BCU-IR03-BUSINESS CONTINUITY PLAN

Table of Contents

EXECUTIVE SUMMARY

Purpose

The Business Continuity Plan consists of the information and procedures required to enable rapid recovery from an occurrence which would disable Baxter Credit Union (BCU), for a period exceeding 24 hours. The purpose of the Business Continuity Program is to ensure that reputation, operational, transactional, strategic, and compliance risks as they relate to a business disruption or disaster are minimized during said disruption. The objectives of the Business Continuity Program are:

- Ensure continuity and survival
- Provide protection of assets
- Mitigate risks and exposures
- Provide preventative measures
- Take control of an interruption.

Successful recovery operations depend on:

- Completing and maintaining an up-to-date Business Continuity Plan and Disaster Recovery Plan.
- Training assigned employees on various aspects of the Business Continuity Plan (business recovery teams).
- Storing and securing adequate backup materials off-site.
- Performing comprehensive tests of the Plan.
- Modifying the Plan as a result of the tests.
- Performing adequate cross-training to reduce reliance on key employees.
- Safeguarding vital records

Assumptions

BCU identifies five levels of disasters:

Level 0	No interruption in operations.
Level 1	Facility and computer equipment damage is observed or access to virtual environment is interrupted, but operations can be resumed within 8 hours.
Level 2	Moderate damage to the facility and/or the computer equipment is observed, or access to the virtual environment is interrupted, but operations can be resumed within 8 to 24 hours.
Level 3	Major facility and/or technical environment disruption, with respect to any BCU department there is interruption in operations for over 24 hours. All functions and employees should be moved to a designated alternate site.
Level 4	Major facility and/or technical environment disruption, with respect to any BCU department. Major salvage operations are imminent and interruption in operation is estimated over 24 hours. All functions and employees should be moved to a designated alternate site.

The Plan assumes:

1. That any facility or department of BCU has been destroyed, Level 4 disaster.
2. Staff is available to perform critical functions defined within the Plan.
3. The disaster will occur at the worst possible time.
4. Selected staff can be notified and can report to the backup site(s) to perform critical processing, recovery, and reconstruction activities.
5. Off-site storage facilities and materials survive.
6. The Business Continuity Plan is current.
7. An adequate number of supplies is stored off-site, either at an alternate facility or off-site storage.
8. BCU's backups are current, correct, and accessible. It is BCU's responsibility to ensure that backup locations, data, and procedures are thoroughly checked and tested.
9. That BCU Recovery sites are unaffected by the incident and prepared to receive the data sent to them.

OVERVIEW

Objective

The objective of the Plan is to provide the information and procedures necessary to:

- Respond to a business continuity event or disaster occurrence.
- Notify necessary employees
- Assemble business recovery teams
- Recover data
- Resume processing to ensure minimal disruption to BCU and operations conducted by departments within the BCU
- Provide customers with continued service until 'normal' operations can be resumed
- Restore normal processing at production facilities

The recovery plan is composed of document resources and procedures to be used in the event of a disaster affecting BCU's services. Each supported computing platform has a section containing specific recovery procedures. In addition to the recovery scripts, each playbook will have a data sheet that contains environment specific data needed for recovery. This plan is available through the BCU's SharePoint site, as well as vendor hosted off network location, to make it more generally available to BCU staff. This plan will be reviewed annually and updated on a regular basis as changes to the data center are made.

Scope

The Business Continuity Plan encompasses all of BCU's Departments, facilities, network, and assets. Various sections of the completed Plan or the entire Plan may be used for other locations, as applicable.

The Plan addresses the following issues and concerns:

- BCU, Main Office and Satellite Office(s) disaster
- Departmental disaster(s)
- Restoration plans for the various business units and functions.
- Restoration and recovery from a cybersecurity event as outlined by BCU's Incident Response Plan.

Structure of the Plan

The Business Continuity Plan is structured in an outline format with sections for activation, team functions, critical telephone numbers for employees, facilities, and critical recovery assets. (Reference the Table of Contents for section titles). The sections are in a logical order and follow the Business Continuity Planning process.

The team approach is used in the Business Continuity Plan. The Plan is structured so that each team is a separate section. The teams (and related sections) are the Command Team, the Business Continuity Team, the Event Team, the Recovery Team, and the Disaster Recovery Team(s). Each section details the procedures and specific responsibilities for each respective team. Each section is also formatted to be used on a stand-alone basis if only one area of BCU is destroyed or temporarily unable to operate. Other sections of the Plan include exhibits, critical telephone numbers, and disaster assessment forms.

Roles and responsibilities

During the time of a business disruption, the traditional organization hierarchy may need to change to accommodate the constant changing information as well as to manage many moving parts. This section defines the multiple teams put in place, their roles, and participants.

Supervisory Committee & Board of Directors

The Board of Directors are responsible and accountable for the following:

- Assigning business continuity responsibilities and accountability.
- Allocating resources to business continuity.
- Aligning business continuity management with business strategy and risk appetite.
- Understanding business continuity risks and adopting appropriate policies and plans to manage events.
- Understanding business continuity operating results and performance.
- Providing a credible challenge to management responsible for the business continuity process.
- Establishing a provision for management intervention if timeliness for corrective action is not met.
- Oversight of continuity risk assessment.
- Oversight of resilience planning.
- Oversight of Business Continuity Plan testing.
- Oversight of remediation of lessons learned from the testing and event.

Chief Information Security Officer: The Chief Information Security Officer (CISO) is the Plan

Administrator, and as such is responsible for declaring a disaster, as well as owner of this standard and is responsible for its initial draft, publication, dissemination, and revisions. The CISO also participates in roles throughout the different teams, as needed.

Business Resiliency Director: The Business Resiliency Director is responsible for:

- The Assistant Plan Administrator and support the Plan Administrator and Command Team as needed.
- Management of the BIA process through the conducting of meetings with relevant stakeholders to complete the BIA and update the Business Continuity Plan accordingly.
- Designing and implementing a business continuity exercise strategy.
- Aligning plans between business units across the credit union.
- Coordinating plans and responses with external entities.
- Designing and implementing a business continuity testing strategy.
- Engaging internal or third-party audit to validate the design effectiveness of the business continuity. program and whether controls are operating effectively.
- Validating the qualifications and independence of auditors leveraged to review the business continuity management program.

Business Continuity Planning Committee: The Business Continuity Planning Committee is responsible for:

- Establishing measurable goals against which business continuity performance is assessed Confirming that tests, training, and exercises are comprehensive and consistent with the exercise strategy.
- Resolving weaknesses identified in tests, training, and exercises.
- Meeting regularly to discuss policy changes, training, and testing plans.
- Assessing and updating business continuity strategies, risk analysis and plans to reflect the current business conditions and operating environment for continuous improvement.
- Reporting the results of audits of the business continuity management program to the Board of Directors.
- Meeting at least quarterly and in break-out sessions as necessary to keep the plan up to date and relevant.
- Maintaining formal meeting minutes.

Event Management Team: The Event Management Team is a cross-functional team that monitors internal and external until issues until resolved, deemed not an issue, or transferred to a risk management team for further management.

Disaster Recovery Team: This team comprised of IT and security professionals is responsible for the design, implementation and testing of recovery and restoration procedures derived from the mutually agreed upon restoration and recovery objectives so that BCU can perform critical business functions during a disruption.

Command Center Team: The Command Center's primary responsibility is to re-establish control of BCU's environment by identifying the necessary functions to regain command of the situation and delegate those tasks and authority to available employees. Refer to the "Command Team" section for details.

Senior Management

Senior Management is responsible and accountable for the following:

- Defining business continuity roles, responsibilities, and succession plans.
- Allocating knowledgeable employees and sufficient financial resources.
- Validating those employees understand their business continuity roles.

General Council and VP of Compliance

General Council and the VP of Compliance are responsible and accountable for:

- Consultation and administration of legal and compliance concerns of business continuity management.
- Liaison between Beazley and BCU for any legal matters.

Business Function Owners: Business Function Owners (BFO) are key stakeholders who are designated as owners of critical business functions attend BIA meetings and identify other Subject Matter Experts (SME) in their organization who can provide the needed technical and operational details to complete the BIA.

Technology Custodian: A Technology Custodian is an individual in the IT organization who is responsible for the operation of a system or technology resource on which a critical business function depends.

Subject Matter Experts (SME): SMEs attend BIA Meetings and provide relevant details used to evaluate the critical business function. SMEs may be from the business unit where the business function is performed or from relevant business units in the information technology organization.

Distribution of the Plan

The Plan is distributed in full to Command Team members and their alternates. Partial editions of this manual may be distributed to the sub-team members, and Departments to assure availability of this plan to any employee or organizational element that may become involved in its implementation, one current and complete copy should be filed and maintained in each of the following locations:

1. CISO / Plan Administrator's home – printed copy
2. Business Resiliency Director's home / Assistant Business Continuity Plan Admin – printed copy
3. Secured location in BCU's Security Department
4. BCU's disaster recovery data center – printed copy
5. BCU's vendor hosted SharePoint: Policy Page – electronic copy
6. BCU's vendor hosted governance platform – electronic copy

Upon approval of any of a change to the Plan or its associated resource, an updated hard copy will be generated and distributed to the off-site locations.

Maintenance of the Plan

Update Procedures

Changes and modifications to the Plan are expected and may be organized in the following manner:

- Update the Business Continuity Plan periodically, at least on an annual basis.
- Submit all Plan changes at least annually to the Business Resiliency Director who will submit to the CISO for review and then to Supervisory Committee to for approval.
- Enter information regarding changes in equipment, furniture, employees, hardware, software, forms, etc., as changes occur.
- Write information regarding changes to specific procedures on the pages of the Plan which contain the procedures as changes occur.
- Distribute updates to individuals' assigned copies of the Plan.
- Update the Business Continuity Plan Distribution Register form to provide accountability for Plan copies (Exhibit I-12).

Control Procedures

NOTE: This plan is confidential and the property of BCU. It should not be allowed outside the Company or used as an example for any other corporation's Business Continuity Plan without the express written permission of the BCU Management.

To properly control the Plan, the Business Continuity Plan Administrator or Coordinator should perform the following activities:

- Determine the number of copies of the Plan that are necessary.
- Distribute completed copies of the Plan to the appropriate Team Members.
- Distribute updates of the Plan at least annually.
- Issue updates by complete section.
- Insert the new updates by section and page number.

Testing the Plan

Realistic testing of the Business Continuity Plan on an annual basis is critical. Reasons for testing the Plan include:

- Determining the feasibility of the business recovery process
- Verifying the compatibility of alternate sites.
- Identifying deficiencies in the existing procedures.

- Identifying areas in the Plan that need modification or enhancement.
- Providing training to the Team Managers and Team Members.
- Ensuring the adequacy of procedures relating to the various teams involved in the recovery process.
- Demonstrating the ability of BCU to recover.
- Providing a mechanism for maintaining and updating the Business Continuity plan.

Alternate Facility Sites

Management should identify alternate facility sites to be used in the event of a disaster. The purpose of an alternate site is to serve as a temporary location for all or part of BCU's departments. Alternate sites may include remote offices, available commercial facilities, or mobile facilities. Specifications to consider when choosing alternate sites include:

- Alternate sites are at a sufficient distance from the main facility to reduce the likelihood of destruction under the same disaster circumstances.
- Alternate sites are equipped to handle increased communication transactions, both incoming and outgoing, if the main office location is destroyed.
- If the main office is not destroyed and alternate location is needed for branch employees, determine what additional capacity is available at the corporate headquarter buildings.
- Alternate sites have adequate space to provide room for additional administrative and customer service employees.
- Alternate site locations are clearly communicated to all team members and responsible persons.

During an emergency resulting in the authorized place of business of this operation center not being able to function, the business ordinarily conducted at such location will be relocated elsewhere. The location of alternate facilities may be selected based upon available sites and needs as determined by the Command Team. Staff may be asked to work from home or other remote locations. In the event a Company Partner or Service Center is closed, notifications are placed on the entrance and social media sites notifying members of the closure.

The Command Team has available to them a Command Post from which Business Continuity Plans can be assessed and implemented. BCU has a partnership with Agility, who will offer mobile sites, computers, and internet in the US, in the event of a disaster. If BCU office(s) are not suitable for occupancy an alternative site will be chosen based on anticipated length of time the site will be needed, availability of communications (telephone service, internet), size and physical condition.

The alternative site could be, but is not limited to, the following locations:

- Agility Mobile Facility delivered to a location determined at the time of business disruption.
- Alternative facilities could also be arranged through the use of local Realtors listed in Appendix

C. These sources will be familiar with what property is available at any given time.

The Command Team will identify alternate facility sites to be used in the event of a disaster. The purpose of an alternate site is to serve as a temporary location for all or part of BCU's departments. Alternate sites may include remote offices, available commercial facilities, or mobile facilities. Specifications to consider when choosing alternate sites include:

1. Alternate sites are at a sufficient distance from the main facility to reduce the likelihood of destruction under the same disaster circumstances.
2. Alternate sites are equipped to handle increased communication transactions, both incoming and outgoing, if the main office location is destroyed.
3. Alternate sites have adequate space to provide room for additional administrative and customer service employees.
4. Alternate site locations are clearly communicated to all team members and responsible persons. Directions to the alternate site(s) are included in the Plan and distributed to all team members and responsible persons.

Activation of the Plan

Protocol states that the Business Continuity Plan Administrator is the individual declaring the activation of the Business Continuity Plan. In the event the Business Continuity Plan Administrator is unavailable, The Business Continuity Plan Coordinators have been granted the authority initiate notification and activation. See the Command Team Specific Responsibilities section for additional information.

PLAN STRUCTURE

For purposes of clarity and simplicity this plan will be divided into three major sections and supporting appendices. The three sections are:

1. Pre-disaster Planning and Prevention
2. Emergency Situations
3. Business Recovery

In this respect the plan will follow a logical sequence of stages:

STAGE NAME	ACTION
1. Preparation	Anticipate and prepare for the emergency. Identify exit routes and evacuation procedures.
2. Detection	Notify responsible authorities
3. Reaction	Initiate safety procedures for evacuation and rescue. Notify security and emergency agencies.
4. Assessment	Determine damage, and potential further damage, and its effect on operation.

5. Authorization	Obtain proper approval to initiate Business Continuity Plan and procedure.
6. Notification	Alert involved employees, Senior Management, and teams.
7. Mobilization	Retrieve resources and prepare for backup command post.
8. Emergency Operation/ Restoration	Set up command post at backup facility.
9. Reconstruction	Begin rebuilding efforts, salvage, insurance claims, etc.

Pre-Disaster Planning and Preparation

This plan will be reviewed and approved annually by the Chief Information Security Officer and BCP Committee of BCU with changes presented to the Supervisory Committee. The plan will be revised annually or whenever significant changes are made to staff or physical facilities.

This phase of the plan addresses actions and precautions which should be performed prior to an actual emergency or disaster. Actions and precautions are made in an attempt to reduce the severity of the emergency and/or facilitate recovery from a disaster.

These include, but are not limited to, the following:

1. Development and assigning responsibilities for the plan.
2. Identification and construction of business recovery teams
3. Placement of early detection devices
4. Placement of emergency equipment and supplies
5. Evacuation procedures for employees
6. Safeguarding special equipment and information

It will be the responsibility of the Business Resiliency Director to coordinate any changes to the plan and distribute the changes to all plan holders. During and after a disaster/emergency situation, BCU will utilize various teams to assist in the activation and implementation of the plan. These teams will be known as:

1. Command Team
2. Administrative Recovery Team
3. Communication Recovery Team
4. Facility Recovery Team
5. Technical Recovery Team
6. Application & Operational Recovery Team
7. Data Recovery Team
8. Security Recovery Team

The names and phone numbers of critical recovery team members are maintained by the human resources department. In addition, Sections of this plan contain a basic description of the responsibilities and duties of each team during an emergency or during the recovery process. Each team member has received a copy of their team lists and knows the basic responsibilities of their team.

