGENCY PLANNER

DISASTER RECOVERY TEAMS

(Business Recovery Teams): A structured group of teams ready to take control of the recovery operations if a disaster should occur.

DNS: Domain Name Server

DRaaS: Disaster Recovery as a Service

F5: An Application Delivery Networking (ADN) technology that optimizes the delivery of network-based applications, and the security, performance, availability of servers, data storage, and other network resources.

FedRamp: Federal Risk and Authorization Management Program

A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

FTP: File Transfer Protocol

FULL RECOVERY TEST: An exercise in which all recovery procedures and strategies are tested.

GENERATOR: An independent source of power usually fueled by diesel or natural gas.

HOTSITE: An alternate facility that has the equipment and resources to recover the business functions affected by the occurrence of a disaster. Hot-sites may vary in type of facilities offered (such as data processing, communication, or any other critical business functions needing duplication). Location and size of the hot-site will be proportional to the equipment and resources needed.

INCIDENT MANAGEMENT: The plans for and actions taken to respond to a disruption of day-to-day operational activities - with the objective of returning to the original state.

ISSO: Information System Security Officer

ITIL: Information Technology Infrastructure Library

IVR: Interactive Voice Response

IXC: Inter Exchange Carrier

LDAP: Lightweight Directory Access Protocol

MAO: Maximum Allowable Outage: The maximum targeted time that mission critical processes can be disrupted without causing

significant harm to the organization's mission.

MAXe: Core Maximus processing system. Customer Relationship Manager.

MTD: Maximum Tolerable Downtime

MPLS : Multi-Protocol Label Switching, a data-carrying mechanism in computer networking

MISSION CRITICAL: Behind BCP Critical, mission critical status notes that a long term disruption to the application \ function would not materially impair the organization's ability to conduct business. Mission critical applications \ functions would not be recovered at the Recovery Vendor recovery site.

NAP: Network Access Protection The first public Internet exchange points (IXPs). Established by the National Science Foundation in the early 1990s, they were set up to provide a standard way to exchange packets for commercial backbones.

NOC: Network Operations Center

PRI: Primary Rate Interface

PRE MORTEM: A strategy in which a manager imagines that a project or organization has failed, and then works backward to determine what potentially could lead to the failure of the project or organization.

POST MORTEM: A project post-mortem is a process, usually performed at the conclusion of a project, to determine and analyze elements of the project that were successful or unsuccessful. Lessons learned.

PBX: Private Branch Exchange

QIC: Qualified Independent Contractor

RECORD RETENTION: Storing historical documentation for a set period of time, usually mandated by state and federal law or the Internal Revenue Service.

RECOVERY POINT OBJECTIVE (RPO): The point in time to which data must be restored in order to resume processing transactions. RPO is the basis on which a data projection strategy is developed.

RECOVERY TIME: The period from the disaster declaration to the recovery of the critical functions.

RECONSTITUTION: A process by which system operations are restored and resumed at the failover site.

RPO: Recovery Point Objective The RPO is the maximum targeted period in terms of hours, that data that can be lost without causing serious damage to a function.

RTO: Recovery Time Objective The maximum targeted period in terms of hours, in which an affected business unit must recover in order to not adversely

affect financial or functional objectives.

RISK ANALYSIS: The process of identifying and minimizing the exposures to certain threats which an organization may experience.

RISK MANAGEMENT: The discipline which ensures that an organization does not assume an unacceptable level of risk.

SaaS: Software as a Service

SALVAGE & RESTORATION: The process of reclaiming or refurbishing computer hardware, vital records, office facilities, etc. following a disaster.

SCOPE: Predefined areas of operation for which a disaster recovery plan is developed.

SFTP: Secure File Transfer Protocol

SMOKE TEST: Smoke Testing is a testing technique that is inspired from hardware testing, which checks for the smoke from the hardware components once the hardware's power is switched on. Similarly, in Software testing context, smoke testing refers to testing the basic functionality of the build.

SOP: Standard Operating Procedure

SPF: Systems Provisioning Form

SSIS: SQL Server Integration Services

TCP/IP: Transmission Control Protocol / Internet Protocol

TEST PLAN: The recovery plans and procedures that are used in a systems test to ensure viability. A test plan is designed to exercise specific action tasks and procedures that would be encountered in a real disaster.

