



BUSINESS CONTINUITY PLAN

Version: CUNWBBCP-v20170207-PUB

**Portions of this document have been omitted and tagged as [CONFIDENTIAL] for distribution.*

Confidentiality Statement: *This document contains sensitive information regarding the operations of CU*NorthWest and the CU*Asterisk partner network. It may not be distributed without the consent of the CU*NorthWest Executive Team.*

Plan Contents

- Introduction4
- Scope and objectives.....4
- Confidentiality Statement4
- Assumptions.....4
- Plan Maintenance5
- Awareness and Training5
- Testing and Exercising5
- Executive Commitment6
- Corporate Environment.....7
 - Operational overview.....7
 - Current Operational Environment8
 - Greenstone Suite (Corporate Office)10
 - Site-Four13
 - CU*Answers15
 - Xtend17
 - eDOC Innovations.....17
 - CU*Answers Imaging Solutions.....17
- Recovery at a Glance18
 - Recovery Timeline19
 - Roles and Responsibilities21
- Emergency Response Plan26
 - Emergency Response Team26
 - Emergency Responders.....27
 - Establishing Command and Control27
 - Incident Assessment28
 - Securing Corporate Assets28
 - Systems/Applications Outage Assessment Report30
 - Declaration of Disaster31
 - Continuity Insurance31
 - Emergency Response Procedures34
 - Fire/Explosion34
 - Building Evacuation.....35
 - Severe Weather / Shelter-in-Place35
 - Flood/Water Damage36

Power Outage	37
Injury/Illness/Mass Absenteeism (Pandemic Policy)	38
Security Incident Report	43
Distributed Denial of Service Attack Response.....	43
Continuity and Recovery Strategies	44
Overview of HA strategy	44
HA Rollover Test Procedures:	45
Overview of DR strategy (in case HA is not an option)	46
Third Party Vendor Communications.....	46
Client Network	47
IT Recovery	49
Overview of IT environment	49
Loss of Data Communications	49
Loss of Telephone Service	49
Internal IT Contingency Plans (non-core-processing)	50
PC/Workstation Build Checklist	50
Business Recovery	51
Alternate Recovery Locations	52
Crisis Communications	53
Key stakeholders	53
Communicating in a crisis.....	54
Publishing CU*BASE Alerts	54
Appendix.....	55
CU*NorthWest Staff Emergency Contact Information	55
Board of Directors	55
Stockholders.....	55
Vendors and Service Providers.....	55
CUNW Voice and T1 Lines	55

LEGAL DISCLAIMER

The information contained in this report does not constitute legal advice. We make no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained in this report. You should retain and rely on your own legal counsel, and nothing herein should be considered a substitute for the advice of competent legal counsel.

These materials are intended, but not promised or guaranteed to be current, complete, or up-to-date and should in no way be taken as an indication of future results. All information is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event, will CU*NorthWest, its related partnerships or corporations, or the partners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information provided or for any consequential, special or similar damages, even if advised of the possibility of such damages.

NOTE

Data and information contained within this Plan (where applicable) has been provided by the CU*NorthWest in the form of electronic files/documentation and as the result of notes taken during conversations with key personnel. It is the responsibility of the Credit Union to maintain this Plan to ensure contents are accurate and current.

Introduction

This document is designed for the purposes of equipping and preparing CU*NorthWest and its partners for the expected impact of unplanned disruptions to business functions and processes and for contributing to the resiliency of operations.

The CU*NorthWest Business Continuity Plan is “a roadmap for continuing operations under adverse conditions (i.e. interruption from natural or man-made hazards)”. The plan is the primary tool used for preparedness training, testing and exercising. The best investment in business continuity management is a well-trained recovery team. The plan should be studied and its contents well known prior to the next disruption.

Scope and objectives

A disaster is a unique event and the provisions of this plan can be used as the basis for controlling specific recovery operations at management’s discretion. Execution of this plan will help facilitate the timely recovery of core processing critical business functions.