Alternate Facilities/Command Post

During an emergency resulting in the authorized place of business of this operation center not being able to function, the business ordinarily conducted at such location will be relocated elsewhere. The location of alternate facilities will be selected based upon available sites and needs as determined by the Management Team. Any temporary relocation of place of business for the center will be discontinued when permanent quarters are restored. The Management Team will use a Command Post from which Business Continuity Plans will be assessed and implemented.

The primary alternate sites for each location are:

Site	Address	Alternate Site
Production Data Center	340 N. Milwaukee Ave. Vernon Hills, IL 60061	TierPoint 3701 W Burnham St., Suite A Milwaukee, WI 53125 877.859.8437
Headquarters	340 N. Milwaukee Ave. Vernon Hills, IL 60061	Incident Response and Business Critical Location Crystal Lake Service Center 415 S. Main St. Crystal Lake, IL 60014
Headquarters	340 N. Milwaukee Ave. Vernon Hills, IL 60061	**Agility Mobile Site** 1-855-447-3750 OPTION 2 PreparisSupport@agilityrecovery.com **Account Executive: Michael McNeill**

If BCU (Headquarters) office is not suitable for occupancy an alternative site will be chosen based on anticipated length of time the site will be needed, availability of communications (telephone service), size and physical condition.

Generators

The Vernon Hills location has a 750K diesel generator with a 2000-gallon tank. Some branch locations have generators or other back-up power sources. Branch locations are owned or leased by our Company Partners.

Vernon Hills is cycled tested once a month. The fuel requirement is diesel fuel, with an annual maintenance being performed every November. They are capable of running on the fuel for 10 days. It gets filled on an average of about every 3 years. The fuel/maintenance is checked monthly via the maintenance agreement which is owned by the Facilities Department.

Emergency Preparation

Members of the Facility Team will be responsible for providing evacuation information. If an emergency exists during office hours, these individuals will be responsible for ensuring that all individuals have been evacuated. The primary objective during an emergency is the protection and preservation of human life. Everything else is secondary. Evacuation procedures are listed in Appendix B of this plan. If time permits, the members of the Administrative Support Team will secure any assets and information, but again, only if there is no immediate threat to human life.

Any individuals evacuated from the building fall under the authority of local municipal units. They will not be allowed to reenter the building until all clear is sounded. In the event of a prolonged disaster, they should plan to report to the backup facility the following day or when all clear is sounded.

The primary objective during an emergency is the protection and preservation of human life. Everything else is secondary.

Pandemic Preparedness and Response Plan

BCU recognizes the unique challenges a pandemic may present and as such has prepared a separate Pandemic Preparedness Plan which is attached as Appendix N.

Immediate Communication

The BCU CEO and or the SVP of Marketing will be the primary spokesperson for the corporation regarding press releases or communiqués during the emergency or disaster. If necessary, after an emergency, this individual is responsible for ensuring a press release to the public regarding the extent of the disaster, its effect on our operations or any other pertinent information or instructions. Sample news media releases are contained the Communication Recovery Team's Responsibilities section of this document and are to be used to expedite this process during possible perplex situations. No other persons are to discuss anything relating to the emergency unless directed by the Chairman of the Board, CEO, or his successor, as designated in the Emergency Preparedness Program.

Appendix C of this plan contains a list of key emergency phone numbers and names, as well as the names and numbers of primary equipment, supply, and support vendors. The entire list of employee contact information can

be found in the Preparis emergency communication portal. Anticipate call lists have been prepopulated or can be created on demand. Employee contact information is also available in the human resources SaaS based system.

Information and Assets

As a preparatory step these actions will be put into place immediately:

- Emergency supplies will be obtained from other offices (if applicable) or purchased from local merchants and equipment from present vendors until reordered supplies and equipment are received.
- Core data processing is replicated to the Data Recovery Center Location in Milwaukee, WI. The Disaster Recovery (DR) Plan IT Services is attached. The DR Plan will be updated continuously and reviewed and tested at least annually.
- Back-ups:

  For a full description of back-ups, please reference the Disaster Recovery Plan. The following contains a summary of back-up processes for the most critical systems.
  - NetApp: Vernon Hills replicates to Milwaukee. For systems using the NetApp unique to Milwaukee, those files are replicated to the Vernon Hills NetApp. There are varying snapshot schedules as well depending on the importance of the data stored (hourly, daily, weekly, and monthly)
  - Commvault: Commvault stores the back-ups to one of three storage servers in three different Azure regions.
  - Microsoft Azure Back-Ups Server: BCU deploys MABS to back up our on-premises server resources, and specifically Hyper-V. MABS provides back-up archive solution to BCU's cloud storage in Azure. Once the back-ups are in the cloud, they can be restored to either of our production or DR data centers.
  - Azure Back Ups: Azure Backups will be used to back-up and restore virtual servers in the cloud environment from a point in time and to recover from a DR event. The backups will occur and be stored in Azure region where the resources are located based on an Azure policy. The backups will be stored in an Azure recovery services vault which the storage will have geo redundant replication enabled to other Azure regions.
  - Azure Replication: Works the same way as Azure back-up, only for replication.
  - SQL: For all production SQL we perform full back up once a week, differential backup every night and transaction log backup ranging from 15 minutes to 1 hour. We also use SQL Always on technology in conjunction with Windows Failover Cluster for DR purposes for key applications.

Business Recovery

Immediately after an all clear has been communicated the Command Team will meet at the designated Command and Control Center. The first task will be to assess the damage and its effect on operations of BCU. Damage assessment forms are shown in Appendix I. The Command Team will also begin to implement this plan and to determine direction for the recovery teams and the Business Continuity
Plan Coordinators. Based on the extent of the disaster, decisions will be made by the Operational Recovery Team to direct the recovery activities.

Command Team General Responsibilities

The Command Team is responsible for performing the following activities:

Complete and maintain the Business Continuity Plan.

- Coordinate the business recovery process.
- Assess the level of disaster (0-4).
- Contact the Team Managers.
- Monitor the business recovery process.
- Make final decisions.

The positions on the Command Team are the Business Continuity Plan Administrator and the Business Continuity Plan Coordinators. Each position has specific responsibilities which are detailed below. In the event the designated Administrator or Coordinator is unavailable, the alternate will assume the specific responsibilities of that position. Other members of the senior management team are also available to support the Command Team. The procedures included in this plan are to assist the departments of the BCU in a guide of how to continue processing in the event of a disaster. The procedures detail high priority tasks, temporary operating procedures, equipment, forms, and supplies, and reconstruction procedures.

Business Continuity Plan Administrator

The Business Continuity Plan Administrator has ultimate responsibility for the business recovery process and related decisions. The Business Continuity Plan Administrator receives first notification of a disaster and activates the business recovery process.

Business Continuity Plan Administrator responsibilities:

- Receive initial disaster notification.
- Select and establish the Command-and-Control Center.
- Determine the extent/level of the disaster.
- Declare a disaster and activate the Business Continuity Plan.
- Establish communications facilities.
- Notify business recovery team Managers.
- Document and monitor business recovery activities.
- Provide managerial direction to all Team managers.
- Prepare the Disaster Assessment Report (refer to Exhibit I-3, Appendix I).

Assistant Business Continuity Plan Administrator

The Assistant Business Continuity Plan Coordinator acts as the assistant to the Business Continuity Plan

Coordinator. The Assistant Coordinator is the Business Resiliency Director, is responsible for assuring procedural compliance with the Plan.

Business Continuity Plan Coordinators

The Business Continuity Plan Coordinators act as the assistants to the Business Continuity Plan Administrator. The coordinators are members of the Management Team which have overall responsibility for activating the Plan and assuring procedural compliance with the Plan for their respective departments. The seven coordinators are composed of:

1. Administrative Business Continuity Plan Coordinator
2. Communication Business Continuity Plan Coordinator
3. Facilities Business Continuity Plan Coordinator
4. Technical Business Continuity Plan Coordinator
5. Operations Business Continuity Plan Coordinator
6. Data Business Continuity Plan Coordinator
7. Security Business Continuity Plan Coordinator

Business Continuity Plan Coordinator responsibilities:

- Assist in determining the extent/level of the disaster, if not previously identified
- Assist in activating the Business Continuity Plan.
- Notify members of senior management.
- Activate notification procedures.
- Activate alternate site notification as needed.
- Supervise and control business recovery activities.
- Inform Departmental Recovery Teams as appropriate.
- Assist in preparing the Disaster Assessment Report (refer to Exhibit 3).
- Collect and evaluate any records recovered from the disaster.

Command Team Specific Responsibilities

The Command Team, along with Senior Management, has specific responsibilities which must be completed to ensure successful Plan execution.

Initial Disaster Alert

Initial notification can come from:

- Police or fire departments
- Employees
- Customers
- Passer By
- Other

Disaster Verification and Assessment

Upon notification of a disaster, the Business Continuity Plan Administrator or Coordinator should attempt to determine the extent of damage. The Command Team will review the disaster's impact on various departments and the feasibility of performing normal business operations in the main facility.

Within four hours of declaring a disaster or within eight hours of an undeclared disaster-related event, the Administrator or Coordinator should prepare a Disaster Assessment Report (Exhibit I-3, Appendix I) including but not limited to:

1. Date/time reported.
2. Name of person placing initial alert
3. Estimated time of arrival at disaster site
4. General description of the disaster
5. External support requirements
6. Damage level assigned to, extent of damage to, and estimated recovery time for:
    a. Employees
    b. Property
    c. Structure
    d. Utilities/Services
    e. Hardware
    f. Software

Preparation of the Disaster Assessment Report will help determine:

- The need for relocation by department.
- The need for an alternate site.
- The need to notify the public of alternate site operations.
- The need to reconstruct data and records.
- The need to notify other business recovery teams to implement their procedures.

Business Continuity Plan Activation

Protocol states that the Business Continuity Plan Administrator is the individual declaring the activation of the Business Continuity Plan. In the event the Business Continuity Plan Administrator is unavailable, The Business Continuity Plan Coordinators, or any member of the Command Team has been granted the authority initiate notification and activation. Upon receiving disaster notification and approval from the Business Continuity Plan Administrator, the Business Continuity Plan Coordinators will contact other members of the Management Team.

The Command Team will meet at the Command-and-Control Center previously agreed upon. To activate the plan, the Administrator or Coordinator will:

- Notify Management of the following:
    - A disaster has occurred and indicate the extent of the disaster.
    - A location and telephone number for the Command-and-Control Center.
    - A meeting date for corporate members to discuss future activities of BCU Business Units.
- Notify Business Resiliency Vendors
    - Notify Agility if alternate networking and/or office space is needed.
    - Notify CUNA Mutual to notify them of declaration of a disaster for insurance purposes.
- Notify other Team Managers as required.
    - Notify Crystal Lake Service Center, Data Center Recovery Location or Agility.
    - Notify alternate site(s) if necessary.
    - Assign employees to the alternative facilities.
- Notify all remaining Senior Management Team Members using the Senior Management Team List (Appendix A). On a ***need-to-know basis***, information to be supplied may include:
    - General description of the disaster
    - Level of disaster
    - Extent of hardware/software damage
    - Extent of damage to property required for operations.
    - The location of the Command-and-Control Center
    - The immediate action required.
    - External support requirements
    - Estimated recovery time

Depending on the magnitude of the facility disaster, the Business Continuity Coordinator's should contact the following:

- Associated Entities
- Couriers

- Other Service Provider
- Direct others with contractual relationships which could be impaired due to the disaster. (See Exhibit C-1 - Critical Contact List and Exhibit C-2 - Vendor List for telephone numbers.)

In the event the BCU headquarters facility is not habitable, transportation to the alternate site(s) may be provided by individuals using their personal automobiles or private transportation systems. For long-term situations, leased vehicles can be used. The Administration Facilities Team will coordinate transportation requirements to ensure that all necessary individuals can travel to the alternate site(s). It may be necessary to arrange with a moving company or vendor for the relocation of large or sensitive equipment.

Recovery Action Planning Activities

The following recovery-related activities will be performed by the Command Management Team:

1. Establish the new operating environment:
    a. Location (main facility status and alternate site availability).
    b. Physical modification required to allow daily activities in new operating environment.
2. Schedule for dispatching various teams.
3. Notification checklists implemented.
4. If necessary, initiate rebuilding process at the affected Business Unit or facility.
5. Expand telephone system capacity at remote office locations at the time of disaster, if necessary.
6. When damage is assessed, assign employees to note vital records recovered at the disaster site.
7. Initiate record salvage procedures, if appropriate.

When deciding the recovery plan, the team shall use the agreed upon recovery objectives and identified and mutually agreed upon as part of the BIA process. See Appendix M for the recovery tiers.

Monitoring Recovery Operations

To monitor recovery operations, the following activities should be performed.

- Receive status reports from each remote office location.
- Receive reports from each Team Manager daily.
- Receive and review the Recovery Status Report from the business recovery team.
- Monitor weather and environmental status.
- Monitor employee activities - hours, stress levels, etc.
- Monitor critical supply deliveries and follow-up.
- Monitor courier deliveries and pick-ups.
- Ensure adequate funds, resources, etc., are available for necessary purchases and expenditures.

- Request additional support as needed.

Establishing the Command-and-Control Center

The Command Team may require a facility from which they can communicate and direct the efforts of the various teams. This facility is called the Command-and-Control Center.

The location of the Command-and-Control Center can be any existing property owned or leased by BCU or any leased location capable of housing 15-20 Command Team members. The Command-and-Control center should be as close to the disaster site as safely possible. Following is a listing of properties that could be utilized as possible Command Center sites.

- BCU, Crystal Lake Service Center
- Agility Mobile Site
- Local hotel or conference center

Following are the procedures to be performed at the Command-and-Control Center:

- Open the facility.
- Contact the Team Managers of the business recovery teams and ask them to meet at the Command-and-Control Center.
- Network Sub Team - Establish communications with the Crystal Lake Service Center and the telephone company.
- Document all activities as they occur.
- Utilize the Business Continuity Planning forms and reports (see Exhibits and Reports Section, Appendix I):

Equipment and Supplies

A ready-to-go stock of equipment will be stored at a location near the Crystal Lake Service Center. The following basic equipment and supplies are needed to enable the Command-and-Control Center:

- BCP Plan
- Telephones
- WIFI/Router/VPN appliance
- Printer

Administrative Recovery Team Responsibilities

The Administrative Recovery Team will be led by the Administrative Business Continuity Plan Coordinator and is the team primarily responsible for the safety of human life and human resource related processes.

Following the activation of the Business Continuity Plan, the Business Continuity Plan Coordinator will notify and instruct the Administrative Recovery Team Manager to report to the Command-and-Control Center.

