Business Continuity Plan

1 | Introduction

Supporting Documentation & Reports
BIA Documentation Internal BCP Policies Threat/Risk Assessment Worksheet Recovery Teams Emergency/Manual Ops. Procedures Emergency Response Procedures

The Board of Directors/Trustees and senior management of InstitutionName (hereafter referred to as the "institution") are fully aware of their responsibility for establishing policies and procedures for comprehensive continuity planning. This business continuity plan (hereafter referred to as the "continuity plan", "plan", or "BCP") has been developed to fulfill this requirement.

No plan can specifically address every potential threat and/or event that may require the institution to activate all, or portions of, its business continuity plan. Therefore, this plan addresses a worst-case scenario and its framework can accommodate emergencies of lesser proportions.

1.1 | Plan Foundation

The institution recognizes that a thorough examination of its infrastructure, assets, and operations—as well as the many threats to which they are exposed—is the foundation upon which an effective, realistic business continuity plan must be developed. Therefore, the institution has conducted a business impact analysis (BIA) to identify the functions, IT systems, employees, vendors and service providers, data, documentation, and records most critical to its survival and ability to recover from a disaster. It has also conducted a threat/risk assessment (TRA) to identify and mitigate the risks associated with these critical resources.

It is based on the findings of the BIA and TRA (as detailed in 2 | Risk Assessment) that this plan has been developed.

1.2 | BCP Policy Statement

→ *If you **DO NOT** have a Board-approved policy, customize the following to define your specific requirements.*
→ *If you **DO HAVE** a Board-approved policy, delete the following and insert/attach, briefly detail, and/or refer to the existing policy.*

The institution's management and Board of Directors recognize the need to establish comprehensive business continuity policies to protect employees, customer/members, 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 institution also recognizes that increasing dependency on electronic data processing for operational support results in a corresponding risk, so that any prolonged loss of this resource could negatively impact overall performance and the institution's ability to continue operations.

It is the policy of the institution to develop and maintain a business continuity plan that will provide the institution with every opportunity to withstand a catastrophic event—whether accidental, malicious, or natural—and to resume total operations in an effective and timely manner. This plan has been developed to minimize the effects of a disaster through pre-planning and contains actions to be taken should an event occur, with or without warning, which causes an emergency to be declared. Its primary purpose is to provide for an orderly, timely resumption of business operations by clearly defining the facilities, resources, equipment, supplies, and documentation required to execute the plan, as well as their role in the recovery process.

The resources and functions of the institution have been identified and prioritized in terms of their criticality to overall operations (Business Impact Analysis). In addition, the technical, malicious, and natural threats and risks to which the assets of this institution may be exposed have been evaluated and ranked by probability and potential impact (Threat/Risk Assessment). These analyses indicate that the institution would experience major adverse effects if its ability to perform its intended functions were interrupted for as little as XXXXXX (XX) hours and therefore, the ultimate goal of this plan is to resume essential business operations and data processing within a XX-hour time frame, followed by the resumption of all operations and processing within one (1) week.

It is expected that, under the guidance of this plan, management will provide swift and decisive leadership, and employees will diligently carry out their tasks and fulfill their responsibilities in order to execute a successful and complete recovery. Additional policy goals include:

- Establish authority & responsibility for plan development, implementation, and maintenance.
- Provide emergency response procedures for identified threats.

- Document backup plans for hardware, software, documentation, and data files.
- Comprehensive strategies for emergency planning.
- Establish requirements for testing the adequacy and effectiveness of the plan.

1.3 | Special Considerations

In the context of this plan and all related documentation, the terms "business continuity", "continuity planning", "contingency planning", and "disaster recovery" all refer to the process by which an entire business or small business units re-establish operations and/or service to internal and/or external customer/users, while ensuring that (1) safety and soundness are maintained, (2) assets are protected, and (3) all regulatory requirements are met. These terms do not mean recreating the functional area as it currently exists or getting back to "business as usual". Rather, they refer to an interim step to resume a functional group's operational capabilities within a pre-defined timeframe, defined by its criticality and the risks associated with or the impact that a delay in its resumption would have on the entire institution.

In addition, the table below lists the generic terms that are used throughout this plan and provides the specific data that directly correlate to these terms. These terms are highlighted **IN BOLD** as they appear in this plan and all related documentation. Additional terms may be defined and used, as required.

BCP-Specific Terms & Designations — **Table 1.3a**

Generic Term	*Correlating Resource/Location/Data*
Operations Center	Refers to the institution's Main Office, Data Center, or any building where most/all critical units/functions and IT resources are housed. **LocationName** (StreetAddress, City, State)
President & CEO	**EnterName**
BCP Manager	**EnterName**, **EnterTitle**
Assistant BCP Manager	**EnterName**, **EnterTitle**
IT Team	Refers to the recovery team that is primarily responsible for overseeing systems restoration at the hotsite(s)/final recovery site. (**TeamName**)
DP Hotsite	**LocationName** (StreetAddress, City, State)
Command Center	**LocationName** (StreetAddress, City, State)
Core Provider	**CompanyName** (StreetAddress, City, State)
Disaster Recovery Provider	**CompanyName** (StreetAddress, City, State)
Telecommunications Provider	**CompanyName** (StreetAddress, City, State)
CAPlus Network Server/Drive	**IndicateLocation/Program Files/CAPlus/**

1.4 | Assumptions & Constraints

This plan has been developed on the following set of assumptions, which are based on the findings of the institution's business impact analysis (BIA) and threat/risk assessment (TRA). However, this plan also addresses exceptions to these assumptions, as required and where applicable, throughout this and all related, supporting documentation.

- The disaster will render all or part of the **Operations Center** unusable or inaccessible;
- The disaster will occur at the worst possible time;
- Current copies of the business continuity plan and all related documentation/data (e.g. BCP-CD) are readily available from offsite storage locations;
- Pre-determined hotsite locations will be available;
- The **DP Hotsite** and/or **Disaster Recovery Provider**(s) will perform according to all applicable, current contracts and agreements and will meet all legal obligations contained therein;
- Required personnel are available and understand their role in the execution of the plan;
- Current file backups are stored and readily accessible from offsite locations;
- Critical documentation is stored and readily accessible from offsite locations;
- Communication lines are available or can be purchased/installed within XX hours;
- Additional PCs and communications equipment/software can be purchased within XX hours;
- Required supplies are stored and readily accessible from offsite locations and/or vendors;
- The basic priorities for the restoration of essential services to the community will take precedence over the recovery of an individual organization;

- A general disaster will affect similar organizations and lessen the net effect on the institution, and;
- Vehicular transportation in the local area is possible.

1.5 | Minimum Requirements

In order to fulfill the goals and objectives and ensure the successful execution of this plan, the institution has made provisions for and will maintain the following requirements.

- Establishing a pre-arranged **Command Center** from which senior/executive management and BCP Management Team can conduct business.
- Establishing a pre-arranged **DP Hotsite** to house critical operations/functions of the institution, as well as any additional hotsite locations required for other critical functions/operations (e.g. Lending, Customer/Member Services) and/or displaced personnel.
- Ensuring availability of equipment and materials required to re-establish operations at the hotsite.
- Pre-assigning required personnel to their appropriate hotsite locations and pre-defining emergency notification procedures.
- Pre-defining the tasks required to be executed after the disaster and assigning them to personnel adequately trained and knowledgeable of his/her responsibilities regarding task completion.
- Ensuring that up-to-date, backup copies of critical data, files, programs, and documentation are stored and readily accessible at offsite/**DP Hotsite** locations.
- At a minimum, making current copies of this plan and BCP-CD available at all hotsite locations and providing all Team Leaders with a copy of the BCP-CD.
- Implementing adequate training programs to ensure that all involved internal and external resources understand their role and are prepared to complete their assigned recovery/reconstruction tasks in the event of an emergency.
- Ensuring provisions for secure transportation of personnel and materials.
- Ensuring that adequate, necessary funds are available to support the recovery.

1.6 | Responsibilities

In order to ensure that this plan remains current and viable, the institution and/or resources indicated below are responsible for ensuring that the following tasks are completed on an ongoing basis.

→ *The same resource may be responsible for more than one of tasks listed below.*

- **EnterResource**
  Training employees/required resources in BCP strategies and responsibilities.