The core framework of this plan was developed with the following objectives:

- To protect personnel and property (assets)
- To minimize the financial losses to the organization
- To serve clients with minimal disruptions
- To mitigate the negative effects of disruptions on business operations

The procedures contained within have been designed to serve as a guide for responding to emergencies based on recognized standards and best practices, written with the FFIEC published recommendations in mind. Details about these recommendations can be found at the FFIEC website or at <http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx>.

Confidentiality Statement

This plan is strictly confidential and is not to be shared with anyone outside the CU*Asterisk network without the express permission of the President/CEO. Full copies of the current Plan are kept by each management team member. All questions from the news media or other external sources regarding the plan or any disaster/incident should be directed to the Incident Manager or CEO.

*See “Crisis Communications” section.

Assumptions

The following assumptions have been considered during the creation of this recovery plan. The specific circumstances of any disruption may require modifications to the recovery effort.

- Key personnel have been identified and trained and are available to activate the recovery plan.
- Current backups of the application software and data are intact and available at a quickly accessible storage facility.
- Service agreements are maintained with the application hardware, software and communications providers to support the emergency system recovery.

Plan Maintenance

The CU*NorthWest Business Recovery Plan will be revised every twelve months or as needed based on:

- Changes in potential threats or risks,
- Considerable changes in business operations, functions, or processes,
- Considerable changes in system or network architecture,
- Audit recommendations,
- Lessons learned from tests, exercises and events.

Revised plans will be distributed to all Emergency Response Team personnel, Board members, and staff with direct roles and responsibilities within the plan. General information about the continuity plan and program will be made available on the corporate web site and a sanitized version of the plan available to client credit unions upon request.

Revised on (Date)	Revised by:	Notes	Board Acceptance (Date)
1/28/2014	C. Green/ J. Lawrence	Initial version in the new format.	2/13/2014
10/23/2014	C. Green/ J. Lawrence	Post HA move to Kentwood, MI.	
2/18/2015	C. Green/ J. Lawrence	Role changes (Ann, Erik departure)	
2/7/2017	C. Green/ J. Lawrence	Site-Four updates, employee changes	

Awareness and Training

To ensure all personnel are knowledgeable of the Plan and aware of their roles during a recovery effort, CU*NorthWest will commit a portion of annual management and staff meetings for educating employees as part of the ongoing business continuity planning cycle. In addition, training events and exercises for those with specific roles and responsibilities will be conducted as needed, particularly when any plan modifications have been made.

Training events will be documented and reported to the board annually.

Testing and Exercising

Recovery plans (or portions thereof) are to be tested regularly to:

- Ensure completeness and accuracy of the procedures within the plan
- Identify area within the plan that are weak and require modifications to improve plan effectiveness
- Provide training and practice for recovery teams
- Demonstrate (building confidence in) our ability to recover critical functions meeting acceptable time objectives.

Types of testing include:

- **Life safety exercises**
 - Examples are building evacuation or shelter-in-place drills
- **Plan walk-through/tabletop reviews**
 - Example is a plan review/walk-through with recovery team member(s) in a conference/meeting room environment
- **Stand-alone exercises**

- Recovery/relocation of a single business unit/department, single process/function, or single device/system.
- An example would be testing VPN backup data communications to simulate an outage of the primary data communications line.
- **Comprehensive exercises**
 - A large-scale recovery effort such as rolling core-processing from the primary datacenter to the secondary datacenter.

*See “Continuity and Recovery Strategies” section for more information.

Date of Testing Event	Areas of Plan Tested	Notes about Test Event	Test Participants
3/15/2015-3/18/2015	HA Rollover from PROD to HA in Kentwood, MI	First full rollover since moving HA environment to Kentwood datacenter.	CU*NorthWest, Site-Four, CU*Answers, CU*South
11/08/2015	HA rollover and rollback same day	First rollover for new leadership team at Site-Four	CU*NorthWest, Site-Four, CU*Answers, CU*South
12/11/2016-12/14/2016	HA Rollover from PROD to HA in Kentwood, MI	First rollover with CU*Answers performing EOD operations for one shift.	CU*NorthWest, Site-Four, CU*Answers, CU*South

*Results of the HA rollover tests are published at: <http://cunorthwest.com/disaster-recovery-and-audits/>