The Administrative Recovery Team manager will ensure that all Team Members are notified and, on a need,***-to-know basis***, information to be supplied may include:

- General description of the disaster
- Level of disaster
- Location of the Command-and-Control Center, if appropriate
- The immediate action required
- Plan for recovery
- External support requirements
- Estimated recovery time

Responsibility	Description
Employee Status	Employee status will be determined by the Business Continuity Plan Coordinators for their Teams. The alternate Administrative Business Continuity Plan Coordinator is responsible if the assigned coordinator is not available. Once status is determined, the following procedures should be used as appropriate: • Contact emergency help and/or notify the Business Continuity Plan Coordinator if individuals are injured. • The Chief Executive Officer will notify closest family members, using the Emergency Contact Number listed on the employee files, (if necessary). • Determine adequacy of staffing for the Team. Report Team status to the Administrative Business Continuity Plan Coordinator.
Temporary Employee Selection	Additional staff may be necessary for continued operations. Staff can be transferred from other locations, or temporary agencies may be used

Employee Payroll Procedures	Payroll is outsourced and time entry may be possible via the Workday.com or Kronos websites, or timecards may be used to continue processing. Since completely accurate time-keeping methods may not be feasible, the following temporary procedures may be used: • A surviving employee designated to process payroll would contact Kronos. • Kronos customer support phone number: 1-844-3358223. • Give them our Company Code Service Center ID. • Designated employee would explain the situation to the Kronos representative. • Kronos representative would ask a series of questions to identify the person calling • Once the employee has been identified, Kronos would walk them through accessing payroll as an administrator to submit payroll. • The employee can use any computer from any location to submit payroll information once they are setup as an administrator. • Kronos would either submit the previous payroll or set up the system to pay employees a designated number of hours. Differences can be reconciled at a later date. Payroll checks are issued by Kronos with direct deposit to the staff bank accounts or if necessary, by paper check via common carrier or courier service.

Communication Recovery Team Responsibilities

The Communication Business Continuity Plan Coordinator, or delegate, are responsible for setting direction and deliver of disaster related messages to internal employees, members, BCU's Company Partners, vendors, and general public. Notification requirements will be determined by the disaster recovery category. Contact lists will be within the plan.

Specific Responsibilities

Information to be provided should include recovery time, access points available if any, actions being taken as part of the recovery, member data information with the purpose of alleviating concern, impact on human factor (depending upon severity of the disaster and as determined by the executive team).

Employee Communication

Designated team leaders will contact assigned employees. Team leaders and employee lists are found in each department's business continuity plan.

Sample communication:

BCU has recently suffered a (specify disaster type). As of (insert date)) BCU is operating with limited resources. You will be contacted by (team leader name) with updates, additional information specific to your work area, and notification of full recovery. We expect to be fully recovered by (insert date, including time if available). As always, the safety of BCU Employees is paramount. Should you need to reach someone at BCU, (team leader name) is your point of contact during recovery time. Thank you for your patience.

Provide Name, Title and contact information

Member Communication

Members will be communicated via the following vehicles depending on availability and according to the disaster category.

- Website
- Hold message on The Hub's primary phone call queue.
- Press Release and/or phone call to local media
- Post to social media sites
- Email to member database (accessible in the Cloud) – when applicable for Category III or higher disasters or deemed appropriate by the Command Center.

Communication messages are as follows:

Website

Sample communication:

BCU has recently suffered a (specify disaster type). As of (insert date and time,) BCU is operating with limited resources. Please check back to this website for information as it becomes available. BCU will post updates, pertinent details, and notification of full recovery as frequently as possible. We expect a full recovery by (insert date including time if available). As always, the security of Members' funds and information is paramount to us. Thank you for your patience.

Provide Name, Title and contact information

Recording on main member relations line

Sample communication:

BCU has recently suffered a (specify disaster type). As of (insert date and time), BCU is operating with limited resources. We will post updates, pertinent details, and notification of full recovery on our website, www.bcu.org as

frequently as possible. We expect a full recovery by (insert date including time if available). As always, the security of Members' funds and information is paramount to us.
Thank you for your patience.

Provide Name, Title and contact information

Press Release and/or phone call to local media

Sample communication:

BCU has recently suffered a (specify disaster type). As of (insert date and time), BCU is operating with limited resources. Updates, pertinent details, and notification of full recovery will be posted on our website, www.bcu.org as frequently as possible. The credit union expects a full recovery by (insert date including time if available). As always, the security of Members' funds, information and Staff are paramount. BCU thanks its Members, Employees and Business Partners for their patience.

Provide Name, Title and contact information

Social Media Posts

Sample communication:

BCU has recently suffered a (specify disaster type). As of (insert date and time), we are operating with limited resources. Updates, pertinent details, and notification of full recovery will be posted to BCU.org as frequently as possible. We expect a full recovery by (insert date including time if available). As always, the security of Members' funds, information and Staff are paramount. Thank you for your patience.

Provide Name, Title and contact information

Business Partner Notification

Designated team members will contact assigned business partners per the contact list. Business partner notification information will depend on the business partner's function. Business Partner lists and functions will be specified by disaster category.

Sample Notification:

Baxter Credit Union (BCU) has recently suffered a (specify disaster type). As of (specify date,) BCU is operating with limited resources. We expect to be fully recovered and operational by (specify date and time if available). You will be contacted by (specify name) for updates and notification of full recovery. (Repeat name) will also be your point of contact during recovery time. Thank you for your patience.

Provide Name, Title and contact information

Board Notification

Designated member(s) of the senior management team will contact all board member(s). Board members will receive a full report about the incident including assessment of the severity of the disaster, strategies concerning recovery, recovery time, human impact, impact on members and their data and media relations communication strategies.

Sample Notification:

Phone, Fax and/or email (depending on availability) –

Baxter Credit Union (BCU) has recently suffered a (specify disaster type). As of (specify date) BCU is operating with limited resources. We expect to be fully recovered and operational by (specify date including time if available). Below is a full report of the impact based on our current assessment:

- *Human Impact – Specify casualties if any.*
- *Status of Current Business Operations & Recovery Time – provide date(s) BCU expects to be fully or partially operational.*
- *Member Communication – Provide communication provided to members and communication vehicles (i.e., website, phone recording, media).*
- *Media Relations – Provide outline and/or press release being sent to the media as well as a detailed list of media sources receiving the information. Should also provide name of spokesperson assigned to handle media inquiries.*

Notification of Regulators:

A member of BCU's Senior Management staff will notify the regional director within five business days of any catastrophic act, unless the event meets the NCUA's definition of a reportable cyber incident, then the incident must be reported in 72 hours. A catastrophic act is any disaster, natural or otherwise, resulting in physical destruction or damage to the credit union or causing an interruption in vital member services, projected to last more than two consecutive business days. An NCUA a cyber incident as "occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system or actually or imminently jeopardizes, without lawful authority, an information system". A reportable cyber incident is a "substantial cyber incident" leading to one or more of these outcomes:

- A substantial loss of confidentiality, integrity, or availability of a network or member information system…that results from the unauthorized access to or exposure of sensitive, disrupts vital member services, or has a serious impact on the safety and resiliency of operational systems and processes;
- A disruption of business operations, vital member services, or a member information system resulting from a cyberattack from a cyberattack or exploitation of vulnerabilities.

- A disruption of business operations or unauthorized access to sensitive data facilitated through, or caused by, a compromise of a credit union service organization, cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise.

Within a reasonable time after a catastrophic act occurs, the credit union shall ensure that a record of the incident is prepared and filed at its main office. In the preparation of such record, the credit union should include information sufficient to indicate the office where the catastrophic act occurred; when it took place; the amount of the loss, if any; whether any operational or mechanical deficiency(ies) might have contributed to the catastrophic act; and what has been done or is planned to be done to correct the deficiency(ies).

Company Partners Communication

Designated team members will contact assigned Company Partners (CPs) per the contact list. Information to be provided should include recovery time, access points available if any, actions being taken as part of the recovery, member data information with the purpose of alleviating concern.

Sample communication:

Baxter Credit Union (BCU) has recently suffered a (specify disaster type). As of (insert date) BCU is operating with limited resources. You will be contacted by (team member name) with updates, any additional information specific to BCU and (insert CP name), and notification of full recovery. We expect a full recovery by (insert date including time if available). As always, the security of Members' funds, information and Staff are paramount to us. Should you need to reach someone at BCU, (team member name) is your point of contact during recovery time. Thank you for your patience.

Provide Name, Title and contact information

Media Relations

In order to ensure that communication of information is timely, factual, and accurate, and that the credit union's reputation is properly managed, the management team will gather and verify information about the incident, assess the severity of the incident, and develop strategies concerning how information is to be released. Management will then designate a spokesperson who will speak on behalf of the credit union for all media communications. **All other employees of the credit union should refrain from speaking/posting to any media (including social media) source concerning the incident**.

Critical Functions:

Media communication contact: Jill Sammons

First Alternate: Kourtney Ross

Second Alternate: Dani Buschick

Media communication contact will work with senior management and business unit team leaders to gather, develop, and execute timely information. Media communications will also be the primary contact for receiving and filtering media requests.

BCU Spokesperson: John Sahagian

First Alternate: Tom Moore

Second Alternate: Lisa Wilson

Third Alternate: Bob McKay

Fourth Alternate: Mike Valentine

Spokesperson will speak on behalf of the credit union for all media communications.

A Sample press release as well as media contact lists may be found in the Shared Drive under Business Continuity Plan.

Category One - Recover in less than 4 hours.

Areas to be contacted under this category include:

- Employees
    - Headquarters
    - Service Centers
    - Remote
- Members
- Critical Business partners

Category Two - Recover in less than one day

Areas to be contacted under this category include:

- Employees
    - Headquarters
    - Service Centers
    - Remote
- Members
- Select Business partners
- Company Partners with Service centers

Category Three - Recover in less than 5 days

Areas to be contacted under this category include:

- Employees
    - Headquarters
    - Service Centers
    - Remote
- Board
- Members
- Business partners
- Company Partners
- Media

Category Four - 7+ days

Areas to be contacted under this category include:

- Employees
    - Headquarters
    - Service Centers
    - Remote
- Board
- Members
- Business partners
- Company Partners
- Media

Facilities Recovery Team Responsibilities

The Facilities Recovery Team is led by the Facilities Business Continuity Plan Coordinator. The critical functions of the Facilities Recovery Team is to help ensure the security of the employees and assets of BCU. In the case of disaster, the Facilities Team will work directly with law enforcement and fire officials to assist the Management Team in the assessment of damage, and to secure the scene for the protection of salvageable assets as well as public safety.

Responsibilities of the Administrative Recovery Team are:

- Assist with assessing the level of damage to the existing facility.
- Contact local governance agencies as necessary
- Secure external security services as necessary
- Direct and control all salvage efforts related to the facility and records.
- Monitor and control all disaster related expenses.
- Determine the need to use alternate processing site(s).
- Document status of the recovery

- Contact appropriate maintenance/repair contractors in the event of extensive facility damage using the Vendor Phone List (Refer to Appendix C)
- Arrange for basic support services required for operations (i.e., delivery services).
- Obtain replacement or additional office equipment as necessary.
- Arrange for ground/air transportation as appropriate.
- Contact the insurance companies, prepare claim forms, etc.
- Contact appropriate construction or service vendors to arrange site preparation to accommodate replacement hardware if necessary (coordinate with Core Processing/Item Processing and Network/Server Sub Teams).

Responsibility	Description
Emergency/Evacuation Procedures	If the disaster occurs during working hours, the Emergency/Evacuation Procedures should be followed as detailed in this Plan (Appendix B).
Transportation of Items	If relocation of a facility is needed, notify courier service of the location of the alternate site and to arrange pickup/delivery
Salvage	The Facility Recovery Team is responsible for the general salvage of any property damaged in the disaster. This includes any equipment, office furniture, paper record media, supplies and personal effects remaining after the disaster. Th is also responsible for boarding up windows and providing any other immediately necessary security at the disaster site. Salvage procedures are required when damage has occurred to records as a result of a disaster. The type of salvage procedures depends upon the record storage media. Record storage media are defined as magnetic, photographic, and paper.

Alternate Site Locations	Alternate site locations to be used in the event of a disaster have been identified and documented in this Plan (refer to Alternate Location Report, and the Executive Summary Section I.). Various departments may have to be temporarily located in several different locations depending on space requirements and availability. If departments are temporarily relocated to alternate areas, appropriate furniture, equipment, and supplies will be purchased and/or rented as needed. In the case of the staff employees, remote working locations is also feasible, especially those who have remote work approval.
Telecommunications Equipment	If the main facility telephone lines are out-of-service, Management Team have cellular phones available and additional cellular phones will be obtained as needed.
Disaster Site	The Facilities Team should maintain security at the disaster site. The Team may need to obtain additional assistance from a security agency or off-duty police officer(s) as necessary. The initial contact will be with the local police/sheriff department.
Alternate Facility Site(s)	Security at the alternate facility site(s) may be provided by current administration or through the services of security agencies. If additional security is required, BCU will hire temporary off-duty police or other security agency employees.
Police and Fire Departments	Local police and fire departments can be reached in all locations via “911”.
Delivery Service Provider Notification	The Administrative Recovery Team should contact the local delivery service providers (USPS, UPS, FedEx & DHL) and instruct them as to where the packages should be delivered. Unless otherwise determined, packages should be delivered to the Command-and-Control Center.

The Equipment, Forms and office supplies can be shared with other sites when need be. Additional supplies can be “rush” ordered from our supplier (see Exhibit C-2 -Vendor List). In the immediate aftermath of a disaster, some departmental employees may be instructed to remain at home on a stand-by basis.

Due to minimal time involved, the Data Center Recovery Location, Crystal Lake Service Center and a Mobile Facility may be used as alternate sites. All computer functions can be duplicated at these locations.

BCU will utilize available commercial space if extend periods of time are required to resume normal operations. Additional furniture, equipment, telecommunication lines, etc. can be in place within a 24 to 72-hour notice as needed.

In the case of the staff employees, remote working locations is also feasible, especially those who have remote work approval.

Technology Recovery Team Responsibilities

When it has been determined to declare a Disaster resulting from a disruption of services required, the Technical Business Continuity Plan Coordinator will lead the effort to perform the restoration of the computing platforms, including the networking and telephony platforms, that have been disrupted.

The Technical Recovery Team may also be asked to assist in a business continuity disruption or other scenario where only sections of The Plan is being enacted. The Technical Recovery Team is charged with the restoration of business services within their stated recovery time and recovery point objectives. The Disaster Recovery Playbooks are stored in conjunction, and in the same manner as the Business Continuity Plan. See Appendix M for the criticality recovery definition and recovery time objectives.

The Technical Recovery Team's primary responsibilities include but are not limited to the following list. Note that the dependent on the declared disaster, this list may vary to address specific situations.

1. Review damage assessment.
2. Determine which hardware, software, network, telephony, storage, and supplies will be needed to start the restoration of a particular system(s).
3. Communicate list of components to be purchased and their specifications to the Administrative Support Team.
4. Review the recovery steps documented in this plan and make any changes necessary to fit the situations present.
5. When hardware begins to arrive, work with vendor representatives to install the equipment.
6. When all components are assembled, begin the steps to restore the operating system(s) and other data from the backups.
7. Communicate any needed technological changes to the network and computing environments in the restoration process to the Security Recovery Administrator to ensure that the associated security risks are identified, mitigated as possible and communicated to the Command team for acceptance of unmitigated risk.
8. Attempt to recreate status of all systems up to the point of the disaster, if possible, with the stated recovery time and recovery point objectives. If not, the system is handed off to the Application & Operation Recovery Team Administrator.

From current location, if available, or from off-site storage, gather necessary program data files, backup run documentation, forms, and supplies to complete off-site processing.

In conjunction with the Facilities Recovery Team, determine the amount of equipment that can be salvaged from current site.

Coordinate resources with Agility Recovery to:

- Cable and connect temporary workstations at the alternate site location, as needed.
- Configure and implement connection to the network at alternate site location as needed.
- Provide Command Team with estimated number of Workstations, and PCs needed to replace destroyed equipment.
- Add non-critical applications as capacity allows and directed by the Management Team.