- **EnterResource**
  Ensuring the **BCP Manager** receives required BCP data updates in a timely manner.

- **EnterResource**
  Maintaining the CAPlus database to a current status.

- **EnterResource**
  Ensuring the plan is in a current state at all times.
  Testing the plan as well as reviewing and approving the test plan prior to its execution.

- **EnterResource**
  Periodically reviewing the backup file creation, rotation procedures, and logs to ensure their viability.

- **EnterResource**
  At least annually, executing the CAPlus BCP maintenance (“Continuity/Monitoring/RM02-BCPMaintenance.doc”) procedure, which includes a review of the “Data Processing & Systems

Restoration Priority Lists", "Recovery Tasks", "Recovery Procedures", and "Emergency Operating Procedures," as well as all additional, supporting documentation and data, to ensure the accuracy of all CAPlus and BCP information.

- **EnterResource**
  At least annually, updating the Board regarding the status of the plan, testing results, and maintenance routines.

1.7 | CAPlus Documentation, Database, & BCP-CD

The institution's CAPlus database ("Data.mdb") and documentation ("Continuity" directory) is installed and maintained internally by the institution on the **CAPlus Network Server/Drive**. This plan contains the minimum information to illustrate the institution's disaster recovery/business continuity strategy, and is supported by reports generated from the CAPlus database that provide detailed information on the specific resource, equipment, and supply requirements of the institution. It is also supported by the following BCP-related documentation and data.

BIA	Contains all business impact analysis (BIA) documentation, including the suggested procedure and worksheet for conducting the BIA. This folder should also be used to store completed BIA interview forms.
Documentation	Contains the core BCP document ("ContinuityPlan.doc") and all supporting documentation (see below), such as hotsite/service provider contracts, BCPs, test results, and insurance coverage documentation.
Monitoring	Contains policies, procedures, and forms required for risk monitoring, including annual BCP testing, review, and maintenance procedures and supporting forms.
Procedures	Contains "Recovery Procedures" (from the CAPlus database) as well as the institution's emergency/manual operating procedures.
Threats	Contains threat/risk assessment (TRA) related documentation, including a procedure and worksheet to conduct the TRA, in order to identify threats and determine their probability of occurrence and potential impact.

All required/standard documentation and data is provided on the accompanying Business Continuity Plan CD ("BCP-CD"), which can be viewed/printed from any PC with a standard CD-ROM drive, printer connection, and Adobe Acrobat Reader installed. Additional supporting elements (e.g. IT compliance reviews, strategic plans, general policies and procedures, flowcharts, regulatory information, testing results) may be required/desired to support the institution's plan and copies may be stored internally by the institution or externally by vendors/service providers. The following table lists and indicates storage location/backup information for all supporting BCP-elements included with this plan.

Supporting Documentation & Materials	**Table 1.7a**
Document/Material Name	*Storage Location/Backup Information*
Departmental/Organizational Charts	**Location/VendorName** (StreetAddress, City, State)
IT/Communications Schematics	**Location/VendorName** (StreetAddress, City, State)
Emergency/Manual Operating Procedures	**Location/VendorName** (StreetAddress, City, State)
IT Policies & Procedures	**Location/VendorName** (StreetAddress, City, State)
Annual BCP Testing Results (Most Current)	**Location/VendorName** (StreetAddress, City, State)
External BCP Review Result/Reports	**Location/VendorName** (StreetAddress, City, State)
Regulatory Examination Results/Reports	**Location/VendorName** (StreetAddress, City, State)
Core Provider **Contract/BCP/Testing Results**	**Location/VendorName** (StreetAddress, City, State)
DP Hotsite **Contract/BCP/Testing Results**	**Location/VendorName** (StreetAddress, City, State)
Estimated Recovery Costs	**Location/VendorName** (StreetAddress, City, State)

Each year, the **BCP Manager** should oversee the review and update of the institution's continuity plan and supporting data/documentation, as described in 6.5 | BCP Maintenance.

NOTE: The beginning of each plan section contains a textbox listing the required and/or supporting data and documentation applicable to that particular section ("Supporting Documentation & Reports").

2 | Risk Assessment

Supporting Documentation & Reports
Threat/Risk Assessment Worksheet Recovery Teams Emergency/Manual Ops. Procedures Emergency Response Procedures

The institution recognizes that a thorough, realistic examination and assessment of its operations, including the many threats to which its financial, human, data, technological, and physical resources might be exposed and for which the cause may be natural (e.g. floods, hurricanes, blizzards), accidental (e.g. power outage, equipment failure), or intentional/malicious (e.g. fraud/theft, sabotage, terrorism), is essential to developing a solid business continuity plan.

In order to mitigate the risks to the stability and security of its facilities, data, IT and communications infrastructure, employees, customers, assets, and critical functions associated with such events, the institution has completed an extensive threat/risk assessment (hereafter referred to as the "TRA")

The institution has conducted a business impact analysis (BIA) in order to identify and prioritize the operations/functions, internal and external human resources, IT resources, documentation, data, records, and materials/supplies most critical to its survival and ability to recover from a disaster. It has also conducted a threat/risk assessment (TRA) to mitigate the risks associated with these critical resources, by identifying which catastrophic events are most likely to occur and which—should they occur—would have the biggest impact on the institution's ability to (1) maintain operations, (2) secure data, facilities, IT and communications infrastructure, and assets, and (3) ensure the safety of employees and customers.

2.1 | TRA Policy Overview

The institution recognizes that catastrophic events could expose its **Operations Center** to physical damage so severe that it would render the building inaccessible or unusable, and that a variety of threats to institution exist for which the cause can be either accidental (e.g. power outage, equipment failure) or intentional/malicious (e.g. fraud/theft, sabotage, terrorism).

The institution recognizes the importance of mitigating these risks and reviews/updates its Threat/Risk Assessment annually.

Click below to view the institution's most recent Threat/Risk Assessment worksheet:
..\Threats\TRA02-Worksheet.xls

2.2 | Emergency Response Procedures

Based on its most recent assessment/review, the institution has determined that the following threats pose the greatest risk to the institution based on factors such as its organization, mode of operations, asset size, services and products offered, technology infrastructure, facilities, and geographic location. Each has been assigned both a probability of occurrence and impact rating of high, medium, or low.

In support of the findings, Appendix A | Emergency Response Procedures contains procedures that have been developed to help the institution respond to these identified, potential threats/events in an attempt to minimize loss of human life and internal resources/assets.

Click below to view emergency response procedures for:

A.4 | Severe Weather & Natural Disasters
A.5 | Building & Equipment Emergencies
A.6 | Environmental Hazards
A.7 | Workplace Disruptions
A.8 | Loss of Workforce
A.9 | Workplace Addiction
A.10 | Labor Dispute
A.11 | Terrorism
A.12 | Systems Intrusion/Abuse
A.13 | Computer Virus Attack
A.14 | Power Outage/Blackouts

3 | Recovery Process

This section contains an overview of the entire recovery process from the events/circumstances that will lead to the declaration of a disaster, including either partial or full execution of this plan, to the renovation of the old/reconstruction of a new, permanent location. Although specifically developed to address emergencies affecting the institution's **Operations Center**, events affecting its branch locations and external processing/operating facilities, (e.g. service providers) are also briefly addressed.

Supporting Documentation & Reports
Facilities Recovery Teams Personnel/Internal Vendors/External Notifications/Recall Roster Emergency Response Procedure Recovery Tasks & Procedures Hotsite(s) Contract/BCP/Test Results Provider(s) Contract/BCP/Test Results

3.1 | Emergency Response & Recovery Procedure

The officer(s)-in-charge should ensure safe and secure emergency management, using all available, applicable procedures and resources in order to protect human life and property. Actions to be taken in response to specific emergency events are detailed in Appendix A | Emergency Response Procedures.

Once the situation is under control, the following sequence of events, (as detailed in "RP01-EmergencyResponse"), should occur under the direction of the **BCP Manager** and officer(s)-in-charge.