Tier 1 Data Center: Non-redundant capacity components (single uplink and servers)

Tier 2 Data Center: Tier 1 + Redundant capacity components

Tier 3 Data Center: Tier 1 + Tier 2 + Dual-powered equipment and multiple uplinks

Tier 4 Data Center: Tier 1 + Tier 2 + Tier 3 + all components are fully fault-tolerant including uplinks, storage, chillers, HVAC systems, servers etc. Everything is dual-powered

UAT: User Acceptance Testing

UNINTERRUPTIBLE POWER

SUPPLY (UPS): A backup power supply with enough power to

allow a safe and orderly shutdown of the central processing unit should there be a disruption or shutdown of electricity.

VDI: Virtual Desktop Infrastructure

VDR: Virtualized Disaster Recovery

VITAL RECORDS: Records or documents, for legal, regulatory, or operational reasons, cannot be irretrievably lost or damaged without materially impairing the organization's ability to conduct business.

VIP: Virtual Internet Protocol

VM: Virtual Machine

VRF: Virtual Routing and Forwarding

VOICE RECOVERY: The restoration of an organization's voice communications system.

WAN (WIDE AREA NETWORK): Like a LAN, except that parts of a WAN are geographically dispersed, possible in different cities or even on different

continents. Public carriers like the telephone company are included in most WANs; a very large one might have its own satellite stations or microwave towers.

WARM SITE: An alternate processing site which is only partially equipped (As compared to Hot Site which is fully equipped).

WMS: Web Map Service

WMS: Windows Media Services

Work Recovery Time (WRT): The time it takes to get critical business functions back up-and-running once the systems (hardware, software, and configuration) are restored to the RPO; this includes the manual processes necessary to verify that the system has been restored to the RPO, and all necessary processes have been completed to address the remaining lost, or out-of-synch, data or business processes.

Zerto: Disaster recovery solution for virtualized infrastructures

Appendix A: Staff Contact Information

CONFIDENTIAL

Name	Title/Function	Phone Number(s)	Email	Contacted	Left Message	No Answer
NaKeita Boyd	Project Manager	O: 317-238-3111 C: 317-413-0898 H:		✓	✓	✓
Debbie Van Meter	Supervisor	O: 317-238-3132 C: 317-441-7260 H:				
Tierra Pinkins	Supervisor	O: C: 317-640-8242 H:				
Colleen Gilbank	Human Capital Specialist	O: C: 317-315-9661 H:				
James Mills	Field Services Technician	O: 317-238-3109 C: 765-624-6502 H:				
		O: C: H:				
		O: C: H:				
		O: C: H:				
		O: C: H:				
		O: C: H:				