Executive Commitment

Board and senior management responsibilities in Business Continuity Planning include:

- Establishing policy by determining how the institution will manage and control identified risks
- Allocating knowledgeable personnel and sufficient financial resources to properly implement the Business Continuity Plan
- Ensuring that the Business Continuity Plan is independently reviewed and approved at least annually
- Ensuring staff are trained and aware of their roles in the implementation of the Business Continuity Plan
- Ensuring the Business Continuity Plan is regularly tested on an enterprise-wide basis
- Reviewing the Business Continuity Plan testing program and test results on a regular basis
- Ensuring the Business Continuity Plan is continually updated to reflect the current operating environment

Corporate Environment

Operational overview

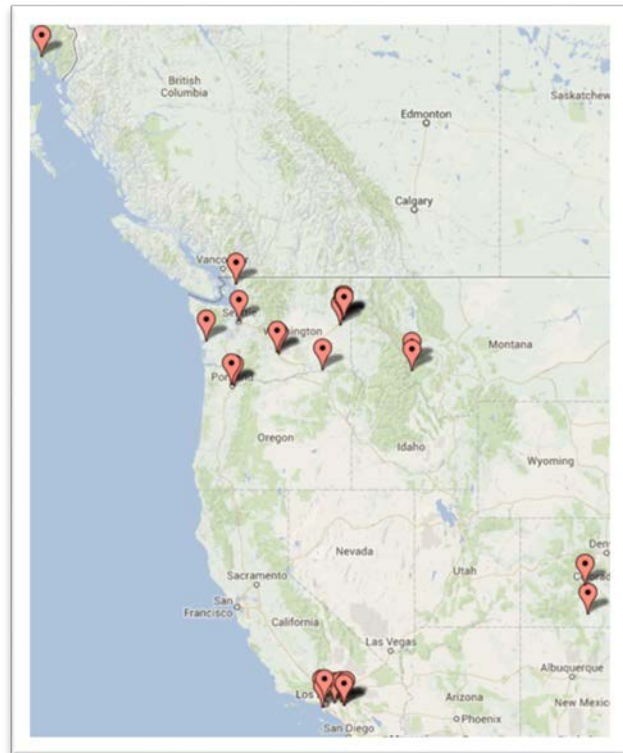
CU*NorthWest was founded in 2005 and is a 100% credit union-owned CUSO located in Liberty Lake, Washington. CU*NorthWest offers a wide variety of services for credit unions including its flagship CU*BASE/GOLD core processing system in both an online (ASP) and in-house environment, as well as Internet development services featuring the It's Me 247 online banking product. Additional services include web site development, network design and security, bookkeeping services, and a complete e-Document solution. CU*NorthWest provides expertise in implementing technical solutions to operational needs, and helps credit unions form strategic alliances and partnerships.



CU*NorthWest is a strategic partner in the CU*Asterisk network that includes CU*Answers, CU*South, Site-Four, Lender*VP, eDOC Innovations, and Xtend. Each of these partners provides products and services that complement the core-processing CU*BASE/GOLD platform.

CU*NorthWest employs 31 staff members and serves 32 client credit unions located in the following states:

- Washington
- Oregon
- California
- Colorado
- Montana, and
- Alaska



CU*NorthWest is an active member of the CU*Asterisk network.



Current Operational Environment

The systems and components required to provide products and services to the client-base are spread among multiple, geographically dispersed CU*Asterisk partner locations as shown below.



CU*NorthWest currently maintains a contract with Site-Four to provide systems and networks for production and high-availability (HA) CU*BASE/GOLD core-processing services including third party EFT communications. The primary production host is located at the Site-Four datacenter in Yankton, SD. The secondary HA host is currently located at the CU*Answers production datacenter in Kentwood, MI. Site-Four owns and maintains all equipment required for core-processing at these two locations.

Additional products and services to complement CU*BASE/GOLD are provided by CU*Answers, Xtend, and eDOC Innovations. Systems and networks used to provide products and services for Xtend and eDOC Innovations are hosted within the CU*Answers datacenters, located in west Michigan.