Emergency Response & Recovery Sequence Overview		**Table 3.1a**
01	**Disaster Declaration**	Assemble the BCP Management Team, relocate to the Command Center and evaluate the situation, determine the need to conduct damage assessment, and decide whether or not to declare a disaster.
02	**Damage Assessment**	As deemed necessary and once the area is determined to be safe, perform damage assessment routines according to "RP03-DamageAssessment", providing an estimated length of time and recommended course of action for recovery.
03	**Hotsite & Team Activation**	As deemed necessary, activate hotsite location(s) and notify Team Leaders. Upon notification, Team Leaders should retrieve all required recovery materials/equipment from offsite storage locations and meet at the Command Center. Once briefed on the emergency and course of action to be taken, Team Leaders should notify and assemble recovery teams at the pre-assigned hotsite location(s), ensuring the timely, accurate completion of assigned recovery tasks and responsibilities defined in this plan.
04	**Recovery Management**	Oversee the recovery of critical data processing and business functions from assigned hotsite location(s), including establishing appropriate security and/or medical attention at the damaged site(s), conducting team status meetings, and coordinating communications with media, customers/members, and employees.
05	**Reconstruction & Relocation**	Coordinate reconstruction of/return to the permanent site, ensuring a smooth, timely transition from recovery (hotsite) to normal (final recovery site) operations.
06	**Post Disaster Critique & Plan Update**	Develop a plan and conduct a post-disaster critique to evaluate the effectiveness of existing BCP strategies and recovery policies/procedures, updating BCP documentation in order to correct problem areas, as deemed appropriate. Replenish updated materials/documentation to all applicable locations/resources.

3.2 | Authorities & Emergency Quorum

Specific actions to be taken following the declaration of a disaster will be at the direction of the **President & CEO**. In his/her absence or incapacitation, the officers designated below, in the order-listed and dependent upon their availability, will assume the leadership role until the designated officer or an officer higher on the list becomes available.

*** Chain Of Command ***		
Executive	**Title**	**Home Phone**
President&CEOName	President & CEO	(000) 000-0000
EVPName	EVP	(000) 000-0000
SVPName	SVP	(000) 000-0000

**Any available officer/senior manager.*

In the event of an emergency/disaster of such proportion that the duly-constituted officers of the institution are unable to function, the applicable provisions of the by-laws shall be suspended and the affairs of the institution shall be conducted as herein provided, so far as permitted by law.

- *Assignment of Duties* | The Board may temporarily assign the duties of an officer to another officer and delegate such duties to that person, as it deems necessary.
- *Quorum* | Available members of the Board shall constitute a quorum that has absolute authority during the emergency, according to the provisions in the institution's By-Laws.
- *Quarters* | If the institution's quarters are so damaged as to render them unusable, the Board shall procure temporary offices out of which to conduct the business of the institution until permanent quarters can be obtained and made ready for occupancy.

3.3 | Plan Activation & Scope

Internal Disasters/Emergencies | The following scenario/response pairs address plan activation procedures for emergencies affecting the institution's **Operations Center**.

Scenario A: If the entire main building/facility is destroyed and/or inaccessible:
→ **BCP WILL BE INVOKED TO THE FULLEST**

Executive and senior managers will report to the **Command Center** and operations will be moved to the **DP Hotsite**. All **Operations Center** staff and branch personnel will report to their hotsite locations.

Scenario B: If the **Operations Center** is destroyed and/or inaccessible:
→ **MOST OF THE BCP WILL BE INVOKED**

Operations will be moved to the **DP Hotsite** and staff working in affected areas will report to their assigned hotsite locations. Staff working in safe, non-damaged areas will report to their normal work locations.

Scenario C: If one or more of the branches is destroyed/inaccessible (including the Main Office):
→ **PARTS OF THE BCP WILL BE INVOKED**

Currency, negotiable papers, and other files (still intact) will be transferred by armored car from the damaged branch to the nearest branch location (or other appropriate, designated location). Teller operations will be absorbed by non-affected branches/locations. Assignments and decisions will be made at the discretion of the officer-in-charge.

External Disasters/Emergencies | The following scenario/response pairs address plan activation procedures for emergencies affecting external locations and/or resources critical to the institution's functions and operations (e.g. providers of outsourced functions/processes, correspondent institutions).

Scenario A: If a disaster occurs at the **Core Provider**'s facilities:
→ DescribeResponse

Provide additional details here, as necessary.

Scenario B: If EnterCondition:
→ DescribeResponse

Provide additional details here, as necessary.

Scenario C: If EnterCondition:
→ DescribeResponse.

Provide additional details here, as necessary.

3.4 | Hotsite/Alternate Locations Overview

Hotsites are temporary, pre-assigned locations used to house business operations and personnel in the event of a disaster until the original or a new location is made available. During an emergency, most, but not all, employees displaced by damage to the **Operations Center** will be required to report to work and have been pre-assigned to a hotsite location. Furthermore, all cash, safe deposit boxes, and negotiable papers still in existence at the **Operations Center** will be moved by armored car to a secure location at the discretion of the officer-in-charge. All other files that are still intact will be removed and stored at available institution and/or hotsite locations.

Command Center | Executive and senior officers normally housed at the **Operations Center** will relocate to this site from which they, along with the rest of the BCP Management Team, will direct and oversee the recovery effort. This site will also serve as the central location for team status meetings.

DP Hotsite | Briefly describe the terms of the hotsite provider contract/setup of the branch hotsite location, as well as the measures taken to ensure a quick and successful recovery (e.g. mirrored servers, regular file backup and rotation procedures, employee awareness). As required, supplement the BCP by including electronic copies of the entire, or applicable parts of, the hotsite provider contract(s) on the BCP-CD.

4 | Recovery Teams & Responsibilities

Supporting Documentation & Reports
Facilities Recovery Teams Personnel/Internal Vendors/External Notifications/Recall Roster Internal Organizational Charts Recovery Tasks & Procedures Emergency/Manual Ops. Procedures Hotsite(s) Contract/BCP/Test Results

The recovery process is managed and directed by the BCP Management and/or Executive Teams, which receive support from the departmental recovery teams in their efforts to restore critical systems, operations, and functions after an emergency is declared.

The departmental recovery teams, comprised of key members of the institution's most critical operating departments and functions, will continue to perform their normal functions to the degree that space and resources allow. Furthermore, at a minimum, one (1) backup/alternate member is assigned to each recovery team in the event that key personnel are not available. Additional backup/alternate members may be assigned, as required. Each backup/alternate member is trained to fulfill all leader/member responsibilities.

Departmental recovery teams are generally responsible for:

- Ensuring normal duties/functions operate as efficiently as possible during the recovery process.
- Restoring normal operations for their department/function as quickly as possible.
- Assisting in the completion of "Recovery Tasks", as directed by the designated team leader.
- Carrying out the directives of the BCP Management and/or Executive Teams.

In addition to these general tasks, the departmental recovery teams have objectives and responsibilities in the recovery process specific to the operational units and functions they represent. Teams and a brief overview of their responsibilities are listed in the following table.

Recovery Teams Overview **Table 4.0a**

Team Name	*Responsibilities*
IT Team	Describe team responsibility here.
EnterDepartmentTeamName	Describe team responsibility here.
EnterDepartmentTeamName	Describe team responsibility here.
EnterDepartmentTeamName	Describe team responsibility here.
EnterDepartmentTeamName	Describe team responsibility here.

Some tasks need to be performed because of the emergency and have nothing to do with the normal operations of the institution, namely those related to damage assessment, reconstruction, and public relations. The BCP Management and/or Executive Teams are primarily responsible for overseeing the completion of such tasks. Furthermore, a number of external resources (e.g. vendors, authorities) may be required to assist the internal recovery teams in the completion of assigned tasks. These resources make up the "External Teams". The organization and responsibilities of the BCP Management, Executive, and External Teams are detailed in the following sections.

4.1 | BCP Managers

Two members of the BCP Management Team have been appointed to the roles of **BCP Manager** and **Assistant BCP Manager**. The **BCP Manager** will interact directly with the recovery teams to manage the recovery process. The **Assistant BCP Manager** will assist the **BCP Manager** as directed and assume the duties of the **BCP Manager** in the event that he/she is absent, incapacitated, or otherwise unable to fulfill his/her responsibilities. The **BCP Managers** will:

- Assess the damage, write the initial report, and present findings to the BCP Management Team.
- Activate the plan and initiate the recovery process, including notifications.
- Ensure regulators (e.g. FDIC, FED, NCUA), correspondents institutions, authorities (e.g. Police/Fire Departments, FBI), and insurance agencies are aware of the emergency situation and kept informed of the institution's status and actions throughout the recovery process.
- Coordinate recovery team activities and status meetings.
- Monitor/Document the recovery and reconstruction processes.
- Report recovery/reconstruction status to the BCP Management Team.