Application & Operations Recovery Team Responsibilities

The Application & Operations Recovery Team is led by the Application Continuity Plan Coordinator. The critical functions of the Application & Operations Recovery Team is to assess BCU's ability to provide services to our members and overall impact to operations. In the case of disaster, the Application & Operations Recovery Team will work the department managers in the assessment of damage, and to share the assessment with the Command Team.

This team will also be responsible for conducting activities leading up to the approval and acceptance of application systems for production use. Once a disaster is declared, the Application & Operations Business Continuity Plan Coordinator will direct the following activities:

- Notify team members and inform them of when and where to meet. Each team member will notify staff and inform them when and where to report to work.
- Be prepared to assist in communication to BCU locations and keep them informed of disaster implementation.
- Assist with processing and/or information questions.
- Identify what systems and operations need recovery.
- Assist Command Team with understanding the member and operational impacts of incident.
- Review recovery tiers and confirm order of operational recovery.
- Work with vendors to identify if their capabilities of providing member services. If unable, coordinate vendor connectivity with Technology Recovery Team.
- Be available to assist other areas as directed by the Command Management Team.

Once the Application & Operation Recovery Team has identified the impact to BCU's applications and operations, the Application Recover team Administrator will partner with the Technology Recovery Team Administrator to

ensure that he/she has a proper understanding of the processes and systems that need to be recovered. The joint teams will used previously agreed upon recovery objectives to restore business processes. If there is a need to veer from the standard recovery order, the Command Team can approve modifications to the recovery order.

For critical processes not needing to be restored by the Technology Recovery Team, the Application & Operations Team is responsible for work with the Team Managers to:

- Understand what processes are being recovered.
- The prioritization of the restoration of recovery.
- Resolving resource conflicts in the recovery process.
- Coordinating recovery processes with vendors.
- Impacts to member service and communication of those impacts to the Communication Recovery Team.
- Establish an on-going communication cadence.
- Monitor and communicate when restoration is complete.

Data Recovery Team Responsibilities

The Data Recovery Team is led by the Data Business Continuity Plan Coordinator. The critical functions of the Data Recovery Team is to help ensure that the data needed to analyze, monitor, and manage member and business processes is recovered appropriately. In the case of disaster, the Data Recovery Team will directly work with Technology Recovery Team and Member Intelligence, analysts, data base analysts and vendors to understand the impacts of the disaster and required assistance to the recovery processes. If appropriate, assist the Command Team with the prioritization of process.

The Data Business Continuity Plan Coordinator will ensure that all Team Members are notified on a ***need-to-know basis***, information to be supplied may include:

- general description of the disaster
- level of disaster
- location of the Command-and-Control Center, if appropriate
- the immediate action required
- plan for recovery
- external support requirements
- estimated recovery time

In addition, the Data Business Continuity Plan Administrator may need to:

- Communicate to the Technology Recovery and Application & Operations Teams the impacts of any data related failed processes
- Coordinate data recovery activities with the Security Recovery Team

- Coordinate data recovery activities with the Technology Recovery Team
- Coordinate data recovery activities with our vendors that provide input files to the data warehouse and lake environments.

Security Recovery Team Responsibilities

The Security Recovery Team is led by the Security Business Continuity Administrator and is responsible for ensuring accurate and timely recovery of any security tools impacted by the incident, ensure that there aren't any new security events resulting from an incident and approve any temporary changes to BCU's security practices. To prevent any negative impact on BCU it is imperative that all communications portray that a well-planned recovery program has been implemented.

The Security Business Continuity Administrator will ensure that all Team Members are notified on a ***need-to-know basis***, information to be supplied may include:

- General description of the disaster
- Level of disaster
- Location of the Command-and-Control Center, if appropriate
- The immediate action required
- Plan for recovery
- External support requirements
- Estimated recovery time

Additional responsibilities may include:

- Working with Security consultants to assess environment and provide professional advice
- As appropriate, engage approved consultants to run forensic activities
- As appropriate, approve temporary changes to BCU's security procedures/policies to ensure the safety of member data, BCU employees and assets.
- Understand any needed technological changes to the network and computing environments in the restoration process and ensure that the associated risks are identified, mitigated as possible and communicated to the Command team for acceptance of unmitigated risk.
- Partner with Technology Business Continuity Administrator to implement needed patches or other changes to the technical environment.

The Business Continuity Plan, in conjunction with BCU's Incident Response Plan, are designed to support BCU in the identification, containment, remediation and resolution of cybersecurity events.

It is imperative that if the event meets the NCUA's definition of a reportable cyber incident, then the incident must be reported in 72 hours. An NCUA a cyber incident as "occurrence that actually or imminently jeopardizes, without

lawful authority, the integrity, confidentiality, or availability of information on an information system or actually or imminently jeopardizes, without lawful authority, an information system". A reportable cyber incident is a "substantial cyber incident" leading to one or more of these outcomes:

- A substantial loss of confidentiality, integrity, or availability of a network or member information system…that results from the unauthorized access to or exposure of sensitive, disrupts vital member services, or has a serious impact on the safety and resiliency of operational systems and processes;
- A disruption of business operations, vital member services, or a member information system resulting from a cyberattack from a cyberattack or exploitation of vulnerabilities.
- A disruption of business operations or unauthorized access to sensitive data facilitated through, or caused by, a compromise of a credit union service organization, cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise.

In the event of the of cybersecurity incident, the CISO should first reference BCU's Incident Response Plan for instructions on how to identify, define and classify a cybersecurity attack. The Incident Response Plan will also provide direction on escalation ad notification protocols. If during the containment and remediation process it's determined that additional resources of the focus of the Command team is necessary, the Business Continuity Plan can be activated.

TRAINING

Training has been incorporated into the Business Continuity Program to ensure all participants understand their unique responsibilities. The BCP Administrator is responsible for the development and oversight of the training program. The Board of Directors is responsible for ensuring the effectiveness of the training program. Reporting of the content and results of training efforts is provided to the Board promptly to allow for remediation of deficiencies.

The training program is developed based on the teams and departments and their individual tasks and responsibilities. Training and testing exercises follow a frequency standard based on the criticality and risk of each unique function. An inventory of current skill sets for business continuity is maintained to ensure all responsibilities are adequately addressed given changes in staff and roles. Some of the elements of the training program may include:

- Exercises
- Potential risks
- Recent continuity events or live tests
- New programs/technologies
- Organizational changes
- Previous (exercise) lessons learned

The training program provides for an understanding of the program, policy, plan, testing methods, test results, and critical business functions. Training on the criteria for activating the Business Continuity Program has also been incorporated. Training is provided to all based on their level of responsibility in the program.

Board reporting occurs annually or more frequently when significant changes to business processes, risks, BIA results, or lessons learned from events occur. Reporting methods include group training events, computer-based training, hands-on exercises, and tabletop exercises. Team training includes cross training to ensure adequate knowledge and understanding to compensate for loss or unavailability of staff. Training materials are updated to reflect changes to the business continuity program as they occur.

TESTING

Testing Plans

This section provides policies to establish the need and frequency for testing the Plan. It is very important to stress the need for and value of testing; an untested plan provides little assurance of the Plan's validity or recovery achievability. Testing strategies should be identified by the Management Team and a detailed testing plan should be developed so, that over a period of time, all aspects of the Plan can be fully tested.

Test Schedule

Performing scheduled tests as outlined by BCU. The Plan should be tested at least annually. Initially, testing should not be scheduled at critical points in the normal processing cycle (e.g., month-end).

The Business Resiliency Director is responsible for performing tests and for documenting the results of the test(s). In addition, the Business Resiliency Director is also responsible for updating the Plan as required, based on the results of the test(s).

Test Procedures

A test plan should be prepared prior to each test which will identify the scope and objectives of the test and the format the test will assume. Realistic testing of all sections of the Plan should be performed periodically. The objectives of testing include:

- Confirmation that the procedures work.
- Identification of areas requiring modification.
- Familiarization and training of employees with the procedures.
- Increased confidence in the ability of BCU to recover in a timely manner.

Test Results

The tests should initially be performed when it will not cause disruption to operations. Once tested, the results of the tests should be documented, and the Plan updated accordingly.

After completion of each test, documentation and results should be completed and stored in a safe place for future reference. Test results should be presented to the BCP Committee and Board of Directors of BCU, and the review of the results documented in the minutes. The results may also be requested by examiners.

Current Testing

The Business Continuity Plan Coordinator's maintain the most current copies of testing documentation and results.

DOCUMENT VERSION CONTROL

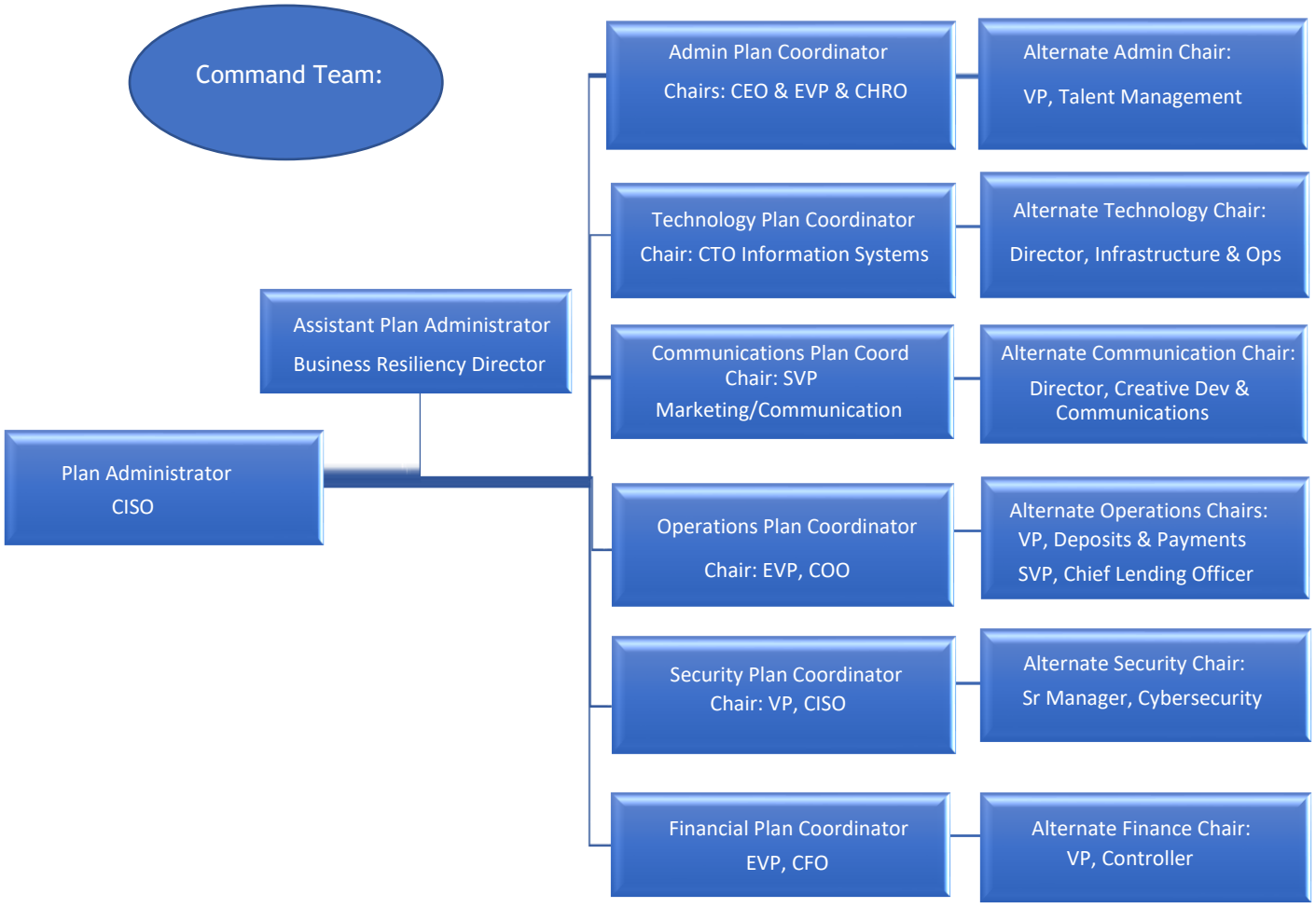
Change History

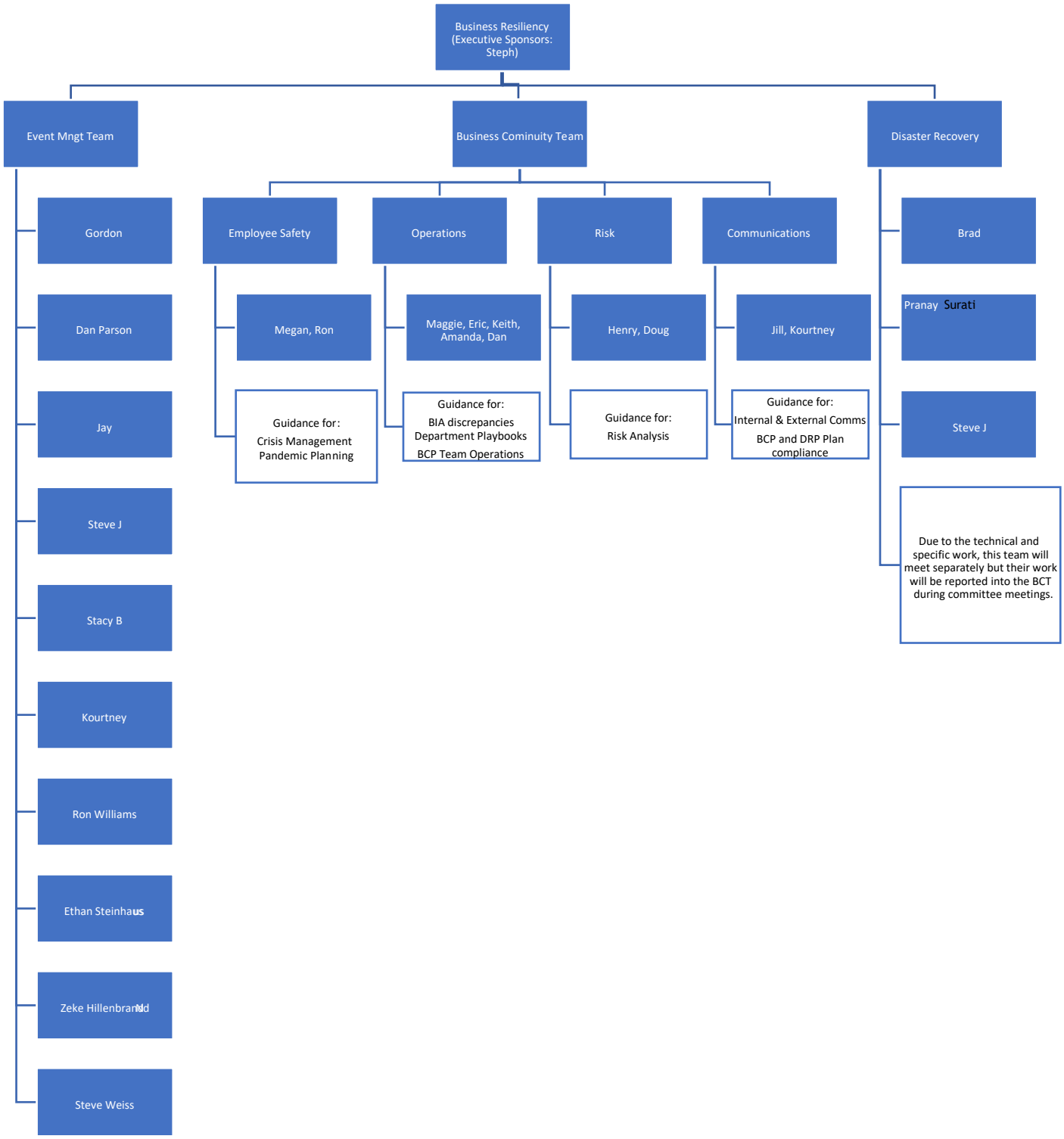
Version	Change	Author	Date
1.0	Plan Refresh: • Document ownership change • Business Continuity Org chart updates • Role updates • Communication Plan update • Pandemic Plan update • Crisis Management updates • Refresh of contract information for all employees • Vendor Management updates	Kelli Bartczyszyn	5/12/2022
1.1	Plan Updates: • BCP scope to include facilities and network • Expand restoration to include cyberattacks • Included NCUA cyberattack notification rule • Add reference to remote work force • Update Critical Vendor list • Miscellaneous minor updates	Kelli Bartczyszyn	4/1/2023
1.2	• Minor wording and employee updates	Keli Bartczyszyn	5/30/2024

Approval History

Version	Name	Title	Date
1.0	Board Approval	Board Approval	5/30/2022
1.1	Board Approval	Board Approval	5/24/2023
1.2	Board Approval	Board Approval	6/26/2024

APPENDIX A: BUSINESS RESILIENCY MANAGEMENT TEAMS




Business Resiliency (Executive Sponsors: Steph)
Event Mngt Team
Business Cominuity Team
Disaster Recovery
Gordon
Dan Parson
Jay
Steve J
Stacy B
Kourtney
Ron Williams
Ethan Steinhaus
Zeke Hillenbrand
Steve Weiss
Employee Safety
Operations
Risk
Communications
Megan, Ron
Maggie, Eric, Keith, Amanda, Dan
Henry, Doug
Jill, Kourtney
Guidance for:
Crisis Management
Pandemic Planning
Guidance for:
BIA discrepancies
Department Playbooks
BCP Team Operations
Guidance for:
Risk Analysis
Guidance for:
Internal & External Comms
BCP and DRP Plan compliance
Brad
Pranay Surati
Steve J
Due to the technical and specific work, this team will meet separately but their work will be reported into the BCT during committee meetings.