For the purpose of this recovery plan we identify dependencies and alternate strategies for the recovery of:

1. CU*BASE/GOLD (core-processing)
2. Customer Support / Client Services (critical business functions)
3. Extended products / services that complement core-processing
4. Back-office and internal operations



The table that follows identifies key products and services provided by each CU*Asterisk partner.

Key products/services and business functions by CU*Asterisk Partner include:

CU*NorthWest	CU*Answers
<p>Departments/Functions</p> <ul style="list-style-type: none"> • Client Support • Technical Support • Sales/Marketing • Finance • Human Resources/Payroll • Programming • Conversions <p>Systems/Applications</p> <ul style="list-style-type: none"> • Secondary Production System (CU*BASE) <ul style="list-style-type: none"> ○ Managed by Site-Four • Secondary Third Party EFT Data Communications <ul style="list-style-type: none"> ○ Managed by Site-Four • Secondary Operations Support • File/Print Services • CU*BASE Development/QC • QuickBooks • SGMS Firewalls 	<p>Departments/Functions</p> <ul style="list-style-type: none"> • After Hours Client Support • Technical Support <p>Systems/Applications</p> <ul style="list-style-type: none"> • It's Me 247 • CU*Talk • CU*Spy • CU*Checks/Check 21 • AnswerBook • ExaVault • VoIP Phones/Fax • Email (MS-Exchange) • Lync • Great Plains/Dynamics • LPI, Latitude, SGMS, Nagios, Gmanage • Active Directory/Domain Svcs. • DataBP • Passageways (portal) • Corporate Web Site • Indirect Lending • PLM
Site-Four	Xtend
<p>Departments/Functions</p> <ul style="list-style-type: none"> • Primary Operations Support <p>Systems/Applications</p> <ul style="list-style-type: none"> • Primary Production System (CU*BASE) • Primary Third Party EFT Data Communications 	<p>Departments/Functions</p> <ul style="list-style-type: none"> • SRS Bookkeeping • Member Reach • Call Center Services • AuditLink • Shared Branching
eDOC	
<p>Departments/Functions</p> <ul style="list-style-type: none"> • eDOC application support and installation <p>Systems/Applications</p> <ul style="list-style-type: none"> • iDOCVault • ProDoc2020 	

Greenstone Suite (Corporate Office)

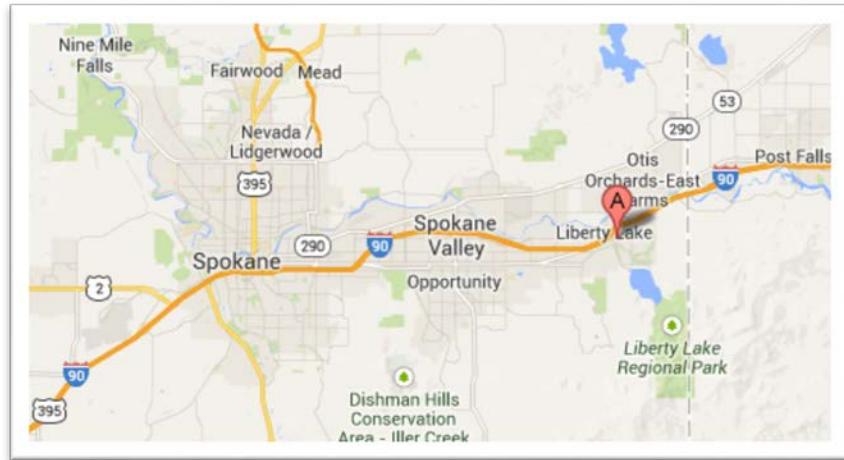
The Greenstone office functions as the corporate headquarters for CU*NorthWest, housing all internal staff.

[A]

CU*Northwest HQ

1421 North Meadowwood Lane
Suite 130
Liberty Lake, WA 99019
866-922-7646

- Corporate Office
- Client Services
- Technical Support
- Administration
- Sales/Marketing
- Conversions
- Etc.



To enable staff to perform critical business functions that support the products and services delivered to client credit unions, workspace and IT equipment are provided including:

- PC/Workstations
- VoIP Phones
- Printers
- File/Print servers
- Etc.