4.2 | BCP Management Team

The BCP Management Team, comprised of the **BCP Managers**, senior officers, and managers, is responsible for providing overall guidance and direction throughout the recovery process and, under the guidance of the Executive Team, major decision-making and status reporting to the Board. Immediately upon notification, the BCP Management Team, under the direction of the **BCP Managers**, will:

- Proceed to the **Command Center** location.
- Review the findings of the damage assessment to ascertain the impact of the disaster, determine the areas affected, and estimate the length of time that service will be disrupted.
- Assess the situation and decide upon the mode of recovery operations, including activation of the recovery teams and hotsite location(s). If the emergency/damage cannot be handled normally, the BCP Management Team will activate all or part of this plan, as described in 3.3 | Plan Activation & Scope.
- Coordinate all legal matters through counsel.
- Receive all requests for space, equipment, supplies, and personnel support and locate workspace for critical functions/personnel, as required.
- Update emergency response telephone messages.
- Manage/oversee the recovery and reconstruction processes.
- Notify and provide status updates to the Executive Team.

4.3 | Executive Team

The Executive Team, comprised of the **President & CEO** and his key executive officers, is responsible for decision-making and communicating recovery status to the Board. The Executive Team will:

- Make all, final recovery/reconstruction decisions.
- Approve and/or draft all media press releases and customer/member correspondence, updates, and notifications.
- Monitor media/news reports of the disaster.
- Notify/delegate responsibility for notification/status reporting to regulatory agencies.
- Provide necessary funds for recovery.
- Ensure the institution's financial liquidity and that adequate financial controls are in place.
- Notify and provide status updates to the Board.

4.4 | Team Leaders

Team Leaders act as a liaison between the BCP Management Team and their respective recovery team(s) in order to provide central control. Immediately upon notification, the Team Leaders, under the direction of the **BCP Managers**, will:

- Notify and assemble their respective recovery teams at the pre-assigned hotsite location(s).
- Oversee the progress of all recovery operations/tasks assigned to their team.
- Notify applicable primary vendors/service providers and request priority/standby support.
- Provide status reports to the **BCP Manager**.
- Forward requests for additional space, equipment, and/or resources to the **BCP Manager**.
- Receive status reports from the **BCP Manager** and disseminate them to Team Members.
- Analyze work requests and forward them to the appropriate person/team. Requests typically come from the **BCP Managers** or other recovery teams in need of assistance.
- Assign knowledgeable staff to assist **IT Team** with the installation/testing of applicable systems/programs.
- As conditions allow, begin to expand functions and call back staff.
- Assist in the institution-wide, business recovery.

4.5 | External Teams

The External Teams consist of vendors, service providers, local and national agencies, industry-related, and other resources required to assist the institution in the execution of this plan and the required recovery tasks and procedures. Required external resources may include, but are not limited to:

Accounting Firms
Appraisers
ATM Services/Suppliers/Support
Audit Firms
Banking Agencies/Associations
Building Contactors
Communications Providers
Consultants
Correspondent Institutions
Courier/Messenger Service Providers
Credit Bureaus
Credit Card Services/Providers
Customer/Member Service Providers
Educational/Training Providers
Employment Agencies
Equipment Vendors/Servicers
Facilities Maintenance Providers
General Office Suppliers
Government Agencies
Health/Dental Care Providers
Hotsite Providers
Human Resources Support
Insurance Providers
Investment/Securities Firms
IT Service Providers
Law Enforcement
Legal Counsel/Attorneys
Lending Support Service Providers
Lodging
Medical Suppliers/Service Providers
Miscellaneous/Other
Office Support Service Providers
Payroll Service Providers
Printers/Copy Service Providers
Public Relations/Marketing Firms
Publishing Firms/Publications
Records Management/Storage Providers
Security Suppliers/Service Providers
Shareholders
Software Vendors/Service Providers
Transportation Providers
Utility Service Providers

5 | IT Environment & Recovery

Supporting Documentation & Reports
Facilities
Workstations/Seats
IT Schematics/Flowcharts
Materials/Documentation
IT Catalogs (Optional)
Recovery Tasks & Procedures
Emergency/Manual Ops. Procedures
Data Backup & Security Procedures
Hotsite(s) Contract/BCP/Test Results
Provider(s) Contract/BCP/Test Results

This section provides an overview of the institution's IT, data processing, and operations environment, as well as the DP recovery process from the restoration of critical systems at the hotsite to the transition back to normal operations at the final recovery site.

The institution's **Core Provider** provides most of the data processing needs for the institution's critical operations, including Functions/Operations.

→ Include electronic copies of all applicable supporting documentation on the BCP-CD (e.g. data backup/information security procedures, hotsite and service provider contracts and BCPs, IT and communications infrastructure schematics for normal operations/at the hotsite) or indicate where these resources can be accessed in "Table 1.6a" in 1.7 | CAPlus Documentation, Database, & BCP-CD.

5.1 | IT Infrastructure & Operations Overview

In addition to the services, systems, and applications provided by the institution's core banking provider, critical operations are supported by a network of additional systems, online services providers, in-house applications, and operating systems.

Requirements for the workstations, hardware, software, devices, and connections supporting the institution's IT infrastructure and operations are defined in the CAPlus database and detailed in applicable reports and supporting documentation included on the accompanying BCP-CD.

5.2 | Branch Network (WAN) Overview

The branch network is used to process online customer/member transactions and is a top priority of the institution requiring immediate attention in the event of an emergency. Any disruption of this service could cause customer/member inconvenience and dissatisfaction.

Requirements for the workstations, hardware, software, devices, and connections supporting the institution's WAN are defined in the CAPlus database and detailed in applicable reports and supporting documentation included on the accompanying BCP-CD.

5.3 | Communications Network Overview

The institution's communications network is a top priority of the institution requiring immediate attention in the event of an emergency. Its primary **Telecommunications Provider** provides the institution with call routing and control for all its telephone communications systems.

Requirements for the workstations, hardware, software, devices, and connections supporting the institution's communications network are defined in the CAPlus database and detailed in applicable reports and supporting documentation included on the accompanying BCP-CD.

5.4 | Data Backup Summary

The success of the institution's recovery from a catastrophic event depends largely on its diligence in creating, maintaining, and implementing data backup procedures. To ensure that the institution will be able to recover from a disaster with minimum loss of critical data, complete and viable backups of the systems housing internal data will be executed and stored at appropriate offsite locations on a strict schedule and regularly tested for their ability to be fully, safely restored. A summary of the institution's backup and rotation procedures for critical servers/equipment is provided in the following table.

→ Complete the following table with information specific to your data backup policies and procedures.

Backup Procedures Overview — **Table 5.4a**

Backup Procedure (Description/Software/Responsibility)	*Frequency/Media*	*Storage Location(s)/Rotation/Additional Info*
Mainframe		
Core Provider **System/Data**		
PC File Server		

LAN/WAN Server		
E-mail Server		
Reporting System		
Statement Run		
End-of-Month		
Pre-Release Backup	As Required	
Pre-Installation Backup	As Required	
Standalone/User PCs	Server / CD-ROM At user's discretion	Individual users are responsible for the backup of critical files and applications residing on their local hard drives. They are encouraged to store these files on the server so that they are included in regular server backups and/or to backup to periodically backup their files to disk/CD and store them in a safe, offsite location (e.g. user's home).

5.5 | DP & Operations Recovery Sequence

Immediately upon the declaration of a disaster and subsequent activation of the hotsite, the following sequence of events will be initiated by the **IT Team** in order to restore operations at the hotsite. Upon request of the **IT Team**, Team Leaders will assign personnel to assist in the testing of restored systems.