APPENDIX B, EMERGENCY PROCEDURES

BCU - Headquarters

FIRE EVACUATION

CALL FIRE DEPARTMENT -911

In the event of a fire at BCU headquarters, it will be the responsibility of the employee finding the fire to alert company management. An announcement will be made alerting all employees and customers of the situation.

Fire extinguishers are located in specific areas of BCU. In the event that the fire alert is given, the designated Fire Warden for that Department will ascertain that all employees heard the alert.

Each floor of the headquarters building shall designate a "FIRE WARDEN". In case the designated Fire Warden is absent an alternate shall also be designated. The names of these Fire Wardens will be given to the BCP Coordinator. The duties of the Fire Warden or alternate will be to:

1. Assure that all customers and employees are aware that a fire alert has been issued and that customers and employees evacuate the building in a calm and safe manner using the stairs.
2. When reaching the safe designated meeting spot, the North-East corner of the parking lot, check that all employees working on his/her department have been accounted for and are safely out of the building.
3. Report to Fire Department the possibility of any missing employee from the floor that may still be in the building.
4. Explain to any new employee of the Department, the Fire Evacuation Plan, the location of the fire extinguishers and the location of the meeting spot after exiting the building during a fire evacuation.

Evacuation Procedures

Applies to

This policy applies to all Vernon Hills employees. Service Center employees should refer to the evacuation procedures of their local facility.

Modified Evacuation Procedures for Employees / Visitors with Disabilities

Employees and visitors with permanent or temporary disabilities that limit their ability to safely evacuate the building are strongly encouraged to report this disability to the occupational health nurse at DF (Ext. 884-2038). This information will remain strictly confidential and will be utilized only to assist in a safe evacuation from the building.

Disabilities are not always obvious. The disability may be permanent or temporary. Inquire if any employees in your group have any special needs that would make evacuation or taking cover difficult or impossible. The employee does not need to disclose the specific disability to you, but if the employee does disclose you must keep this information confidential.

- All employees with any type of disability that could hinder their ability to evacuate the building or to take cover must have a minimum of two "buddies" to assist them.
- "Buddies" may be selected by the employee or their supervisor. The "buddies" should work near the employee with Disabilities, have a similar work schedule and be level-headed in emergency situations.
- A minimum of two "buddies" accompany the affected employee to the stair tower entrance.
- Enter the stair tower entrance after all (or a majority of) the traffic from your area has entered. NOTE: The Vernon Hills facility has three stair towers: North, Central and South.
- One "buddy" stays with the affected employee and the other sends word down to the Fire Department that there is an employee in (specify location) stair tower needing assistance.
- Close the door and remain there until the fire department evacuates you from the stair tower.

Fire Evacuation Guidelines (Vernon Hills facility)

Previous to the Evacuation

- Become familiar with your workplace.
- Know two ways out of the building.
- Formulate a workplace escape map showing two ways of exiting the building.
- Appoint a designated alternate head counter.
- Evaluate the need for a buddy for any employee with a permanent or temporary disability.
- Report Disabilities (Temporary or Permanent) to Human Resources.
- Use the “BUDDIES” system: Two or more co-workers that will help the individual with the disability to evacuate.

During The Evacuation

- Leave by the nearest safest exit,
- Follow the overhead “EXIT” signs.
- Go down to the first floor and out to the exterior.
- Always keep the doors closed.

After The Evacuation

- Once outside, go to your assembly area for the head count:

If your nameplate has SW or SE, gather by the entrance to the CDW parking lot.

If your nameplate has NW or NE, gather at the Southeast side of the parking lot. This is at the back of the building in the grassy area along Milwaukee Avenue

For example, if your nameplate is 01SE010, you will go the area marked Evacuation Assembly Point Southwest / Southeast.

- Headcount every member of your department.
- Re-enter the building only when the "ALL CLEAR" is given. Only Security, Facilities Management or fire Department will give the "ALL CLEAR".

If Evacuation Is Not Possible

- Stay below the smoke at all times.
- If trapped, close all doors between you and the fire.
- Signal for help from a (telephone, cell phone, fax, window).

Always…

- Assume all alarms signify a true emergency.
- Be responsible for your visitors.
- Refrain from smoking until the head count is completed.
- Never use the elevators in an emergency evacuation.
- Close all doors behind you.
- Refer media questions to the appropriate company management.
- Stay Calm.

Contact

For more information, contact BCU Human Resources or Vernon Hills Building Management.

POST EMERGENCY

1. When the danger has passed, the officers will check BCU's facilities for damage and will determine if BCU is immediately operable.
2. If it is determined that BCU is temporarily inoperable, BCU will be closed and the BCP Command Team will be assembled.
3. If the BCU is operable, the employees and customers will be directed back to the lobby.

Completion of all procedures is not mandatory. THE SAFETY OF THE EMPLOYEES AND CUSTOMERS IS ALWAYS THE FIRST PRIORITY. Employees should proceed directly to the Designated Meeting Place if they feel that they do not have enough time to safely follow all procedures.

Natural Disasters

TORNADOES

Tornado Safety – Vernon Hills only

(all remote Service Centers should follow their local plant/building procedures)

Tornado Shelter Procedures

- There will be an announcement when there is danger of a tornado.
- Move all employees and guests to safe areas, away from windows and large rooms.
- Supervisors should make a sweep of their department to make sure employees and guests have left for a safe area.
- Remain in safe area until warning expires or until emergency personnel have issued an all-clear signal either by the paging system and or personal notification.
- If building has been damaged, assemble crisis team to assess damage, administer first aid and order evacuation, if necessary.
    - **NOTE:** If we are instructed to evacuate the building after the threat is over, please remain on the property so a complete head count can be established.
- If an employee or visitor is unable to take the stairs, contact a MERT Team member by dialing 8888 for assistance.

Accounting, Finance, and Auditing should go to the South Stairwell.	**Talent Management** should go to 4th floor north break area, copy area and washroom corridor.
Lending Operations should go to the North Stairwell. **Building Services** should go to the Facilities Storeroom. 1SE012	**General Admin, Senior Management, and H.R.** should go to the Executive Storage Room 4SW016 or 4th floor restrooms. **Service Center Staff** should go into the Branch Equipment File Room 1SW009
	Members should be escorted to the 1st floor washroom corridor. Stay with the member until the all clear is given.

Marketing and Business Development should go to the North Stairwell.	**Investment Advisors and Executive Services** should go to the Investment Advisors File Room 1NW031 and Copy Room.
Information Systems 2nd floor should go to the Fitness Center Storage Room 2NE075A. **Computer Room Operators** should go to the Staging Room 1SE017.	**Collateral and Documentation** should go to the 3rd floor north break area and copy area
Collections and Titles should go to the 3rd floor washrooms	**Member Relations** should go to the Floridian Room 3SW015.
Mortgages and Sales should go to 2rd floor north break area, copy area, Infirmary, Mothering Room, and washroom corridor.	**Account Service** should go to the Account Services File Room 3SW038 and Elevator Lobby.
Loan Sales should go to 3rd floor north break area, copy area and washroom corridor.	**Cards and Fraud** should go to the South stairwell.

Note:

- We have some employees located sporadically throughout the building, so please identify the department nearest your primary location and utilize the proper safe area.
- Some employees may be located in "Common Areas" during a tornado emergency. In an event such as this, locate the safe area nearest the common area. Safe Areas Include: Elevator Lobbies, Break Areas North and South, Copy Areas North and South, Washrooms and Stairwells

ALL SAFE AREAS ARE LOCATED ON ALL FLOORS

In addition, the southeast corridor on the first floor is an additional safe area.

POST EMERGENCY

1. When the danger has passed, the officers will check BCU's facilities for damage and will determine if BCU is immediately operable.
2. If it is determined that BCU is temporarily inoperable, the customers will be asked to leave the premises.
3. If BCU is operable, the employees and customers will be directed back to the lobby.

Completion of all procedures is not mandatory. **THE SAFETY OF THE EMPLOYEES AND CUSTOMERS IS ALWAYS THE FIRST PRIORITY**. Employees should proceed directly to the Safety Area if they feel that they do not have enough time to safely follow all procedures.

EARTHQUAKES

Earthquakes have no reliable prior warning. All employees should be aware that if an earthquake occurs, they should take cover under a desk, table, bench or stand in a doorway or against an inside wall. During the quake, one should avoid glass windows (both interior and exterior), bookshelves or any object that could fall.

After the initial earthquake, the possibilities of fire or aftershocks are likely. The employee should assist any person that might have been injured in their immediate area by rendering First Aid and assisting them to leave the building under the "Fire Evacuation Plan." Once outside the building, the

employee should move to the designated "meeting spot" as in the "Fire Evacuation Plan" away from the building avoiding falling glass and/or building material. Fire Wardens shall ascertain if all employees are present and, if not, inform the appropriate authorities so rescue operations can be made.

The Business Recovery Team should be notified for implementation of the Business Continuity Plan.

HAZARDOUS MATERIAL

BCU's Command Team will determine the action(s) to be taken in the event of a hazardous material spill/leak threatening BCU and/or its staff. At the time an alert is issued, the Fire Wardens or their alternates of each Department shall make sure that all employees are aware that an alert has been issued. All employees should (if time permits) close all exterior windows and doors, turn off all air circulation equipment that brings outside air into BCU, close file cabinets, turn off or place in idle state all computers and machines they were working with (the exception to this is the mainframe and network servers). Negotiable items should be secured. However, efforts should be abandoned if the safety of an employee would be compromised in doing so.

If directed by emergency personnel to evacuate the facility, proceed to a designated safe zone established by your city/county emergency planner, and await further direction.

NUCLEAR EMERGENCY

BCU's Command Team will determine the action to be taken by in the event of a nuclear emergency. When a declared readiness condition is announced by state civil defense during working hours, BCU will follow instruction related to each readiness condition (REACON).

REACON 3 - International situation degenerated to the point where a break in diplomatic relations may occur, a nearby nuclear facility has announced a potentially hazardous situation or nuclear transport vehicle is disabled in the area. All employees will be alerted to stand by for further announcements.

REACON 2 - Serious deterioration of international relationships with a break of diplomatic channels and possibility of hostile actions, a nearby nuclear facility has issued an alert to a probably hazardous situation or a nuclear transport in the area has been involved in an accident. Management will outline action to secure records and negotiable items. Staff will be reduced to minimum operation. Staff members relieved of duties will be permitted to go home or to a civil defense shelter area in the building. The middle area of the lower floor has been designated the "Civil Defense Shelter Area" for this building.

REACON 1 - War is imminent or hostilities may have already occurred. This declaration may be announced before or concurrently with "Attack Warnings", a nuclear facility has been compromised or a nuclear transport vehicle has spilled its load in the area. BCU's records will be moved to the safe areas. Upon securing the BCU assets, employees will be permitted to leave the premises or go to the civil defense area in the lower level of the building.

BOMB THREATS - STANDARD OPERATING PROCEDURE

PURPOSE

The purpose of this section is to define and describe acceptable staff procedures for preventing or responding to a bomb threat, to avoid confusion and to assign responsibility for the performance of necessary tasks.

POLICY

It is the institution's policy that all employees will take extraordinary measures to ensure their own safety and the safety of other persons who may become involved in a bomb event, including:

- Recognizing that delivering a bomb threat is primarily a business crime.
- Caring for their own safety first, before considering others' safety.
- Complying with the offender's demands if it's possible; and
- Facilitating the offender's successful delivery of the bomb threat if it's possible.

Staff employees are responsible for taking preventive measures to reduce the potential of a bomb being placed within the facility, including:

- Constantly remaining aware of their surroundings and their geographic location.
- Becoming and remaining familiar with all areas of your facility and with the things that should be in those locations.
- Carefully following facility entry and exit safety measures.
- Observing, acting upon and reporting any unusual incidents and behavior.
- Knowing what to do during a bomb threat, including:
    - Knowing procedures to follow during emergency responses.
    - Studying procedures.
    - Reviewing suspect description and reporting forms.
    - Ensuring that the workstation in use contains all emergency forms, and that the surrounding areas are kept free from debris and other items that may conceal a bomb; and knowing the locations and capabilities of security devices.
- Not discussing personal and business issues with non-employees, including:
    - Institution and employee information.
    - Physical layout of the office.
    - Personal matters.
    - Details of item/document-handling procedures.
    - Transportation route information; and
    - Security procedures.

Staff employees are responsible for taking appropriate measures to protect themselves and to assist a law enforcement agency during a bomb threat, including:

- Remembering that your primary responsibility is to help the police find the bomb.
- Completing the appropriate form and asking all questions, if it's possible, because the primary purpose of the person receiving the threat call is to keep the caller on the telephone line while obtaining as much information as possible.

- Notifying the nearest supervisor or the Facilities Manager of the bomb threat at the earliest opportunity.
- Keeping the telephone line on which, the call was received open for the duration of the event and ensuring that any notifications are made on alternate telephone lines.
- Doing exactly what the offender commands, including:
    - Repeating the commands back to the offender if you can.
    - Telling the offender, "I'll do exactly what you tell me to do".
    - Not making any comments that threaten the offender.
    - Attempt to develop rapport with the offender by developing a "relationship".
    - Agreeing to do whatever the offender tells you to do.
    - Promising not to call the police.
    - Suggesting that the Facilities Manager should talk with the caller.
    - Remaining as the offender's contact person for the duration of the incident, if practical, if the caller specifically demands it.
    - Remaining the only person talking with the caller but having another employee monitor the call, and each employee is responsible for completing the appropriate form.
    - After receiving the initial message, asking the caller to repeat the message for clarity; and
    - Remembering that no employee is to act in any way that might endanger his/her safety, or the safety of another person.