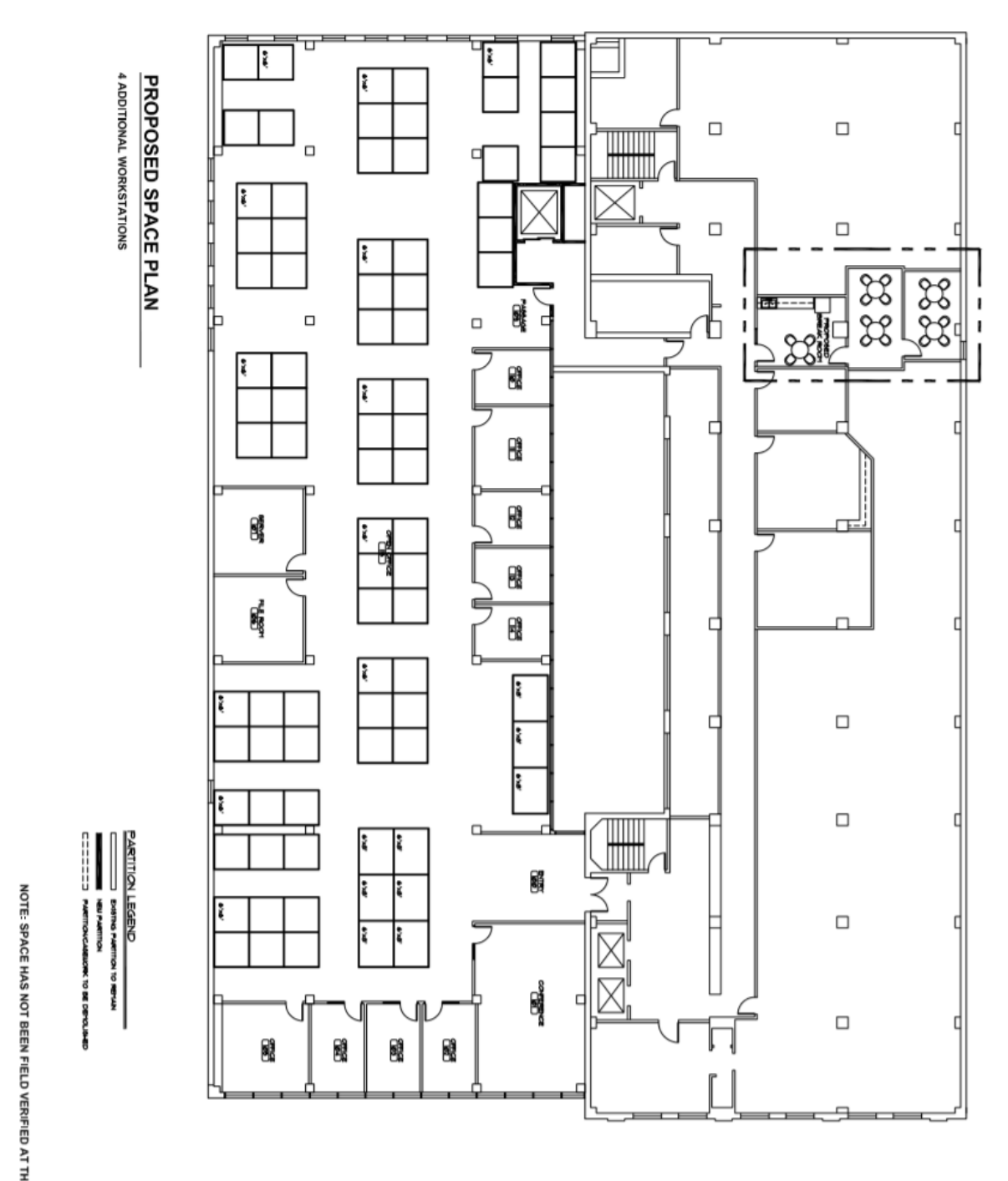
CONFIDENTIAL

Appendix B: Client / Vendor Contact Information
CONFIDENTIAL

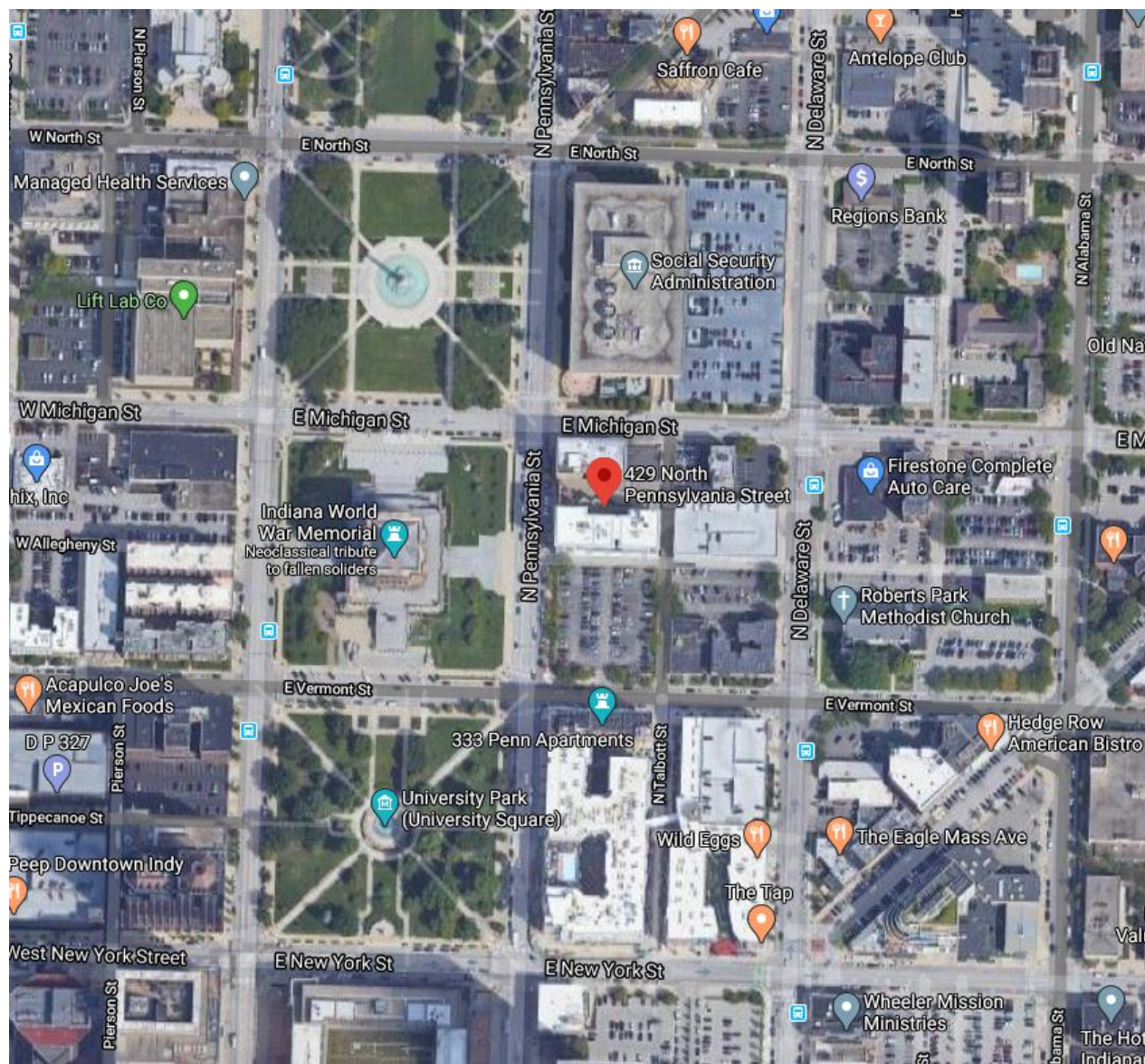
Vendor	Contact Name	Phone Number(s)	Email	Contacted		Left Message	No Answer
FSSA	Harold Ducote	O: 317-233-2834 C: 317-427-3501 H:	harold.ducote@fssa.in.gov	✓		✓	✓
FSSA	Meredith	O: 317-234-5780 C: H:	Meredith.Edwards@fssa.in.gov				
DX Enterprises	Josh Schimmel	O: 765-412-1429 C: 765-446-8610 H:	Josh.schimmel@gcgainc.com				
Engaging Solutions	James Hansen	O: C: 317-452-4835 H:	jhansen@engagingsolutions.net				
BCForward	Jessica Rutledge	O: 866-363-1132 C: 317-493-2019 H:	Jessica.rutledge@bcforward.com				
Stenz	Donna Grau	O: 317-262-4999 C: H:	dgrau@stenzcorp.com				
		O: C: H:					
		O: C: H:					
		O: C: H:					
		O: C: H:					

CONFIDENTIAL

Appendix C: Site Floor Plan



Appendix D: Site Aerial Maps and Driving Directions



Appendix E: Bomb Threat Checklist

Bomb Threat Checklist *(developed by Department of Homeland Security)*

CALL RECEIVER NAME:

TIME CALL RECEIVED:

PHONE NUMBER WHERE CALL RECEIVED:

TIME CALLER HUNG UP:

Ask the Caller

- Where is the bomb located? (building, floor, room, etc.)
- When will it go off?
- What does it look like?
- What kind of bomb is it?
- What will make it explode?
- Did you place the bomb? Yes No
- Why?
- What is your name?