DP & Operations Recovery Sequence Overview		**Table 5.5a**
01	**Backup Retrieval**	Retrieve backup media and files from their offsite storage locations (identified in 5.4 | Data Backup Summary).
02	**Hotsite Activation**	Notify/Activate the hotsite(s) and send the most current available backups to the appropriate processing/backup facility locations.
03	**Equipment Inventory**	Inventory PC and server hardware and software and communications lines/devices required at the hotsite and place orders for missing/damaged items, immediately.
04	**Primary WAN Restoration**	Restore primary online services to the branches from the hotsite by [BrieflyDetail] and create a working environment for XX users.
05	**Critical Systems Restoration**	Restore critical systems, applications, including connectivity to outside service providers, in the order designated in the "Systems Restoration Priority List" (detailed in 5.6 | Data Processing & Systems Restoration Priority Lists).
06	**Departmental Recovery**	As systems are made available, affected departments will be notified and required staff will report to and work from the hotsite. Functional departments will be recalled in the order designated in the "Data Processing Priority List" (detailed in 5.6 | Data Processing & Systems Restoration Priority Lists).
07	**Hotsite Support & Operations**	Once the hotsite is made fully operational, support for hotsite operations will be provided by the appropriate team/resources. Hotsite operations will continue until the final recovery site is made available.
08	**Final Recovery Site Restoration**	Once the old/new permanent location is made available, the appropriate resources will work to fully restore operations at the final recovery site.

5.6 | Data Processing & Systems Restoration Priority Lists

Due to limited resources, it may become necessary to follow a priority sequence when allocating DP systems/resources at the hotsite. Priorities, as detailed in the following tables, are based upon the results of the institution's BIA, which included an assessment of the time that each department can operate without systems support before the loss of its function(s) begins to negatively impact the institution's ability to meet the demands and expectations of its customers/members and community.

→ Complete the following tables with information specific to your data processing and systems restoration priorities.

Data Processing Priority List		**Table 5.6a**
Department/Function	*CL*	*Criticality Rating*
	01	**Immediate**

	02	**Within 24 Hours**
	03	**Within 48 Hours**
	04	**Within 72 Hours**
	05	**Within 1 Week**
	06	**Within 2 Weeks**

Systems Restoration Priority List	**Table 5.6b**
CL	*System/Service*
01	
02	
03	
04	
05	
06	
07	
08	
09	
10	

6 | Risk Monitoring

Supporting Documentation & Reports
Internal BCP Policies Risk Monitoring Procedures

The institution's Board and senior management understand their responsibilities to arrange and oversee the annual testing, review, and updating of the BCP document and all related data and documentation. Furthermore, the institution recognizes the need to update and retest the BCP anytime significant changes are made to its organizational structure, operations, and/or IT environment.

6.1 | BCP Testing

At least annually, and as deemed necessary, the institution will develop an overall BCP test plan that includes objectives, scripts, schedules, and review/reporting of test results. Testing procedures will include the participation of required personnel, as well as backup/alternate personnel in order to ensure a smooth recovery in the event that key individuals are not available. Tests will also include all critical external resources (i.e. External Teams). The following issues will also be addressed:

- Criticality of service/departments
- Volume of transactions
- Interdependencies between internal and external (e.g. outsourced) business functions/systems
- Availability and adequacy of required resources to provide planned level of service
- Ability to recover and restore backup data and applications
- Duplication of tested backup media in case problems are encountered during testing
- Normal business operations will not be jeopardized and data is secure
- Deviation from scripts to test unplanned events
- Reporting and conflict resolution for test results
- Independent/third-party participation, oversight, and/or review

6.2 | Testing Methodology

The institution has adopted and adheres to the following testing methodolog(ies), which have been chosen based upon resource availability, size, complexity, and services offered. The institution will primarily utilize **IndicateTestingMethod** testing. Additional methods may be used, as deemed necessary, in conjunction with or independently of the primary method.

→ Add, delete, and/or edit items and descriptions below to best describe your institution's testing methodologies.

Walk-Through	Discuss/walk-through plan in conference room setting, including individual/team training and clarification/highlighting of critical elements, to ensure critical/key personnel are familiar with BCP and understand their role(s) its execution.
Tabletop/Mini-Drill	Identify specific event scenario(s) and apply the BCP to each to practice and validate functional response capabilities, evaluating individual/team knowledge of responsibilities through limited simulation of hotsite activation, recovery team mobilization, and emergency notification sequence(s).
Full-Scale Testing	Implement all/portions of the BCP by processing data/transactions using actual backup media at the hotsite, including validating recovery procedures/functions and DP test scripts and evaluating team/individual knowledge of responsibilities and practicality of BCP through role playing/simulation of hotsite activation, recover team mobilization, emergency notification sequence(s), release of member/customer and media communications, hotsite operations, interaction with external teams/resources. Full-scale testing is conducted over a sufficient time-period to allow issues to fully develop as they would in a real emergency.

6.3 | DP Hotsite Requirements & Testing

The **BCP Manager** will ensure that the **DP Hotsite**'s documentation of the institution's workstation, hardware, software, and communications requirements is current and up-to-date. Furthermore, the **BCP Manager** will also ensure that the appropriate changes are made to the institution's contract with the **DP Hotsite** as changes occur that affect configuration/processing requirements (e.g. major conversions, server upgrade).

In addition to maintaining documentation of requirements, live testing is required to ensure that IT resources (e.g. servers, workstations, communications devices/lines) are properly configured to support hotsite operations. Therefore, at least annually, the **BCP Manager** will work with required internal and external resources to test and validate the institution's ability to successfully restore the required systems, applications, and connections at the hotsite(s). Prior to testing, the **BCP Manager** will also work with the appropriate resources to develop a written test plan that meets the following criteria:

- All critical applications are tested.
- Test goals are set in advance.
- Realistic conditions and volumes are used.
- Actual backup systems and data files (from offsite storage locations) are used.
- Major/required service providers participate in testing.
- Several user departments participate in testing at the same time to uncover potential conflicts.
- User participation schedules are clearly defined.
- Internal Audit (and/or third-party auditors) participates in the development and review test plans, procedures, and results.
- Post-test analysis, including a comparison of actual to expected results, is clearly documented.
- Corrective action plans for all problems encountered during testing are defined and implemented.
- Subsequent, required changes to the institution's **DP Hotsite** contract/provisions and/or this plan are made in a timely manner.
- Results, including scope, frequency, and a summary of the plan's overall effectiveness, are reported/presented to senior management and the Board in a timely manner.

6.4 | Test Results Reporting

Upon completion of each scheduled test, the **BCP Manager** will report/present results to the Board and work with the appropriate resources to develop a project plan and timeline for problem resolution. Test results reports will include:

- Assessment of whether test objectives were met.
- Validation of test scripts/data processing routines.
- Corrective action plans for all problems encountered during testing.
- Description of gaps between the BCP and test results.
- Proposed modifications to the BCP and/or **DP Hotsite** contract/provisions.
- Recommendations for future tests.

6.5 | BCP Maintenance

Routine plan testing will coincide with the annual review and maintenance of this and all applicable, supporting documentation and data in order to ensure the institution's BCP strategies and provisions remain in compliance with internal and external requirements. Procedures and forms for conducting the annual BCP review are provided on the BCP-CD. At least annually, the **BCP Manager** will execute the BCP maintenance procedure in order to review and update:

- BCP documentation
- Required internal/external resources and recovery team assignments/responsibilities
- Identified potential threats, including probability/impact ratings
- Assumptions on which the BCP is based

- Materials, documentation, data, and IT resource (e.g. workstations, schematics) requirements at the hotsite(s) and final recovery site
- Systems restoration/data processing priority lists
- Supporting policies/procedures, including CAPlus recovery tasks and procedures, as well as applicable emergency notification/response, manual operating, hotsite security, and data backup/storage/rotation procedures
- Adopted testing methodology(ies) and strategies

6.6 | BCP-CD Update

Once annual maintenance is complete and all updated materials have received the required approvals, the **BCP Manager** will:

- File all associated hardcopy documentation accordingly.
- Update the BCP-CD and make the required number of copies.
- Distribute the updated BCP document, BCP-CD, and additional supporting documentation and plan elements to all required internal/external resources and locations (e.g. Team Leaders, hotsite locations).
- Ensure that all outdated copies of the planned are appropriately destroyed or archived.
- Provide any additional training that may be required due to changes in recovery plans, such as new/modified evacuation plans, recovery tasks, manual operating or notification procedures.

7 | Additional Considerations

In accordance with FFIEC regulations, the institution maintains and enforces additional internal policies/procedures, standards, and practices in order to ensure compliance at every level of its organization.