Staff employees are responsible for continuing to take appropriate and timely measures to protect themselves and to assist a law enforcement agency after a bomb threat, including:

- Immediately notifying the Facilities Manager.
- Being assigned to the Facilities Manager handling the bomb threat call for the duration of the incident.
- Awaiting further instructions from the Facilities Manager.
- Following the instructions received from the Facilities Manager, any on-site supervisor, or a representative of the responsible law enforcement agency.
- Not activating the robbery alarms in response to any bomb threat call.
- Any other employees witnessing unusual or suspicious activities within or around the office during the call are to immediately report this information to the Facilities Manager.
- Searching the areas immediately surrounding their workstations and reporting objects that are unusual or suspicious, remembering that no employee will touch or disturb the object.
- If the office is evacuated, all persons leaving the building will be guided to the appropriate emergency staging area(s) by members of the emergency evacuation team.
- Identifying witnesses and asking them to remain, pending contact by the law enforcement agency.
- Remaining at the emergency staging area until they are authorized to leave by the Facilities Manager or the Security Director.
- Completing reports and forms as it's appropriate; and
- Referring all requests for interviews by the media to the law enforcement agency or the Security Director.

CIVIL DISTURBANCES

Upon receiving notification that a civil disturbance threatens the building or your office space, contact Management and give the following instructions:

- Exact LOCATION of the Demonstrators
- Approximate number of Demonstrators
- Demonstrator's current activity
- Your Name: Time:

Notify your employees and visitors about the civil disturbance and contact your assistants and assign them specific emergency duties.

- Give them pertinent facts about the Civil Disturbance
- Assign them to execute the following emergency procedures -- for safety and protection of BCU employees and company assets:
- Lock all doors except your main entrance door.
- Lock, or have someone stand by to lock all sensitive areas as appropriate e.g., office doors, equipment rooms, storerooms, mail rooms, desks, file cabinets, vaults, etc., to protect company assets, employees, and visitors.
- Notify all employees and visitors about the Civil Disturbance and warn them to avoid personal contact with the demonstrators and try to not make any comments or statements to further anger the demonstrators.
- Advise all employees and visitors to avoid leaving the building unless there is no danger that they will be harmed by the demonstrators.
- Advise all employees and Visitors to avoid walking through the Lobby Areas while the demonstrators present a threat to break and shatter ground level windows.

IMPORTANT: Periodically advise all employees and visitors of the situation.

If the demonstrators have invaded the building and they are in your area, you should do the following:

- Immediately contact Management, employees, and visitors:
  - Advise them of this change in status of the emergency.
- Assign employees to execute the following (additional) emergency procedures to ensure safety:
  - Lock your main entrance door.
  - Have a responsible employee stand by at the entrance door with a key to allow authorized employees (only) to enter and/or leave.
  - Lock all sensitive areas as appropriate.
  - If the demonstrators invade your floor(s) and office(s), your employees should make notes of all rooms and/or areas invaded by the demonstrators to facilitate follow-up searches for suspicious items.
- When the demonstrators leave or are removed by the Police and the Civil Disturbance is no longer threatening the building:
  - If the demonstrators invaded your floor(s) and office(s):
  - Immediately contact Management and give them a list of your floor(s) and office(s) that were invaded.
  - Tell your assistants to initiate a quick search of your invaded floor(s) and office(s) for any items that are unusual or foreign to the normal environment.

IMPORTANT: Warn them to be alert for unattended and suspicious items that were carried by the demonstrators, e.g., clothing, knapsacks, bags, etc. Also, warn them not to touch, move, jar, disturb, or cover any suspicious items that are found. Tell them to warn their employees and visitors accordingly. Tell them to advise you immediately when they finish their search so you can immediately relay the information to Management.

MEDICAL EMERGENCIES

If there is a "Medical Emergency" within your office or observed by you, call 911 and give the following information:

- Nature of the Medical Emergency.
- Exact location and name of the sick or injured person.
- Confirm to Management if an ambulance or doctor has been notified.
    - If not, your supervisor will contact an ambulance service and make ready their entrance into the building, if necessary.
    - If the sick or injured person requests that you call their doctor, do so and notify your supervisor so assistance can be given the doctor when entering the building.

Assign one of your assistants to stand by in the area where the sick or injured person is located to meet the doctor and/or ambulance attendants and guide them to the sick or injured person.

If the sick or injured person is to be sent to the hospital, try to send a friend or fellow employee along to comfort the person and help him/her at the hospital until a relative arrives.

CONCLUSION OF MEDICAL EMERGENCY

Following the conclusion of the Medical Emergency:

- Consult with your assistants and determine if they encountered any special problems or incidents during the performance of their emergency duties.
- For future reference by your supervisor, prepare a brief written report of your efforts and actions in response to the emergency, including any special problems or incidents that you encountered, and submit the reports to your supervisor as soon as possible. (NOTE: Retain copies of your report for future reference by yourself, your Employer and/or any Company Executives.)

OTHER EMERGENCIES

ELECTRIC POWER OUTAGE

The building is equipped with emergency lighting which will turn on during a power outage. If an outage is of short duration, it should cause little concern. If it is of longer duration, you may wish to leave the building. You will be advised by Company Executive Management on any action to be taken.

APPENDIX C, CRITICAL PHONE LISTINGS

EXHIBIT C-1, CRITICAL CONTACT LISTS

EMERGENCY RESPONDERS	Service	Phone	Address or Contact name
Emergency		911	
Ambulance	Ambulance	911	
Fire Department	Countryside Fire Protection District	847-367-5511	
Police Department	Non-Emergency	847-362-4449	
County Sheriff's Dept	Non-Emergency	847-377-4000	
FBI	Local Field Office		
UTILITY COMPANIES	**Service**	**Phone**	**Address or Contact name**
Electric Utility	Mid-American Energy Services, LLC	800-432-8574	PO Box 8019, Davenport, IA 52808
Macke Water Systems	Water Systems	847-459-1030	Gartenberg, Alan
Sewer			
SECURITY	**Service**	**Phone**	**Address or Contact name**
Convergint Technologies	Security Services	224-412-2118	Tom Eich
Waukegan Lock & Safe	Locksmith	847-336-3910	Bill Oechsle
Baxter Security	Security Services	224-948-3484	David Koehn
RD Systems	Security Services	714-873-6923	Kozick, Dan
Glenbrook Security Services	Security Guard	847-279-6465 x 38	Bucklin, Roy
ResourceOne	Security Services	614-203-1737	Brodbeck, Dale
CUNA	**Service**	**Phone**	**Address or Contact name**
CUNA Mutual	Insurance Carrier	800.356.2644 665.5502 or 608.236.8509	Jason Disch Jason.Disch@cunamutual.com
COURIERS	**Service**	**Phone**	**Address or Contact name**

APC (UPS)	APC by Snyder Electric	800-800-4272	877-272-2722
Post Office	Mail	847-566-3902	Vernon Hills Post Office

EXHIBIT C-2, CRITICAL VENDOR LISTING

Owner	Vendor Name	Vendor Contact Name	Vendor Contact Phone	Vendor Contact Email
Joe McCarthy	Accenture (fka Prime Alliance Solutions, Inc.)	Laura Roberts	512-726-1565	l.roberts@mortgagecadence.com
Davi Allen	Akuvo	Carla Bramble		
Scott Zulpo	AT&T	Nicolas Wood	312-203-1391	nw593p@att.com
Dominique Angom	Blend	Chris Etterman	408-805-0082	chrise@blend.com
David Brydun	Cenlar FSB	Charlie Fues		chfues@cenlar.com
Harvey Rindt	Clifton Larson Allen	David Anderson	612-376-4699	david.anderson@claconnect.com
Karl Grom	Concur Technologies, Inc.	Thomas M. Nolan		
Scott Comeau	CUNA Brokerage Services, Inc			
Joe McCarthy	Fannie Mae	Hoelscher, Priscilla		priscilla_m_hoelscher@fanniemae.com
Amy Primrose	Federal Home Loan Bank of Chicago	Jeff Long	(312) 552-2669	jlong@fhlb.com
Maggie Garcia	Federal Reserve Bank (FRB)	Pavel Reytikh	312-322-6087	Pavel.Reytikh@chi.frb.org
Davi Allen	Fidelity Information Services LLC (FIS)			
Keith Parris	Genesys Cloud Services, Inc.	Genesys US Legal		
Scott Zulpo	Jack Henry-Symitar	Kristie Osborn	417-601-2286	KrOsborn@jackhenry.com
Scott Comeau	LPL Financial LLC			
Scott Zulpo	Masergy Communications	Nobino Zachariah		nobino.zachariah@masergy.com
Scott Zulpo	Microsoft	Misti Hempfling		Misti.Hempfling@microsoft.com
Lidya Garcia	NYCE Payments Network, LLC, (FIS)	Gentile, Fran	470-416-2764	Fran.Gentile@fisglobal.com
Maggie Garcia	PSCU Financial Services, Inc.	Tom McGargill	(402) 884-0929	tmcgargill@pscu.com
Lauri Galdine	RBA Consulting	Rachelle Epley		Rachelle.epley@rbaconsulting.com
John Sahagian	Salesforce.com	Julie O'Gara	312-821-6011	jogara@salesforce.com
Eric Liesener	Temenos (fka Akcelerant)	Bryan Niedzwiecki		bniedzwiecki@temenos.com
Stephenie Southard	TierPoint LLC	Nicole Dupree	984.328.5662	nicole.dupree@tierpoint.com
David Brydun	VISA	Angela Kuo		akuo@visa.com

APPENDIX D, OFF-SITE STORAGE

OFF-SITE STORAGE FACILITY ACCESS

BCU utilizes both physical and virtual data centers to store system back-ups. In addition, the physical data center contains:

- Business Continuity Plan
- Offline FRB Wire codes
- Employee emergency contact info
- Supplies
- Back-ups:
    - NetApp: Vernon Hills goes to Milwaukee. For those unique to Milwaukee, they come to the Vernon Hills NetApp.
    - Commvault: Commvault it's back-ups to the appropriate Azure region. Full back-up to one of three storage servers in two different Azure regions.
    - Azure Back Ups: Conceptually everything has a primary region and a DR region. The backups happen in the primary region and the back-ups to a vault in the DR regions.
    - For example, North Central is the primary processing where all new things are being built so their back-ups would be sent to South Central.
        - Azure Replication: Works the same way as Azure back-up, only for replication.

APPENDIX E, BYLAWS AND RESOLUTIONS

BYLAWS TO PROVIDE FOR EMERGENCY OPERATIONS BY SURVIVING STAFF

EMERGENCY PREPAREDNESS

EMERGENCIES: In the event of an emergency declared by the President of the United States or the person performing his functions, BCU's President, Executive Vice President, Senior Vice President, or in the absence of all the above, their successors will implement the Business Continuity Plan or portions thereof needed to conduct the affairs of the corporation, under such guidance from the directors as may be available except as to matters which by statute require specific approval of the Board of Directors and subject to conformance with any government directives during the emergency.

BYLAWS TO PROVIDE FOR EMERGENCY OPERATIONS THROUGH EXECUTIVE COMMITTEE ACTION

OFFICERS PRO TEMPORE AND DISASTER

The Board of Directors shall have the power, in the absence or disability of any officer, or upon the refusal of any officer to act, to delegate and prescribe such officer's powers and duties to any other officer, or to any director, for the time being.

In the event of a state of disaster of sufficient severity to prevent the conduct and management of the affairs and business of this corporation by its directors and officers as contemplated by these Bylaws, any two available shall constitute a quorum for the full conduct and management of the affairs and business of the corporation in accordance with the provisions of the Bylaws. In the event of the unavailability, at such time, of a minimum of two members of the board, shall have full conduct and management of the affairs and business of the corporation in accordance with the foregoing provisions of this section.

This Bylaw shall be subject to implementation by resolutions of the Board of Directors passed from time to time for that purpose, and any provisions of these Bylaws (other than this section) and any resolutions which are contrary to the provisions of this section or to be the provisions of any such implemented resolutions shall be suspended until it shall be determined by any interim director(s) acting under this section that it shall be to the advantage of this corporation to resume the conduct and management of its affairs and business under all the other provisions of these Bylaws.

RESOLUTION TO PROVIDE OFFICER SUCCESSION

BE IT RESOLVED, that if consequent upon war or warlike damage or disaster, the president of these normal executive duties, then the authority and duties of the president shall, without further action of the Board of Directors, be automatically assumed by the following individuals:

1. CFO
2. COO
3. EVP HR
4. CISO

Any one of the persons mentioned who in accordance with this resolution assumes the authority and duties of the president, shall continue to serve until he/she resigns or until the elected president of this corporation, or a person higher on the above list, shall become available to perform the duties of president of the corporation.

BE IT FURTHER RESOLVED that anyone dealing with this corporation may accept a certification by either of the officers above that a specified individual is acting as president in accordance with this resolution; and that anyone accepting such certification may continue to consider it in signatures of two officers of the corporation.

A minimum of five directors shall constitute a quorum for the transaction of business at all meetings of the Board of Directors. Any vacancy in the Board of Directors may be filled by the majority of the remaining Directors, though less than a quorum, or by a sole remaining Director. In the event of no surviving Directors, then Company Executive Management or employee of the corporation will contact a director of BCU who shall immediately appoint the new Directors.

TALENT SUCCESSION:

In the event sufficient employees are disabled so that it becomes impossible to manage daily activities, and sufficient replacements cannot be recruited from elsewhere, the Chief Human Resources Officer shall secure a sufficient number of talents from elsewhere to manage the daily activities of the corporation.

Additional staff succession planning is documented in BCU's HRIS platform.

APPENDIX F, PROCESSING STATUS

The Data Center's daily schedule is managed by BCU's OpCon environment. This environment is along with its dependent systems, such as the SFTP environment, have four-hour recovery times with a recovery point of 15 minutes.

SEE Applications and Servers by RTO and RPO 2021-22 for daily schedules.

Applications and Servers by RTO and R

APPENDIX G, EMPLOYEE LISTINGS

BCU utilizes a third-party hosted mass communication tool that allows for mass outbound communication using the following methodologies:

- Email
- SMS messages
- Phone message delivery
- Message via the Preparis mobile app

The tool also for the creation of custom call groups allowing for a mass communication to all employees, or a subset thereof. While the communication tool is used outside of business disruptions, emergencies, and disasters, in a disaster, this would BCU's primary method of communicating to employees.

For convenience and expediency, the following chart contains contact information for BCU's senior management team.