Exact words of the threat

Information about caller:

- Where is the caller located? (background/level of noise)
- Estimated age:
- Is voice familiar? If so, who does it sound like?
- Other points:

Callers Voice

- ☐ Female
- ☐ Male
- ☐ Accent
- ☐ Angry
- ☐ Calm
- ☐ Clearing throat
- ☐ Coughing
- ☐ Cracking voice
- ☐ Crying
- ☐ Deep
- ☐ Deep breathing
- ☐ Disguised
- ☐ Distinct
- ☐ Excited
- ☐ Laughter
- ☐ Lisp
- ☐ Loud
- ☐ Nasal
- ☐ Normal
- ☐ Ragged
- ☐ Rapid
- ☐ Raspy
- ☐ Slow
- ☐ Slurred
- ☐ Soft
- ☐ Stutter

Background Sounds

- ☐ Animal noises
- ☐ House noises
- ☐ Kitchen noises
- ☐ Street noises
- ☐ Booth
- ☐ PA system
- ☐ Conversation
- ☐ Music
- ☐ Motor
- ☐ Clear
- ☐ Static
- ☐ Office machinery
- ☐ Factory machinery
- ☐ Local
- ☐ Long Distance

Other Information:

Threat Language

- ☐ Incoherent
- ☐ Message Read
- ☐ Taped Message
- ☐ Irrational
- ☐ Profane
- ☐ Well Spoken

Appendix F: Active Aggressor / Active Shooter

Active Aggressor / Active Shooter

Run when an active shooter is in your vicinity.

Hide if evacuation is not possible, find a place to hide.

Fight as a last resort, and only if your life is in danger.

Run

If there is an escape path, attempt to evacuate.

Keep your hands visible to law enforcement.

Evacuate whether others agree or not.

Leave your belongings behind.

Help others escape if possible.

Prevent others from entering the area.

Call 911 when you are safe

Hide

Lock and / or blockade the door.

Silence your cell phone.

Hide behind large objects.

Remain very quiet.

Your hiding place should be:

- Out of shooters view

- Provide protection if shots are fired in your direction.

- Not trap or restrict your options for movement.

Fight

Attempt to incapacitate the shooter.


Act with physical aggression.


Throw items and improvise weapons.

Commit to your actions.

First Responders


 When law enforcement arrives remain calm and follow instructions.


 Put down any items in your hands (bag, jacket, phone, etc.)

 Raise hands and spread fingers.

 Keep hands visible at all times.

 Avoid quick movements towards officers such as holding on to them for safety.

 Avoid pointing, screaming, or yelling.

 Do not stop to ask officers for help or direction when evacuating.

Immediate Action Steps to Consider

- ☐ Does the incident present a continuing danger?
- ☐ If the situation is ongoing, have someone stay on the line with the 911 operator.
- ☐ Obtain the physical description of the attacker, including distinguishing characteristics.
 - Provide law enforcement with the location of the active shooter.
 - Number of shooters.
 - Physical description of shooters.
 - Number and types of weapons held by shooters.
 - Number of potential victims at the location.
- ☐ Thoroughly search the area for missing or hiding staff / customers / visitors.
- ☐ Immediately dispatch Maximus Human Capital representatives to provide or assist law enforcement with serious injury / death notification(s).
- ☐ Provide security measures as appropriate.
- ☐ Provide professional help for staff and family to cope with the long-term effects of the trauma.

Unique Considerations

- Understand the plans for individuals with disabilities or other access and functional needs.
- Look for the two nearest exits anywhere you go, have an escape path in mind and identify places you could hide.
- Law enforcement may give early media statements. Coordinate Maximus messaging with theirs.
- Identify witnesses for law enforcement investigation.
- Protect the crime scene from any contamination that could obstruct law enforcement investigation.
- Call for external cleanup and repair services, as needed. Do not allow on-site employees to clean up a bloody crime scene.
- Identify the location of victims in the hospitals – they may be admitted under an alias (standard procedure for gunshot victims).
- Determine what to do with the desk / work area of fatally injured employees.
- When appropriate, let your family know you're safe.

RUN HIDE FIGHT – Department of Homeland Security Video

Appendix G: Disaster Recovery Box Inventory List

The Disaster Recovery Box is a 'Go Box' assembled by the project that contains items needed to carry out basic and initial life safety, communication, notification, and business continuity plan activation procedures during the first minutes and hours of a crisis event. At time of disaster, the Go Box should be available at the project site in a location that allows it to be retrieved 'on the way out the door'.

Business Continuity Disaster Recovery Plans, critical contact lists, and essential items that support initial recovery efforts should be included in the Go Box.

The items listed below are not required, but are recommended. We cannot always anticipate what type of crisis may hit and when. However, we can prepare ahead of time with the tools and processes that can provide a rapid response to a wide array of business disruptions.