Supporting Documentation & Reports
Internal Policies & Procedures Insurance Coverage Documentation Service Provider Agreements Vendors/External

7.1 | IT Policies & Procedures

The institution maintains and enforces strict adherence to documented policies and procedures governing the acquisition, administration, security, and use of its IT resources, as documented in **EnterDocumentName,** in order to ensure that:

→ One or more of the following elements may be required to support the BCP. If applicable policies, procedures, or practices exist, they should be reviewed to ensure that BCP issues are adequately addressed and revised, as necessary. In such cases, the following statements can be used as-is or modified to detail the applicable policies, practices, and provisions. If an element is non-applicable based upon the size, organization, and/or operations of the institution, replace the provided statement with a brief explanation of why the particular element has been determined to be non-essential/inapplicable.

- Hardware/software acquisitions are justified and compatible with the institution's strategic and business goals and objectives.
- Adequate physical and controls are in place to prevent unauthorized access to internal systems, applications, and critical internal and proprietary information, data, and documentation.
- Internal users understand what constitutes misuse/abuse of their access rights, as well as their responsibilities in protecting assigned workstations/equipment from unauthorized use.
- External users (e.g. vendors, customer/members) understand the institution's policies for acceptable use, as well as the user's vs. the institution's responsibilities in safeguarding private/personal information.
- Critical servers, applications, reports, data, and documentation are backed up, rotated, and tested on a regular basis.
- Systems access and use is regularly monitored by the appropriate resources(s) to ensure internal data, systems, and applications have not been accessed or compromised by unauthorized users.
- Policies and procedures are reviewed and updated as part of annual BCP maintenance to ensure they remain in compliance with internal requirements and state/federal regulations.
- Adequate management approval and oversight is provided for in the development, maintenance, and implementation of the institution's IT policies and procedures.
- Updated policies and procedures are distributed to all required resources and posted/revised in applicable materials (e.g. notices, contracts, websites) in a timely manner.

7.2 | Systems Development & Life Cycle (SDLC)

SDLC is a documented strategy/plan for the acquisition, modification, and implementation of computer systems, software applications, and other IT enhancements in the institution's operating environment, including approvals, pre-testing and problem resolution, and project scheduling and status-tracking. It is the policy of the institution to ensure that BCP requirements are evaluated and addressed during SDLC stages, including:

- Department/system requirements for resumption/recovery
- Backup and storage information
- Security provisions (e.g. password protection, authorized access table, system monitoring)
- Hardware and software requirements at the hotsite(s)
- Inclusion in BCP testing routines
- Staffing and facility requirements

7.3 | Change Control

Change control, or change management, is the practice of ensuring that changes made to critical applications, equipment, resources (e.g. personnel, vendors), and utilities affecting the production environment are carefully examined so that any subsequent changes to existing documentation (e.g. service provider contracts, hotsite requirements, policies and procedures, backup routines) are addressed and implemented in a timely manner. It is the policy of the institution to clearly define and document change control/management strategies and procedures, as detailed in **EnterDocumentName**.

7.4 | Data Synchronization

Data synchronization is the comparison and reconciliation of interdependent data files at the same so that they contain the same information (i.e. at the primary site/at the recovery site). The institution recognizes that management and testing of BCP arrangements and provisions are critical to ensuring that the recovery environment is synchronized with the primary work environment. Therefore, it is the policy of the institution to ensure proper change control, information backup, hotsite planning, and testing procedures are routinely performed in order to prevent data loss and ensure a timely, full recovery.

7.5 | Insurance Coverage

It is the policy of the institution to perform periodic, management review of the provisions and limits of all its insurance policies in order to ensure that adequate coverage for identified, potential emergency situations/events is provided and remains compliant with legal, managerial, and Board requirements. Furthermore, the institution understands the limitations of insurance policies and that, while some reimbursements for financial losses incurred as a result of a disaster may be provided, they are, by no means, a substitute for an effective business continuity plan.

7.6 | Training Programs

The institution recognizes that, in order to be effective, all required resources must be adequately trained in the execution of business continuity and disaster recovery strategies. Therefore, it is the policy of the institution to ensure that key personnel and critical external resources are made fully aware of:

- What their individual/team BCP responsibilities are and how to adequately fulfill them
- What to do if key resources/personnel are not available
- Which conditions call for implementing all/parts of the BCP (Scope)
- To what degree their teams will be involved (depending on the type/severity of the emergency)

7.7 | Communications Planning

It is the policy of the institution to maintain detailed procedures for emergency notification and media/customer/member communications (e.g. recall roster, hotlines, newsletters, e-mails, press releases, Internet bulletin boards) in order to provide employees, external contacts/resources, and customers/members with information regarding the status of the recovery effort throughout the process. Notification tasks/procedures and contact information are provided in applicable reports on the accompanying BCP-CD (e.g. Recovery Tasks, Recall Roster, External Teams).

7.8 | Government & Community Resources

The institution understands that it must coordinate with the surrounding community, government officials, and news media in order to ensure the successful implementation of the BCP. Therefore, it is the policy of the institution to maintain relationships with community resources and agencies that may be required to support the recovery/reconstruction processes. Furthermore, facilities access and cleanup tasks will be coordinated with local police and fire departments and, depending on the nature and severity of the emergency, FEMA or the FBI.

Appendix A | Emergency Response Procedures

This section contains general and event-specific emergency response procedures. Based upon the results of the threat/risk assessment, events that have been determined the most likely to occur and/or to pose the greatest risk to the institution's ability to continue normal operations are addressed.

A.1 | Main Office Evacuation

Employees detecting an emergency that may require evacuation should notify a department manager who will contact the **President & CEO** to obtain a decision on whether or not to evacuate. In the event of the **President & CEO**'s absence/incapacitation, the officers designated in the table in 3.2 | Authorities & Emergency Quorum, in the order listed and dependent upon their availability, will make the decision on whether or not to evacuate. **For immediate and/or life-threatening emergencies, the building will be evacuated immediately prior to notifying a senior officer**.

The need to evacuate a building may not be immediate and, when time permits and there is no immediate risk of physical danger, the following actions can be taken to minimize damage/loss of equipment, files, and data:

- Place critical files/records/documentation into fireproof cabinets or vaults.
- Power down, in proper fashion, any equipment that is in use.
- Unplug and place waterproof covers on equipment before leaving.
- Secure negotiable items and other items of value in vaults, cabinets, and drawers.
- Take PC file backups and portable PCs with you when you vacate the building.

UNLESS IN IMMEDIATE DANGER, personnel will remain at their posts until directed to leave by a Branch/Department Manager. Evacuation of a selected floor/area will be directed by branch/department managers, who will ensure that the following evacuation guidelines are adhered to by employees.

→ Remove highlighted text about elevators if not applicable.

- Ensure orderly evacuation, keeping people calm.
- Bring elevators to the lobby floor and lock them.
- Evacuate quickly through doors, testing them for heat prior to opening them.
- Ensure that handicapped personnel are accounted for and are aided in their evacuation.
- Ensure that restrooms, conference rooms, cafeterias, lounges, etc. are checked and evacuated.
- Ensure that non-employees are escorted out of the building.
- When the floor/area has been completely and successfully evacuated – LEAVE.
- Once outside, go directly to area designated as the evacuation point (**EvacuationPoint**) and await further instructions.
- At the evacuation point, meet in departmental groups, take a head count, and notify authorities if employees are missing.

No personnel, under any circumstances, will attempt to use an elevator when an alarm has sounded as the opening of elevator doors during a fire causes a draft that can turn a minor fire into a serious one.

A.2 | Branch Evacuation

Tellers, under the direction of their branch managers, will place all cash, checks, and pertinent tickets in their cash boxes. If there is time, secure the cash boxes in the vault and proceed to exit from the building. If there is not sufficient time, the teller will lock the cash box in the cash drawer and proceed to exit from the building. The Branch Manager/Head Teller will lock under-counter safes and the main cash vault before exiting the building.

Managers, tellers, or employees that have locked a cash box, vault, cabinet or drawer, should take the keys with him/her when leaving the building. The keys should then be labeled and turned

over to their manager if the locked unit contains cash, checks, negotiable items, or any other items of value, including items of a confidential nature.