EXHIBIT G-1, SENIOR MANAGEMENT ADDRESS/PHONE LIST

Name	Title	Mobile
Anita Wilson-Wellen	BCU VP, Talent Management	630-400-1567
Bhavana Guglani	SVP, Chief Digital Officer	408.667.8050
Brett Engel	Treasurer, VP Finance & Risk	630-217-4849
C. J. Presto	BCU SVP / CFO	773-895-4555
Chuck Smith	BCU VP, Controller (Accounting)	847-431-0751
Dan Cook	BCU VP, US Retail Branches	651-249-5826
Dan Parsons	BCU VP, US & PR Branches	847-417-8518
Dave Blum	BCU SVP, Corp Relations/US Service Ctrs (Admin)	815-861-7566
Davi Allen	BCU VP, Consumer Lending (Collections)	847-668-9220
David Brydun	BCU SVP, CLO (Loan Sales)	847-508-1599
Doug Wright	BCU VP, Audit/Compliance (Auditing)	847-204-9694
Jill Sammons	BCU VP, Marketing & Communications	630-212-9554
Jim Block	BCU EVP & COO (Admin)	847-875-6738
Joe McCarthy	BCU VP, Real Estate Lending	602-769-1842
John Sahagian	BCU VP, Chief Data Officer (Admin)	847-380-9183
Keith Parris	BCU VP, Contact Center Ops & Technology	630 870 2922
Kerriann Mills	BCU VP, General Counsel (Legal)	954-732-2338
Lisa Baron	BCU EVP & CHRO (Admin)	847-977-6464
Maggie Garcia	BCU VP, Deposit Products (Member Operations)	773-263-7513
Mike Valentine	BCU President & CEO (Admin)	847-507-9455
Scott Zulpo	BCU SVP / CTO	847-527-7302
Stephenie Southard	BCU VP, Information Technology - Cybersecurity (CISO)	224-360-4058

EXHIBIT G-2, EMPLOYEE NOTIFICATION PROCEDURE

After the Business Continuity Plan has been activated, use this procedure to alert employees. MAKE COPIES OF THIS PROCEDURE, AS NECESSARY. Based on availability of Calling Tree Representatives, this procedure may be delegated to the Human Resources Team or divided among team members.

Place call – Say "MAY I SPEAK WITH (individual)?"

A. **If available**, provide the following information:

- Brief description of the problem:
- Location of the Command Center: _____

  _____
- Telephone number at the Command Center: _____
- Immediate action requirements. (Report to the Command Center – or – stand by).
- ACTION REQUIRED: _____

  _____

B. **If not available**, - say "WHERE MAY I REACH (individual)?"

- **If at any location other than work**, get the number, make the call, and provide the above information.
- **If the individual is at work**, indicate you will reach the individual at work. (DO NOT DISCUSS THE SITUATION WITH THE PERSON ANSWERING THE PHONE).
- Record the information on the calling tree list and notify the Management Team as soon as possible.

IMPORTANT NOTICE: BY FOLLOWING THE ABOVE INSTRUCTIONS, YOU WILL NOT ALARM MEMBERS OF THE EMPLOYEE'S FAMILY UNNECCESSARILY. DO NOT DISCUSS THE SITUATION WITH MEMBERS OF THE FAMILY.

EXHIBIT G-3, EMPLOYEE CALLING TREE

BCU Employee Calling Tree Process

Department VPs are required to retain their own call tree records. In an emergency BCU will utilize Agility's
Preparis SMS and phone notification system. This process is owned by the BCP Committee and SVP of Marketing. The staff phone number database is pulled from the HR records and updated to Preparis weekly.

W:\Managers Only\Manager Contacts\May 2022 contact list.xlsx

APPENDIX I, RECOVERY WORKSHEETS AND FORMS

EXHIBIT I-1, ALTERNATE SITE CONTRACT(S)

Contract Recovery/Alternate Site Details	Description
Site Name	
Address	

Telephone	
Contact Person	
Contract Duration	
Contract Renewal Notification	
Renegotiation Circumstances	
Emergency Circumstance Authorization	
Priorities/Penalties	
Time Requirement	
Testing	
Costs	
Resources	
Impending Changes	
Security Considerations	
Operation Conditions Under Disaster and Testing: o **Hours of Operations:** o **Employee availability:** o **Process to Negotiate Extension of Service**	
Proprietary Information	
Termination Conditions	
Hardware Configuration	
Guarantee of Compatibility	
Availability	
Support Requirements	
Facility Requirements	
Software Environment of Backup Site	
Coordinating Backup Services	
Basis for Backup Consideration o **Fixed Fees:** o **Usage Fee:** o **Mutual Backup Agreement:** o **Some Combination:**	
Backup-Specific Hardware Required	
Backup-Specific Hardware Rental Arrangements	

Backup Site Manpower Support Expected	
Non-Mainframe Resource Equipment	
Backup Testing Process	
Other	

*** All written agreement(s)/contract(s) should be attached to this form.**

EXHIBIT I-2, DEPARTMENTAL RECOVERY WORKSHEET

Department: ____________________

High Priority Tasks	Frequency	Staff	Forms/Equipment	Supplies

EXHIBIT I-3, DISASTER ASSESSMENT REPORT

Rapid Assessment Form

Item	Description
Location	
Date/Time Reported	
Name of Person Placing Initial Alert	
Arrival at Disaster Site	
General Description of Disaster	
External Support Requirements o Fire o Police o Security Guards o Staffing Agency	
Category	**Damage Level (1-3 Minor-Extensive)**
Property damage Assessment o Parking o Grounds	
Structure Damage Assessment o Access - Doors - Windows o Floors - Drainage - Water lines o Ceilings o Walls	
o Access - Doors -Windows	
o Floors - Drainage -Water lines	
o Ceilings	
o Walls	
o Roof	
Utilities/Services	

o Electrical	
o Lighting	
o Heating	
o Cooling	
o Telephones	
o Communications	
o Plumbing	
o Water Supply	
o Fire Protection	
o Security System	
o Elevators	
o UPS System (Batteries & Equipment)	
Hardware	
o Main computer	
o [Other] terminals	
o Microcomputers	
o Printers	
o Data Communication Equipment	
o Modems	
o MICR equipment	
o Other	
Software	
Documentation	
Team Members	

EXHIBIT I-11, INVENTORY LIST

Company procurement will coordinate the request for supplies, furniture, and equipment for all departments displaced by physical damage to their work areas. Purchasing will be in ongoing communication with the Facilities Team to determine changes in purchase quantities for furniture and equipment.

All purchase requests will be delivered to purchasing as soon as possible. General office supplies should be ordered within 12 hours if a disaster has been declared.

Item Description	Quantity	Location/Department
Office chairs	20	Main office
3x8 folding tables	10	Main office
Notebook computers	10	Main Office
Printers	2	Main Office
Copiers with Sorter (50 PPM)	1	Main office
Fax machines	1	Main office
Laser printers	2	Main office
Cases of 8.5x11 white paper	2	Main office
General office supplies for workstations	15 sets	Main office
Typewriters	2	
Calculators	4	

PC, telephone, other specific equipment, and furniture will be based on approved purchase orders.

EXHIBIT I-12, PLAN DISTRIBUTION REGISTER

To be completed and retained by the Business Continuity Coordinator whenever the Business Continuity Plan is updated and redistributed.

Date _____

Copy #	Distributed by	Signature	Distributed to*	Signature

* "Distributed to" may be a location, i.e., offsite storage, in which case the Business Continuity Coordinator should sign to verify the distribution.

APPENDIX K, BUSINESS IMPACT ANALYSIS AND RISK ASSESSMENT

Overview

BCU management has recognized the potential risk of financial and operational losses associated with a disruption.

The purpose of this overview is to identify and document the potential impact that would occur as a result of the business disruption scenarios. These disruption events may have a significant effect on the business operations of BCU.

The scope of this analysis is focused on failure issues encompassing five failure events. The failure events are as follows:

- Power Failure
- Computer Systems Failure
- Telecommunications systems failure
- Main Office not accessible
- BCU or CP Office(s) are not accessible

Other potential business failure events or effects are possible, however, management estimates that these will have an immaterial operational or financial impact, if any, on business and thus are beyond the scope of this analysis.

Assumptions and Definitions

Attached is a risk assessment of the potential threat factors to BCU and correlation to each respective broad failure event defined above. These threat factors were objectively and subjectively reviewed and were assigned common threat factor characteristics applicable to determining their operational and financial impact to the organization upon occurrence. These threat factors were as follows:

- Likelihood of occurrence
- Impact of the disruption

All other potential threat factors do not present within this risk assessment were considered insignificant, i.e., their pertinence to each failure event was determined to be insignificant to the results of this analysis.

Unquantifiable & Hypothetical Failure Events

Many failure events encompass variables which are much too volatile or unknown to be given consideration in any form or computation within the scope of this analysis (i.e., negative publicity, failures by third-party providers and their inability to perform as agreed, etc.). Due to the unquantifiable nature of certain events, it becomes management's responsibility to interpret and take action on matters they consider material.

Business Impact Analysis Results

Based upon the results of the risk assessment summary in this section and the results of our subjective analysis, we have determined that the following financial statement impact would most – likely occur as a direct result of each of the following failure events:

- Main Office not accessible – Expected costs cannot reasonably be estimated due to the nature of this failure event. The organization does maintain property and casualty insurance for such an event, which is reviewed for adequacy in relation to market values on an annual basis. Management believes that the insurance coverage would cover substantially all expected costs associated with the lack of accessibility of the Main Office location and that all related deductibles would be considered insignificant to the operations of BCU.
- Office(s) not accessible – Expected costs cannot reasonably be estimated due to the nature of this failure event. The organization does maintain property and casualty insurance for such an event, which is reviewed for adequacy in relation to market values on an annual basis. Management believes that the insurance coverage would cover substantially all expected costs associated with the lack of accessibility of the office location(s) and that all related deductibles would be considered insignificant to the operations of BCU. Management also believes that the financial and operational impact of this failure event can largely be mitigated by transacting customer business at the main office location within the organization or by the use of a temporary facility.

Suggestions for Interpretation of this Overview

The results of this analysis have been derived from a current objective and subjective evaluation process of both financial and operational factors directly relating to these failure events identified (Main Office not accessible and Office(s) not accessible.) The intentions for readers of this analysis are to provide a reasonable estimate of the overall business impact to the organization in the event that one of these failure events occurs. Regardless of this analysis, reasonable and prudent business decisions must be made considering both financial and operational aspects should one of these failure events occur to minimize the financial and operational impact of occurrence.

Risk Assessment Process

One of the first steps in preparing a business continuity plan is to identify the areas of high exposure to BCU. To accomplish this, employees with facilities and management responsibility and knowledge participated in a risk assessment process.

For the purpose of survival of BCU and its employees, it is vitally important BCU recognize these threats that have the potential to result in a disaster and thereby affect the ability of BCU to conduct business.

During the risk assessment process, the relative probability of occurrence of each threat was estimated. The threats were categorized into three broad categories: Man-made threats, natural threats, and technological threats.

Man-made Threats

Man-made threats are just those, threats that are made by humans. Man made threats comprise those situations/events, which are caused with intentional harm or injury to employees, disruption of services, or destruction of property.

Natural Threats

Natural threats, to put it simply, occur in nature. Natural threats comprise those situations/events, which occur in nature with no assistance from humans. While natural threats are predictable within certain limits using technology, they continue to dictate the geographic locations in which business operates, and where and how facilities are constructed.

Technological Threats

Technological threats include items such as chemical releases, radioactive contamination, transportation accidents or the failure of technology in general. This category involves man-made mechanisms or systems that, when not properly controlled or functioning, have a negative impact on the surrounding environment. Technological disasters may be started intentionally, by accident, or as a result of some natural event.

The risk assessment/business impact analysis considers:

- The source of the disruption.
- The type of disruption.
- The probability of its occurrence.
- Its initial impact on the organization.
- It potential for expanding in severity over time and the associated impacts.
- The estimated length of time the business may be disrupted.

Rather than attempting to determine exact probabilities of each potential threat, a qualitative rating system was used to identify threats with the highest probability according to the one to five scale defined in the table below.

Likelihood	Description
Rare (1)	The threat event rarely occurs and may require specific combinations of conditions in order to occur.
Unlikely (2)	The threat event is unlikely to occur, even under normal circumstances.
Moderate (3)	The event has an average probability of occurrence under normal circumstances
Likely (4)	Under normal circumstances it is likely that threat will materialize.
Almost Certain (5)	There is a near 100 percent chance that the threat will materialize at some point in BCU's operation.

The risk assessment was also used to determine the impact of each type of potential threat on BCU employees, building and functions if the particular threat occurred. The impact levels from 1 to 5 are:

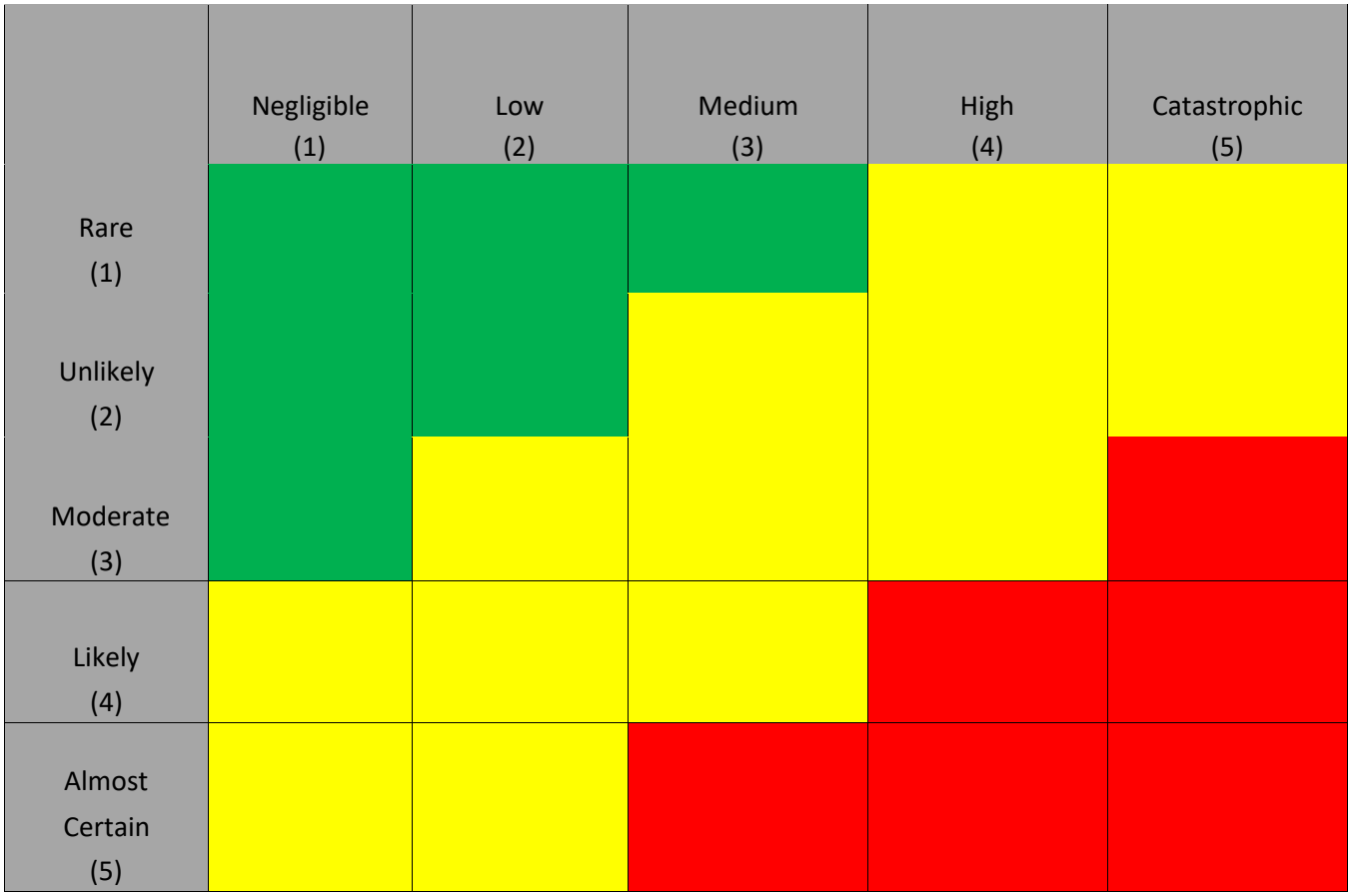
Impact	Description
Negligible (1)	The occurrence of the event will have minimal impact on the reputation or finances of BCU.
Low (2)	The occurrence of the event will cause a small but measurable impact to either the reputation or finances of BCU.