Systems and network devices at the Greenstone Office are monitored 24x7 by CU*Answers Network Services.

*See "IT Recovery" section for procedures to recover IT equipment at the Greenstone Office location.

UPS units are installed in the server room to maintain power to critical LAN components (FW, router, switch, file/print servers, OPS console, etc.) for short-term power outages. UPS has the capacity to power critical network devices for up to 4-6 hours. There is no generator currently in place at the Greenstone Office location.

*See "Emergency Response Procedures" for scenarios such as power outages for the Greenstone Office location.

In the event the Greenstone Office is not available, alternate recovery locations include:

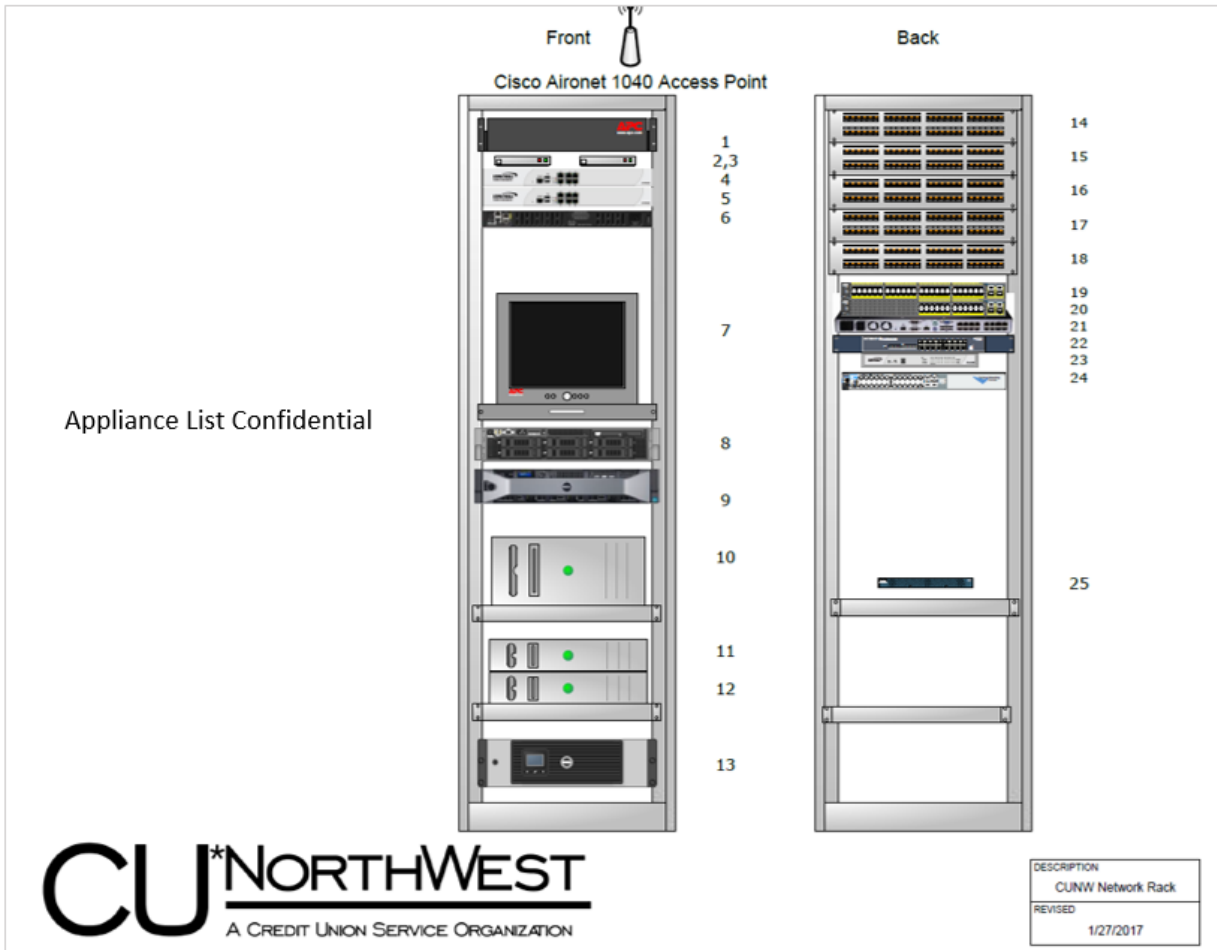
- Remote access (SSLVPN) for most support personnel with an Internet connection
- Spokane Firefighters Credit Union (approx. 20 minutes from Greenstone Office)
- Cheney Federal Credit Union (approx. 35 minutes from Greenstone Office)
- Prime Source Credit Union (approx. 25 minutes from Greenstone Office)