UNLESS IN IMMEDIATE DANGER, Branch/Department Managers in areas that have vaults should lock the vaults after placing negotiable items and other items of value in the vault, and then direct the evacuation as described above. Managers in charge of areas that do not have vaults should lock negotiable items and other items of value in available drawers or cabinets, and then direct the evacuation as described above. Ensure that all employees, as well as all non-employees in the building at the time of the emergency, exit the building.

A.3 | Medical Response & General Safety

The first priority in any disaster is to protect human life. In cases where the emergency/event causes power outages, flashlights and other backup power options will be implemented. When there is extensive destruction of the facilities, especially of the type and magnitude as to threaten human life and other assets, management will:

- Above all, ensure the safe evacuation of all persons present in the building.
- At the evacuation point, managers will take a count of employees. If any are determined to be missing, notify the appropriate personnel (e.g. police, fire departments) who have the authority to enter the building and can search for missing employees.
- Tend to injured individuals, supplying basic first aid techniques as space, time, and resources allow. For severe injuries, do not move individuals unless the threat of further harm is perceived.
- Allow building re-entry only after all appropriate clearances are given.
- Check for live power lines, exposed gas/water/sewage pipes, and/or items in danger of falling.
- Monitor the situation via available information sources, including TV and radio reports.
- Coordinate cleanup and restoration efforts with appropriate internal/external resources, including the removal of hazardous materials and activation of decontamination procedures, as required.
- If the building remains unsafe for any period of time, appropriate warnings will be conspicuously posted to keep people from entering the facility.

A.4 | Severe Weather & Natural Disasters

An emergency caused by severe weather conditions could require management to make a decision that could result in early closing, late or limited opening, or closing of the institution. Management will keep abreast of adverse weather conditions and will relay the general instructions to employees, as required.

- Move away from outside walls and windows to the center of the building adjacent to the elevators.
- Stay at the center of the building until the “All Clear” is given, then return to your work areas.
- Report any damages and injuries that have occurred.
- If a major threat to human life is perceived, refer to A.1 | Main Office Evacuation.
- As required, tend to injured individuals, supplying basic first aid techniques to the extent that space, time, and resources allow. For severe injuries, do not move individuals unless the threat of further harm is perceived.

A.5 | Building & Equipment Emergencies

Building and equipment emergencies are any emergencies associated with power, water, and gas systems or services caused by either accidental or intentional/malicious events, such as fire, bombings/explosions, air contamination, or hazardous chemical spills. Employees will adhere to the general guidelines below.

- Call a senior manager to report the emergency.
- If not in immediate danger, shut down PCs using standard procedures.
- If not in immediate danger, disconnect (pull the plug) on electrical equipment to avoid damage caused by a surge of electricity once power is restored.
- If a major threat to human life is perceived, refer to A.1 | Main Office Evacuation.

- As required, tend to injured individuals, supplying basic first aid techniques to the extent that space, time, and resources allow. For severe injuries, do not move individuals unless the threat of further harm is perceived.

A.6 | Environmental Hazards

Should a significant pattern emerge in which employees experience and/or report dizziness, allergies, colds, headaches, skin/eye/respiratory irritation, nausea, fatigue, and other similar symptoms:

- Call a senior manager to report the incident.
- Management will enlist building security/janitorial personnel to attempt to locate the source of the pollutant and, if possible, will take the necessary measures to eliminate the hazard. External resources (e.g. gas company, poison control center) may be required to deal with the situation.
- If the source of the pollutant cannot be located or a major threat to human life is perceived, refer to A.1 | Main Office Evacuation.
- Management will contact and request the immediate presence of local and state health departments, as well as other appropriate external resources, to evaluate indoor air quality, help in the detection/location of the pollution source, and ascertain overall building safety.
- Management will coordinate cleanup and repair efforts with appropriate internal/external resources, including hazardous materials/pollutants removal and activation of decontamination procedures.
- If the building remains unsafe for any period of time, appropriate warnings will be conspicuously posted to keep people from entering the facility.

A.7 | Workplace Disruptions

Should a person or group of people become violent and/or attempt to prevent employees or customers/members from entering the institution or conducting normal business transactions:

- Call a senior manager to report the incident.
- Tend to injured individuals, supplying basic first aid techniques to the extent that space, time, and resources allow. For severe injuries, do not move individuals unless the threat of further harm is perceived.
- If a member of the media approaches you, refer him to senior management.
- DO NOT, under any circumstances, confront the protestors either physically or verbally. Senior management will handle the situation.
- If a major threat to human life is perceived, refer to A.1 | Main Office Evacuation.
- Call the police and other authorities, as required.
- Monitor media coverage of the incident and evaluate the need to activate A.20 | Negative Publicity.
- After the incident, ensure employees are provided emotional counseling, as necessary.

A.8 | Loss of Workforce

Whenever an emergency causes a situation where there is widespread loss of employees and/or critical personnel:

- Re-assign/train existing personnel to ensure adequate dedicated resources are allotted to critical departments/functions WITHOUT over-taxing resources, to the extent possible.
- Encourage cooperation and teamwork, and ensure management tolerance and flexibility.
- Reschedule non-critical projects, as required.
- Evaluate the need for and develop alternate work schedules, including rotating schedules and weekend hours, offering incentives such as overtime pay or comp time, as required.
- Evaluate the need for and hire external help on a temporary or permanent basis, as required.
- Plan for the worst-case scenario, one in which the lost workforce is not expected to return.

A.9 | Workplace Addiction

If you suspect an employee is suffering from addiction or is under the influence of drugs or alcohol on the job:

- Contact a senior manager to report the incident/cause for concern.
- At a minimum, managers will escort the employee into a private area to inquire about the reported behavior WITHOUT revealing the identity of the employee reporting the incident.
- Based upon the employee's reaction/response, the evaluating managers will determine the need to further investigate the employee.
- If the employee is discovered to be under the influence of drugs or alcohol, he/she will be immediately suspended and arrangements will be made to have the employee escorted home.
- Senior management will decide upon the best course of action to further handle the situation.

A.10 | Labor Dispute

Labor disputes are usually predictable and employees often give advanced notice when a strike is planned. When such a situation is expected:

- Senior management will try to reach a compromise to curb the strike before the date at which it is scheduled to take place.
- If compromise is not reached and strike begins as planned, temporary employees from branch offices or employment agencies will be used, as required.
- If violence occurs, refer to A.7 | Workplace Disruptions. Log strikers' activities and videotape actions for any possible, future legal evidence.
- If a major threat to human life is perceived, refer to A.1 | Main Office Evacuation.
- Hold meeting(s) with strikers to continue negotiations until a compromise is reached.
- Monitor media coverage of the incident and evaluate whether or not to activate "Negative Publicity" response procedures.
- After the incident, ensure employees are offered emotional counseling, as deemed necessary.

A.11 | Terrorism

A terrorist threat is an act that is intended to force or intimidate someone into doing something using violence or the threat of violence. The threat may be made against an individual or a group. Terrorist threats often involve bomb threats, threats to burn down buildings, or threats to release harmful biological/chemical agents into the building. If you receive a terrorist threat:

- Write down the threat and/or demand(s) made.
- Call a senior manager to report the incident.
- Follow any instructions you are given.
- Do not discuss the incident with anyone unless instructed to do so by senior management/authorities.
- If a major threat to human life is perceived, refer to A.1 | Main Office Evacuation.
- If the threat is of a biological or chemical nature, refer to A.6 | Environmental Hazards.

A.12 | Systems Intrusion/Abuse

Unauthorized access to computer systems is the gateway to a variety of "cyber-crimes", including cyber-terrorism, computer hacking, sabotage, theft, fraud, data corruption, and virus attacks. When unauthorized access and or abuse/misuse of computer systems is suspected:

- Assess whether the intrusion has originated from an internal or external source. Senior management will coordinate with the appropriate external resources to investigate the crime. DO NOT accuse employees until substantial information is gathered.

- IT and senior management will jointly decide on the best course of action to pursue, which may include one of the incident response procedures described in subsequent sections or a custom strategy based upon the particular situation.
- Consult with legal contacts to determine appropriate legal action.
- Computer and data security will be evaluated and upgraded, as required (e.g. passwords changed).
- An independent contractor/accountant will be hired to evaluate the status of the data in question.
- If data is lost, corrupted, or compromised, determine the extent of damage.
- Obtain backup copies from offsite storage locations and restore data/systems, as required.
- If private customer/member, employee, and/or corporate information have been compromised, a statement should be drafted and sent to all affected parties explaining the situation and detailing the measures taken to prevent similar, future intrusions.