Items for Consideration -

- ☐ Business Continuity Disaster Recovery Plan
- ☐ Contact Lists
- ☐ Emergency First Aid Kit
- ☐ Flashlights / Batteries
- ☐ Emergency Crank Radio
- ☐ Phone Chargers
- ☐ Laptop / Battery / Cable
- ☐ Duct Tape / Re-sealable Bags / Garbage Bags
- ☐ Whistle / Bullhorn
- ☐ Pens / Paper

Appendix H: Third Party or IN EB related Business Continuity / Disaster Recovery Plans

NA

Appendix I: Associated Documentation

Examples:

Contracts

EPG

Cyber Policy

Landlord Response Document

Regulatory Documents

Appendix J: Procedures Change Form

Document any changes to normal IN EB procedures during a recovery event.

(Print and save two-page hardcopies as appropriate) Ensure these changes do not carry over to normal operations following the 'return to home'.

Normal Procedure:

Short term change:

Manager Signature:

Date: mm

/dd

/yy

Normal Procedure:

Short term change:

Manager Signature:

Date: mm

/dd

/yy

Appendix K: Recovery Notes

(Print and save hardcopies as appropriate)

IN EB Incident Recovery Notes

The evolving facts must be captured for purposes of legal documentation.

Date: mm /dd /yy **Time:** a.m. ☐ p.m. ☐ (check one)

Impacting Event:

Discussion:

Decisions made: (By whom?)

Expectations:

Results:

Notes:

Appendix L: Incident Response Tracker

(Print and save two-page hardcopies as appropriate) Modify as needed for IN EB recovery response.

Date – Event Time – Senior Manager on site –

IN EB Initial Actions – Senior Person on Site

- ☒ Conduct a head count to make certain that all employees are accounted for.
- ☐ If necessary, contact emergency services by dialing 9-1-1.
- ☐ Call the MMS Service Desk at 888-349-7762 to initiate a Cherwell ticket to track event impact.
- ☐ Contact the Core Recovery Team members.
 - ☐ Business Owner –
 - ☐ Project Manager –
 - ☐ Local IT –
 - ☐ Local Facilities –
 - ☐ Operations Manager –
- ☐ Establish an Incident Command Center.
- ☐ Update the Emergency Information Line and direct staff to the number for updates.
- ☐ Initiate site control and determine if the site should be shut down.
- ☐ Do not move anything that could be classified as evidence.
- ☐ Ensure telephone coverage at the site. Restrict use of two way radios.
- ☐ Inform site personnel to direct requests from outside groups to you.
- ☐ Post workers to restrict entry to the site. Only those authorized will be permitted entry, and ID must be shown.
- ☐ Do not speak to the media until directed by Corporate Communications.
- ☐ If the site will be shut down, update the Emergency Information Line to advise staff on when to return to work.

IN EB Business Owner or Project Manager

- ☐ Determine what happened, when and where it happened, and who is involved.
- ☐ Verify the current status of the site (Is a clean shut down appropriate?).
- ☐ Identify witnesses and debrief as quickly as possible.
- ☐ Gather number and names of injured / fatalities and their family contact phone numbers.
- ☐ Initiate Core Recovery Team conference call.
- ☐ If needed, contact corporate and Legal, Human Capital.
- ☐ Notify Client of event and consult with them on plans for BCDR activation.
- ☐ Direct operations manager to reroute customer calls (if appropriate).
- ☐ Identify potential spin-off crises and be aware of secondary impacts.
- ☐ Designate someone to stay with the injured worker(s) at the hospital until family members arrive.
- ☐ Document the incident in writing (and on video recording if appropriate).
- ☐ Inform any surrounding areas that may be affected by the incident.
- ☐ Instruct staff at the incident site to contact their families to let them know they are okay.

IN EB Crisis Management in Coordination with Corporate

- ☐ Identify the audiences that need to be contacted for update purposes.
- ☐ Gather details on past negative issues which the media may refer to.
- ☐ Track all media coverage via a monitoring service and the Internet.
- ☐ Provide critical-incident stress counseling for employees who witnessed the incident or were nearby.
- ☐ Provide appropriate media updates in coordination with MMS Corporate.