*See "Establishing Command and Control" section for more information on alternate work locations.

CU*Asterisk partners are also available to assist with performing critical business functions in the event the Greenstone Office is not available.

- **Client Services** support is available at CU*Answers
- **Operations** support is available at Site-Four and CU*Answers

- **Programming, Management, Finance, Sales, Conversions, and Technical Services** support is available at CU*Answers.



[Image above shows computer rack at the Greenstone Office]

Appliance List Confidential



1
2
3
4
5
6
7
8

DESCRIPTION
CUNW GMS/DEV Rack
REVISED
2/7/2017

[Image above shows DEV system at the Greenstone Office]

Site-Four

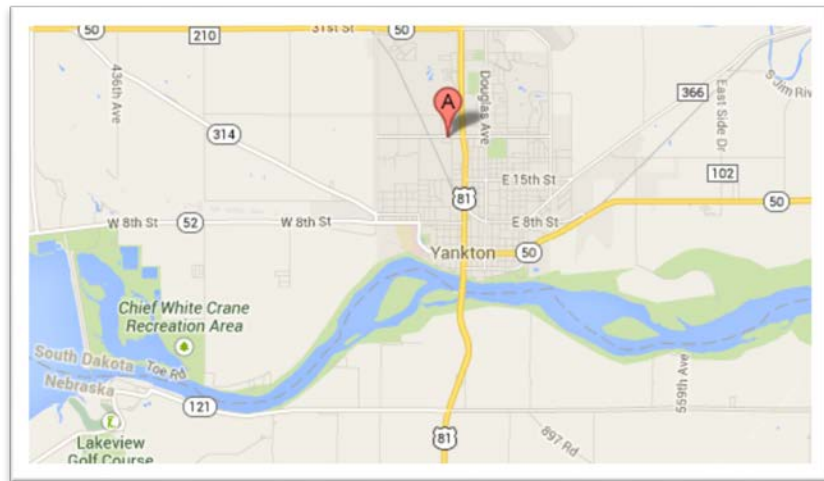
Site-Four is a CUSO and CU*Asterisk network partner. Primary production of CU*BASE/GOLD core-processing is provided by Site-Four from the state-of-the-art datacenter in Yankton, SD. Staff at Site-Four are responsible for daily operations of the host and network configurations that communicate client credit unions and third-party EFT vendors. Site-Four also provides core-processing CU*BASE/GOLD for CU*South (CUSO and CU*Asterisk network partner located in Fairhope, AL).

In the event that systems at the Site-Four location in Yankton are not available, rollover procedures are performed to bring core-processing online at the HA location at CU*Answers (Kentwood, MI).

[A]

Site-Four, LLC
PO Box 356
609 West 21st Street
Yankton, SD 57078
[CONFIDENTIAL]

- Production Datacenter
- CU*BASE/GOLD
- iSeries Administration
- Operations Support
- Client VPN
- Third Party EFT
- Etc.



Site-Four Emergency contact information:

- [CONFIDENTIAL]
- [CONFIDENTIAL]
- [CONFIDENTIAL]

Prevention measures taken by Site-Four to mitigate the risk and/or impact of an emergency or disaster at the Yankton datacenter include but are not limited to:

- Fire detection, suppressant, fire system, and fire monitoring service
- Offsite storage of combustibles
- Smoking prohibited inside Site-Four facilities
- Video security surveillance systems to discourage theft and/or destruction of assets
- Intrusion alarm system with battery backup with Internet connectivity to a monitoring service (alternate dial-up connectivity).
- Alarm systems with redundant VPN connection in Parkston (alternate dial-up connectivity)
- Daily, monthly, and annual backup/archiving of key information
- Limited access to sensitive areas and data
- Insurance coverage for rebuilding and recovery

Site-Four has their own business recovery plans and perform regular recovery testing.