Medium (3)	The occurrence of the event will have a significant impact on the reputation or finances of BCU and mitigations should be considered.
High (4)	The occurrence of this event will have a major impact on the reputation and/or finances of BCU and mitigations are needed in order to minimize this impact.
Catastrophic (5)	If this event occurs and no mitigations are in place to reduce the impact BCU is likely to cease operations.

Inherent Risk

The inherent risk associated with each threat is determined by multiplying the likelihood that a threat will occur by the impact to the organization if it does. If the assessed level of risk for a particular threat is outside BCU's risk tolerance, risk management strategies can be put in place to reduce either the likelihood the threat will materialize or the impact to BCU if it does.

The Risk Map below can be used as a guideline for determining where the risk from each threat falls in the risk model as a guideline for understanding if or how mitigations can be implemented. Risk can never be completely eliminated and in some cases, the cost of mitigating the risk may outweigh the financial impact to BCU should the risk occur.



Risk Assessment

Due to the table size, BCU's risk assessment is linked below. There is also a screen shot of the table to demonstrate the fields and data within the table:

BCP Risk Assess

BCU Business Resiliency Threat Assessment

Last updated: 2021

Threat	Likelihood (1-5)	Impact (1-5)	Risk	Mitigations for Likelihood	Likely % Eff	Migitation for Impact	Impact % Eff	Residual Risk
Pandemic	5	5	25	Placement of gloves, masks, increased cleaning. During a pandemic no team events, meetings in conference rooms, staying 6 feet apart and other restrictions as mandated by State of IL and recommendations by CDC.	25%	Implementation of vitual desktop environment. Enhancement of BCU's internet bandwidth and redudancy, updating of related security practices, virtualization of meetings, creation of senior management work from home team.	60%	4
Improper Handling of Data	2	4	8	Implementation of and annual training on handling of member data.	30%	Implementation of dedicated drives and permissioned folders.	45%	2
Explosion	1	5	5	N/A		N/A		5
Bomb	1	5	5	N/A		N/A		5
Nuclear Fallout	1	5	5	N/A		N/A		5
Biological Incident	1	4	4	N/A		N/A		4

APPENDIX L: NETWORK DIAGRAMS AND EQUIPMENT INVENTORIES

Network Diagrams and Network Inventories are maintained in document repositories managed by the IT Department.

APPENDIX M: BUSINESS IMPACT ANALYSIS

BCU

Business functions and processes are identified by BCU and have been analyzed. For each function, the business process owner and subject matter experts assessed the criticality of the function to the survival of the business, any risks which may affect the function, and what the overall impact to the business would be for an interruption to the process. These factors determined the Return to Operation (RTO) and Recovery Point Objective (RPO).

Criticality

Criticality measures the effect a loss of the function or process would have on the business it was not returned to operation within the RTO time frame. The assessment uses a qualitative scale from nonessential to catastrophic. The definitions for each value are below.

Criticality	Description	Recovery Time
Non-essential	This function or process is not essential to the success of the business. It may be provided as a convenience for customers or employees or may be an efficiency enhancing function. Without this function or process the business would survive but might be impaired.	30 Days
Normal	The business relies on this function or process to accomplish routine tasks related to the successful delivery of service to customers or other parts of the business. Some workarounds are available, and the business can cope with an interruption in this process for up to one week.	7 Days

Important	This function is important to the continued and smooth operation of the business. Interruptions to this function may disrupt other functions or there may be unacceptable consequences to working around it. If this process is not restored within 72 hours irreparable damage to the business will occur.	72 Hours
Urgent	The business cannot function effectively during interruptions to this process. Workarounds are too cumbersome to be effective and other processes are significantly affected by the loss of this one. Interruptions of longer than one day may cause irreparable damage to the business.	24 Hours
Mission Critical	Those services/processes that are critical to: • Money movement for members and BCU cash management • Employee network access • Infrastructure to support both	< 8 Hours

Business Functions			Impact to Business			Recovery Expectations	
Business Function	**Business Owner**	**Technology Custodian**	**Criticality Rank**	**Projected Loss (VH, H, M, L)**	**Maximum Tolerable Downtime (MTD)**	**Recovery Time Objective (RTO) in Hours**	**Recovery Point Objective (RPO) in Hours**

APPENDIX N: PANDEMIC PREPAREDNESS AND RESPONSE PLAN

Introduction

BCU has an obligation to protect and secure its assets and to provide a safe and secure environment. The organization has a business recovery policy as approved by its Board of Directors and has an established business recovery plan to guide its response to various potential business interruptions.

Federal agencies have issued risk alerts to the potential development of worldwide human health-related conditions that could create a range of impacts on the normal conduct of business within the United States. These circumstances are classified as a "pandemic." In an effort to plan for and be prepared to respond to such a circumstance, the organization has developed this Pandemic Response Plan (PRP) as a component of its Business Continuity Plan.

A pandemic is described as an epidemic occurring over a wide area that crosses international boundaries and usually affects a large number of people. Simply stated, it is a global outbreak of a disease. An epidemic is a widespread breakout of a disease in a single community or area. The purpose of the organization's response planning is focused on a pandemic situation. The best-case scenario would be advance notice that a pandemic has been declared in order to prepare. However, a pandemic could arrive before officials have even raised an alert. As such, it is essential that we have a response plan in place that acts to protect all individuals involved in the operation and use of the organization and safeguards organization assets.

Assumptions

During a pandemic, the Credit Union will remain focused on its key commitments:

- Operating to maintain member stability.
- Promoting the maintenance of a sound and efficient financial system; and
- Meeting the currency needs of our members.

This pandemic response plan includes basic assumptions related to the general operations of the organization for the safety and security of our employees and members. The primary assumption is that the organization is able to provide a safe workplace for our employees to work in and our members to conduct their financial business. Specifically for this pandemic response plan, it is assumed that BCU has available to it clean water, waste disposal systems, electrical power, gas power, operational HVAC systems and security systems. If these basic operational assumptions are not met and a safe work environment is not available for our employees and members, it may not be feasible to operate any or all of our locations and/or our corporate headquarters to serve our members.

Pandemic Alert Systems

BCU Management can monitor the following alert systems to obtain information regarding the threat and progression of a pandemic event:

http://www.who.int/csr/disease/avian_influenza/phase/en/index.html http://www.cdc.gov/flu/
http://www.flu.gov/planning-preparedness/federal/index.html#
http://www.pandemicalertlevel.com/ http://www.flupandemicalert.com/
http://www.hhs.gov/pandemicflu/plan/appendixc.html http://www.ncua.gov

Pandemic Response

The Command Team will coordination and implementation of this Pandemic Response Plan as described herein. The Command Team has the authority to create a Pandemic Response Team to coordinate and implement the appropriate response.

Activation

Upon communication that a pandemic is arriving/has arrived in the United States we will begin monitoring the national situation. If the basic assumptions are met, the pandemic response plan will be activated immediately after it comes to the attention of the Pandemic Response Coordinator that there is an imminent threat of a pandemic situation affecting BCU within its geographic field of membership.

Upon activation of the PRP, the Command Team will meet early every morning and the BCP Plan Administrator, Technology BCP Coordinator, Administration BCP Coordinate, and the Operations BCP Coordinator will meet late every afternoon to determine critical function capabilities and expected staffing levels in order to effectively serve members. These meetings may determine which Locations and functions will be available for member service, on a daily basis. As a result of these meetings, communication will be provided to the general management team on decisions and recommendations made. These meetings will continue each day until the Command Team feels that the pandemic impact is well controlled.

Employee Safety

Underlying this strategy is a determination that the safety of staff is a key objective.

At the discretion of Command Team, and based upon best available information concerning pandemic influenza health risks, the following actions may be taken:

- All employees will be encouraged to wash their hands and use hand sanitizers frequently.
- Social distancing will be encouraged with the goal of maintaining a minimum distance of six feet between employees at all times, if possible.
- Employees will be encouraged to cover their nose and mouth with a tissue or handkerchief when coughing or sneezing.
- Shaking hands will be discouraged.
- Sharing food within BCU facilities prohibited.
- Eating lunch at restaurants and other unnecessary trips outside the office will be discouraged. Employees will be expected to bring their own lunches and wash any utensils and containers at home.
- Enforce work-at-home requirements as either required by federal or state authorities as well as to limit the exposure of employees to pandemic illness.
- BCU Management will encourage and, if possible, facilitate immunization of all employees with the annual influenza vaccine and pneumonia vaccine.
- Other activities identified and deemed necessary by the Command Team.
- All employees will be prohibited from coming to work while ill, or while members of their household experience pandemic related symptoms. If an employee begins to run a fever or feel ill while at work, they will be required to go home immediately and not return until all symptoms have disappeared.

- Current cleaning contracts will be reviewed and updated appropriately to incorporate rigorous disinfection of common areas during daily cleaning as deemed necessary by the Facilities BCP Coordinator.

Assignment of Individual Access

When access to BCU or CP facilities is restricted due to a pandemic, all individuals will be assigned a priority level which will be used to prioritize equipment and back-up activities that must be planned for. All department managers will identify their associates per the following categories:

1. Critical – the individual's access or assigned tasks are critical to daily functions or the processing of member's credit union business.

2. Nice to Have – individuals that do not have critical access or assigned tasks, but their availability or contributions are important to BCU's daily functions or the processing of member's credit union business.

3. Others - individuals that do not have critical access or assigned tasks and their availability or contributions are not important to BCU's daily functions or the processing of member's credit union business.

Skills Inventory

Perform skills inventory to identify employees' skills in other areas of the organization for redeployment in case of a staffing emergency in a critical location/area.

Travel

During a pandemic, travel restrictions may be enforced by the federal or state government as well as BCU.

Communication

The Marketing Department, in conjunction with the Command Team, is responsible for internal and external communication. In accordance with the *Communications Protocol*, all other employees should be instructed not to give statements to the media.

Topics of communication can include but are not limited to:

- Employee well being
- Company Partners support
- Benefit information
- Links to government, Company Partners
- HR Guidance for Managers
- Personal Pandemic Planning

Example of BCU's communication efforts to the COVID pandemic can be found here: COVID-19 Employee Resources (sharepoint.com)

Supplies

BCU will purchase and maintain a stock of health protection supplies (as enumerated below) to be utilized by employees, and members in open branches, in the event of a pandemic. The decision concerning the type and number of supplies to be purchased, and when they should be utilized, shall be made by the Command Team based upon the best available information concerning health risks posed by a pandemic.

The following items may be purchased at the discretion of the CEO for pandemic preparedness (quantity of supplies will be based on size of office):

- Liquid Hand Sanitizers
- Tissues
- Computer keyboard/mouse (to be sanitized frequently with chlorine solution)
- Bottled Water
- First aid kits
- Face/eye guards
- Medical gloves (non-latex)
- Sanitizer wipe/spray
- Facial masks
- Biohazard waste bags

Event Matrix

See the threat levels and responses detailed below. Additional decisions for Pandemic events or crises that are centric to lack of human resources / staffing will be performed by the Command Team. This assessment will be performed during the onset or immediately after the event, depending on the threat source.

To combat this possibility of a pandemic disaster BCU has developed the following strategy and a series of color-coded response stages.

Stage One: Plan for It (color code WHITE) with the objective of creating pandemic response action plans to reduce the health, social and economic impact of a pandemic.

Stage Two: Act and React (color code YELLOW) once a pandemic was declared, ongoing strategies would include:

Stage Three: Keep it Out (color code RED)

Stage Four: Stamp it Out (color code RED) if these strategies were not successful, the next strategy would be:

Stage Five: Manage It (color code RED)

Stage Six: Stand down – Recovery (color code GREEN)

EXECUTIVE DECISION MATRIX: PANDEMIC SCENARIOS

The following matrix would be used to determine the status of a pandemic and the subsequent actions required.

Stage	Code	Description	Action
1	**WHITE** (Information /Advisory) Planning	• No current outbreak of the ' pandemic' anywhere in the world • Preparedness planning and preparation under way	• Complete planning and preparation • Maintain preparedness focus • Monitor national and international pandemic situation • Monitor Travel Advisory • Business as usual
2	**YELLOW** (Standby)	• No current outbreak of the ' pandemic' anywhere in the USA • Preparedness complete	• Maintain preparedness focus • Monitor national and international pandemic situation • Monitor Travel Advisory • Business as usual
3	**RED** (Activation) (Keep it out)	• Pandemic strain now human-to human • Contagious, with some employees possibly being infected • Isolated and contained incidents of contamination, or • Pandemic officially declared • No vaccine available	• Maintain preparedness focus • Ensure relevant departments can quickly move to next stage • Communicate to staff about preparedness and plans • Communicate to staff about personal preparedness • Action Containment Plans • Allow employees to work from home if they are part of the remote workforce • Revoke travel to affected regions for work purposes • Review all other travel with possible blanket revocation • Review all pandemic plans • Monitor national and international pandemic situation • Business as usual

		Scenario Based Actions 1. Credit Union employees out of town at time of outbreak, borders not closed a. Operate credit union with only essential employees taking precautions to mitigate exposure to disease b. Delegate authority as required 2. Credit Union employees out of town at time of outbreak, borders closed a. Ensure affected employees have access to cash (credit card) b. Delegate authority as required 3. Rush on cash detected a. Arrange for extra cash deliveries b. Invoke overdraft and liquidity management plans

Stage	Code	Description	Action
4	(Stamp it out)	• Pandemic officially declared in the United States • No vaccine available	• Action Status-Red Plans as per scenarios below • Monitor national and international pandemic situation • Action against rush on cash as above • Delegate authority as required
		Scenario Based Actions 1. Pandemic not in the area, movement not restricted a. Invoke 'go home stay home' policy for staff arriving at work unwell b. Revoke all travel by Credit Union employees for work purposes c. Communicate to staff about personal preparedness d. Review plan with staff e. Business as usual 2. Pandemic in the area, movement not restricted, schools etc. remain open a. Invoke 'go home stay home' policy for staff arriving at work unwell b. Revoke all travel by Credit Union employees for work purposes c. Communicate to staff about personal preparedness d. Review plan with staff e. Business as usual 3. Government closes schools but national quarantine not invoked a. 1 and 2 above, plus b. Utilize BCU policy regarding leave to care for family c. Utilize 'working from home' plan with business activity restricted to essential services 4. Government orders national quarantine of workforce a. All Action-Red plans fully operational b. Declare Status Red – Stage 4	
Stage	**Code**	**Description**	**Action**

5	(Manage it)	• Influenza pandemic officially declared • Workforce / population quarantined • Business Activity restricted to essential services only	• Monitor national and international pandemic situation • Review activity based on scenarios below
		Scenario Based Actions 1. All resources available, all key available employees a. Continue with Status Red-Stage 4 activity b. Monitor and review business activities c. Media releases/notifications as appropriate . All resources available, key employee options becoming restricted a. Review business activities and revise b. Delegate authorities as required c. Media releases/notifications as appropriate	
		3. Some resource failures occurring, key employee numbers variable a. Review business activities and revise b. Delegate authorities as required c. Media releases/notifications as appropriate	
6	**GREEN** (Stand down) (Recovery)	• Population protected by vaccination • Pandemic officially declared over in Metropolitan area • Business recovery required	• Monitor national and international pandemic situation • Delegate authority as required • Invoke Business Recovery Plans