Local or Corporate Spokesperson / Public Information Officer

- ☐ Write, and get clearance for, all statements and releases.
- ☐ Designate someone to screen your calls from the news media.
- ☐ Complete the media log sheets.
- ☐ Anticipate media questions.
- ☐ Assemble necessary background information and literature.
- ☐ Instruct reporters on your safety procedures before going on-site. If they violate any of the procedures, you have the right to ask them to leave.
- ☐ Advise reporters of a time and place for future updates.
- ☐ Follow-up on additional media inquiries.
- ☐ Conduct de-escalation meetings.
 - Ideally before staff leaves for home.
 - Provide current, appropriate information to staff
 - Collect information & Dispel rumors
 - Inform staff of next day expectations
 - Advise everyone not to discuss the event with media
- ☐ Schedule, Lead, Document, and Report on Incident.
 - Schedule timely status reviews.
 - Host the bridge call and direct the response efforts.
 - Document decisions made, by whom, when, why, expectations, and results.
 - Post incident – provide notes and lessons learned to BCDR team for After Action Report.

Executive Management

- ☐ Humanitarian Response.
 - Address the people related issues of a traumatic event.
 - Provide emotional first-aid during the initial management response
 - Ensure everyone is safe and accounted for
 - Protect staff from exposure to additional trauma
 - Make contact with victims and families experiencing traumatic stress reactions
 - Communicate status of event and its recovery
 - Consider a 'buddy system' for support in coping during the early aftermath
 - Provide critical-incident stress counseling for staff who witnessed the incident or were nearby.
 - Consider the response needs of affected family members.
- ☐ Maintain close contact with the Incident Commander to determine involvement.
- ☐ Approve all statements/communications to the outside world.
- ☐ Work closely with legal counsel.
- ☐ In the event of injury/fatality be prepared to make the visit/call to the family.
- ☐ In the event of a highly visible crisis be prepared to make the initial statement to the news media...with no Q & A.
- ☐ Establish and maintain communication with employee base and other audiences.

Appendix M: Recovery Status Report

Person Reporting: _____ Department: _____

Date: _____

Time: _____

Location: _____

Employee Health and Safety:

No Issues _____ or Assistance needed for: _____

Status of Condition: _____

Action Taken: _____

Department's Risk of Loss to the Company

Department's most critical function that is imperiled because of the incident:

Status of the function's operation: _____

Department's Recovery Status

List any resources needed for the recovery that are not immediately available.

Appendix N: Damage Assessment

Note: Please complete the form with the current information that is available.

Access/Safety/Security

- ☐ Open Access to Building
- ☐ Limited Access to Building – Explanation: _____
- ☐ No Safety Concerns
- ☐ Safety Concerns – Explanation: _____
- ☐ No Security Concerns
- ☐ Security Concerns – Explanation: _____
- ☐ Other Concerns: _____

Structure

Walls

- ☐ No Visible Damage
- ☐ Visible Damage – Explanation: _____

Floors

- ☐ No Visible Damage
- ☐ Visible Damage – Explanation: _____

Ceilings

- ☐ No Visible Damage
- ☐ Visible Damage – Explanation: _____

Equipment

Maximus Owned or State Owned? _____

Destroyed	Yes	No
Moved During Disaster	Yes	No
Water Leaks	Yes	No
Smoke Damage	Yes	No
Signs of Electrical Problems	Yes	No

Explanation: Mechanical/Utilities

Lighting

- ☐ Primary Working
- ☐ Primary Not Working – Explanation: _____

Backup

- ☐ Working
- ☐ Backup Not Working – Explanation: _____

Heating

- ☐ Working
- ☐ Not Working – Explanation: _____

Cooling

- ☐ Working
- ☐ Not Working – Explanation: _____

Ventilation

- ☐ Working
- ☐ Not Working – Explanation: _____

Plumbing

- ☐ Intact – Working Condition
- ☐ Ruptures – Leaking – Not Working – Explanation: _____

Services

Access

- ☐ Control – Key Pad/Card Access Working
- ☐ Key Pad Not Working – Explanation: _____

Fire Protection

- ☐ Sprinklers Not Activated
- ☐ Sprinklers Activated: – Explanation: _____

Power

- ☐ Working
- ☐ Not Working – Explanation: _____

Un-Interruptible Power Supply System

- ☐ Batteries Working
- ☐ Not Working – Explanation: _____

Circuit Breakers and Power Cables

- ☐ Not Damaged
- ☐ Damaged – Explanation: _____