A.13 | Computer Virus Attack

Virus attacks are designed to self-replicate and usually do so without warning. When a virus is suspected/discovered on any network or standalone machines:

- Immediately run virus detection software and delete any files found to contain the virus. (This includes deleting it from the "Recycle Bin" to permanently erase the file.)
- Make sure all passwords are changed after the attack.
- Collect all electronic storage media used on the affected machine to ensure they are not also infected.
- Alert the entire organization of the virus as well as fellow colleagues to whom the virus may have been inadvertently passed.
- Instruct users to run virus scans and script updates immediately upon notification.

A.14 | Power Outage/Blackouts

If the power goes out:

- Determine whether the outage is specific to the institution or the community in general.
- Turn off computers and equipment to avoid surges when power is restored.
- Monitor the situation via available information sources, including radio reports (battery-powered).
- Implement backup power provisions/procedures, if applicable.
- Backup copies from offsite storage locations will be used to restore any lost data.

A.15 | Communications Failure

If voice or data connectivity to external resources and/or service providers is unavailable:

- Determine whether the outage is specific to the institution, the community in general, or if there is a connectivity problem at the service provider's facilities.
- The IT Department will contact the telecommunication(s) provider or service provider (depending on the situation) to assess the amount of downtime anticipated.
- Based on the downtime estimate, senior management will decide whether or not to implement manual/emergency operating procedures.
- Backup copies from offsite storage locations will be used to restore any lost data.

A.16 | Equipment/Software Failure

If any computer/communications equipment appears to be working improperly (e.g. makes an unusual noise, screen flickers) or a software application continually fails to perform its intended function:

- Save work, and close all applications.
- Log off and immediately shut down the computer.
- Do not shake or strike the equipment or attempt to repair it in any way.

- Contact the IT department and report the problem.
- IT will inspect the equipment/software and evaluate cause, type, and extent of damage, working with the required resources to repair/replace the equipment.
- Backup copies from offsite storage locations will be used to restore any lost data.

A.17 | Delivery Malfunction

If a scheduled delivery has not arrived at the anticipated date/time:

- Contact the primary supplier/service provider to assess the situation.
- In the event that the primary service provider temporarily cannot meet demand/perform required services, contact the secondary supplier/service provider.
- Assess any damages/major inconveniences caused by the service disruption.
- Consult with legal contacts to determine appropriate legal action.
- Evaluate the need to change suppliers/service providers.

A.18 | Transportation Disruption

If a major travel/transportation disruption (e.g. traffic, flight delays, road closings) that may prevent normal operations due to employee absences or delay of delivery and/or receipt of packages/mail is expected or encountered:

- Reschedule appointments and travel arrangements in advance, when possible.
- Contact employees and inform them of alternate routes/transportation methods, when possible.
- If scheduled travel plans are disrupted, call and inform the institution of the situation.
- Track the whereabouts of any missing or lost employees.
- In the event of an accident, find out the location and status of injured employee(s).
- Confirm that known travel disruptions have not delayed the delivery of time-sensitive mail/packages. Track the whereabouts of any missing items. Refer to A.17 | Delivery Malfunction.
- Purchase new corporate vehicles, as required.

A.19 | Run on Financial Institution

A financial run on the institution could occur when a large number of members withdraw substantial funds in a short amount of time. This desire to withdraw funds could be based on a number of financial and non-financial-related circumstances. The institution should maintain the ability to control large numbers of members doing business at the institution at the same time. Staff will consider taking the following actions depending on the circumstances:

- Limit the number of members in the building at one time.
- Contact local police for assistance and/or arrange for private security guards.
- Contact armored car company for emergency cash deliveries to branches and ATMs.
- Contact affiliated/correspondent institutions to ensure adequate liquidity for the institution.
- Consider extending lobby hours and encourage members to use ATMs or drive-up terminals.
- Close the branch, as required.

A.20 | Negative Publicity

If the institution feels it has received negative publicity or been misrepresented in any way that could affect its reputation among its customers/members, business community, and/or employees:

- Evaluate the situation and clearly document what has been communicated.
- Construct a detailed and concise message detailing verified facts.
- Immediately schedule a press conference or distribute information through appropriate media/communication channels.
- Follow-up on press conferences and releases.

- Ensure employees, customer/members, shareholders, and the surrounding community is made aware of how the institution is handling the situation.
- Explore other response avenues, as deemed necessary/appropriate, such as letters to the editor or TV/print ad campaigns.
- Monitor media reports of the situation and respond, as deemed appropriate.
- Avoid "no comment" replies. Inform reporters that you are unsure of the answer, do the research, and then get back to them as soon as possible.

A.21 | White Collar Crime

White-collar crime is usually defined as an unlawful act committed by an employee, including theft, embezzlement, fraud, espionage, and sabotage. When white-collar crime is suspected:

- Senior management will coordinate with the appropriate external resources to investigate the crime. DO NOT accuse employees until substantial information is gathered.
- If employee(s) are discovered to have committed or to be planning to commit a white-collar crime, they will be immediately fired.
- Computer and data security will be evaluated and upgraded, as required (e.g. passwords changed).
- An independent contractor/accountant will be hired to evaluate the records in question.
- Inventory records, files, equipment, and materials and report missing items to police.
- Consult with legal contacts to determine appropriate legal action.

A.22 | Unauthorized Facilities Access

If a physical break-in to the facility is detected:

- Do not move any items and alert police immediately.
- Hire the appropriate vendor to change all locks and/or combinations to the facility and secure areas that were broken into.
- Inventory records, files, equipment, and materials, then report missing items to police, providing them with a complete list of internal/external personnel with authorized access to materials for investigation purposes.
- Take statements from witnesses, if possible.
- Evaluate the effectiveness of current security controls and upgrade for increased protection, as required.
- Computer and data security will be evaluated and upgraded, as required (e.g. passwords changed).
- Consult with legal contacts to determine appropriate legal action.

A.23 | Bomb Threat

If you receive a bomb threat:

- Note the exact time of the call/incident. This is important since most bombs are activated by timers.
- Ask the caller the following questions and write down as many details as possible:
  - When is the bomb set to explode?
  - What type of bomb is set to explode?
  - What does it look like?
  - Where is the bomb?
  - What is your name?
- Call a senior manager to report the incident and follow any instructions you are given.
- Do not discuss the incident unless instructed to do so by senior management/authorities.
- If a major threat to human life is perceived, refer to A.1 | Main Office Evacuation.

A.24 | Extortion Threat

Extortion is the act of demanding money by threats. The demands may involve threats against persons and/or property. If you receive an extortion threat:

- Write down what the extortionist said.
- Call a senior manager to report the incident and follow the instructions you are given.
- Do not discuss the incident with anyone unless instructed to do so by senior management/authorities.
- If a major threat to human life is perceived, refer to A.1 | Main Office Evacuation.

A.25 | Pandemic

If the institution feels that a pandemic is beginning to affect the area(s) in which it operates, InstitutionName will assemble a pandemic response team. This team will consist of the Executive Staff, Disaster Recovery Coordinators, Human Resources, Marketing, and Branch/Retail Services. The team will begin monitoring daily reports on the spread of the pandemic. The team will report its findings and recommendations to the Executive Staff (Team) on a daily basis. Sources to monitor include the World Health Organization (WHO), The Center for Disease Control (CDC), and State and Local government health organizations.

As it becomes more apparent that the pandemic has begun to affect the local geographical region:

1. Evaluate the situation and determine whether the situation requires the institution to close its lobby facilities at any or all branches.
2. Evaluate the situation and determine whether the situation allows the institution to open its drive-up facilities at any or all branches.
3. Determine if prophylactic materials, like latex gloves and surgical masks, should be distributed to any or all branches.
4. Determine the minimum staffing level required to continue business operations.
5. Determine available staff and what can be done remotely from a person's home versus what must be done at specific institution locations.
6. Distribute information through appropriate media/communication channels to inform members that banking activity can continue via XXXX and ATMs.
7. Ensure employees, members, shareholders, and the surrounding community is made aware of how the institution is handling the situation.
8. Monitor the situation via available information sources, including TV and radio reports.