*See "Continuity and Recovery Strategies" section for additional details

site-four

PRIMARY – YANKTON, SOUTH DAKOTA
RACK A3

Appliance List Confidential



[Image above shows the computer rack at the Site-Four datacenter]

CU*Answers

CU*Answers is a CUSO and CU*Asterisk network partner. CU*Answers maintains three locations in Michigan and is the primary developer and vendor for CU*BASE/GOLD software. In addition to the corporate offices in Grand Rapids, MI, CU*Answers maintains a primary production datacenter in Kentwood, MI, a secondary non-core recovery datacenter in Muskegon, MI, and a high-availability environment at the Site-Four datacenter in Yankton, SD, as part of a colocation agreement.

[A]

CU*Answers Corporate Office

6000 28th street SE
Grand Rapids, MI 49546
[CONFIDENTIAL]

[B]

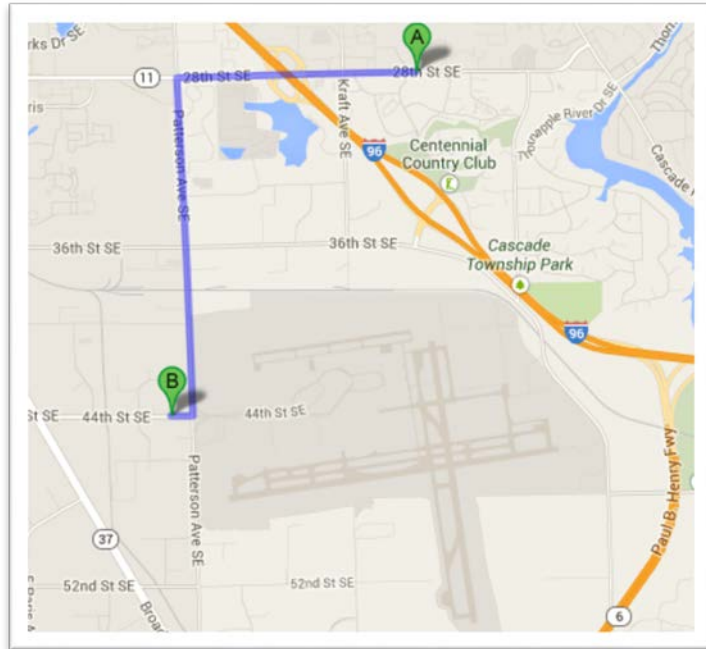
CU*Answers Production Datacenter

4695 44th street SE
Kentwood, MI 49512
[CONFIDENTIAL]

[not shown]

CU*Answers Secondary, Non-Core Recovery Datacenter

316 Morris Ave.,
Muskegon, MI 49440
[CONFIDENTIAL]



While Site-Four provides CU*BASE/GOLD core-processing for CU*NorthWest client credit unions, CU*Answers provides many of the complementary products and services including:

It's Me 247
CU*Checks
Exchange Email
Internal Portal

CU*Talk
AnswerBook
VoIP Phone System
Corporate Web Site
Secondary Operations Support

CU*Spy
GoAnywhere
Lync Communicator
Great Plains/Dynamics
CU*A Imaging Solutions

Etc.

In addition, CU*Answers provides support for critical business functions from many departments including:

Client Services
Network Services
Accounting
Administration
Etc.

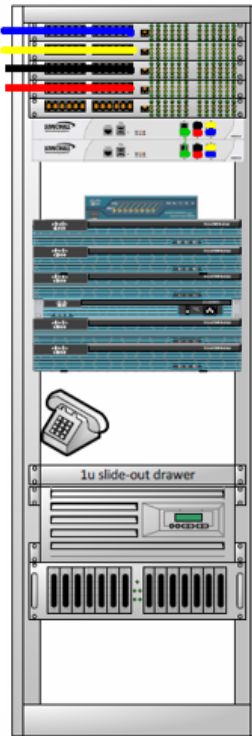
Operations
Programming
Marketing
Collections

Conversions
Human Resources
Web Design
Internal Auditing

CU*Answers maintains a separate Business Continuity Program with regular recovery testing. Information about the CU*Answers program including reports from recovery exercises and test can be found at:

<https://www.cuanswers.com/solutions/business-continuity/>

Appliance List Confidential



site-four
DR – GRAND RAPIDS, MICHIGAN
S4-DR Rack-1
2014-09-27

[Image above shows the HA network at the CU*Answers datacenter]

*See "Overview of IT Environment" for MPLS and VPN data communications diagram.

In September of 2014, a project was completed to move the HA network from the Tierpoint (Liberty Lake, WA) location to the CU*Answers production datacenter in Kentwood, MI. In addition to the HA host, secondary data communication lines for third-party EFT vendors and backup VPN communications for client credit unions have been installed and configured. The CU*Answers datacenter relationship and all equipment for the HA network is owned and managed by Site-Four.

The CU*Answers state-of-the-art datacenter includes redundant components such as:

- Power sources (utility, UPS, generator),
- Internet Service Providers (ISP), and
- Computer Room Air Conditioning (CRAC) units.

The datacenter also includes physical access security (proximity fobs, video surveillance, etc.) and is staffed 24x7.

Systems at the Kentwood location are not mission critical for primary production core-processing when systems at the Site-Four location are available. CU*BASE/GOLD data is replicated in real-time to the HA host using iTERA software by Vision Solutions. Replication status is managed and monitored by Site-Four. Regular rollover exercises are performed to validate procedures and confirm operations from the Kentwood location.

Systems and network devices at the Kentwood location are monitored 24x7 by Site-Four and by CU*Answers Network Services. A copy of the CU*Answers SSAE-16 (SOC 1 Type 2) report is available at:

<http://www.cuanswers.com/solutions/accounting/audit-results/>

CU*Answers Emergency Contact: [CONFIDENTIAL]

Xtend

Xtend is a CUSO and CU*Asterisk network partner that provides services for credit unions to reach members through marketing, call center, and shared branching services and to complement back-office accounting operations and mortgage processing. The sole office for Xtend is located within the CU*Answers headquarters in Grand Rapids, MI. Products and services delivered by Xtend are hosted at the CU*Answers datacenter(s) in MI and are included in the recovery plans for Xtend and CU*Answers.

Products and services provided by Xtend to CU*NorthWest and its clients include:
SRS Bookkeeping, Call Center Member Reach, Audit Link, etc.

Xtend Emergency Contact: [CONFIDENTIAL]

eDOC Innovations

eDOC Innovations is an electronic document solutions provider and CU*Asterisk network partner. The eDOC corporate office is located in Middlebury, VT. A remote office used primarily for software development and support is located in Midway, UT. The eDOC ASP environment is hosted at the CU*Answers Kentwood datacenter and part of the eDOC and CU*Answers recovery plan.

Products and services provided by eDOC include:
ProDOC, iDocVault, Check21, etc.

eDOC Emergency Contact: [CONFIDENTIAL]

CU*Answers Imaging Solutions

CU*Answers Imaging Solutions (CIS) supports online and in-house electronic document products and strategies. The sole office for CIS is located within the CU*Answers headquarters in Grand Rapids, MI. Products and services delivered by CIS are hosted at the CU*Answers datacenter(s) in MI and are included in the recovery plans for CU*Answers. Products and services supported by CIS include:

ProDOC, iDocVault, CheckLogic, CU*SPY, etc.

CIS Emergency Contact: [CONFIDENTIAL]

Recovery at a Glance

Planning for every possible scenario is not practical nor effective. Possible scenarios considered for this plan include:

- Loss of site or denial of access (no physical access to one or more sites)
- Loss of critical functions (service, department, vendor, supplier, etc.)
- Loss of power or other services (utilities, cooling, etc.)
- Loss of critical equipment (hardware/software)
- Loss of communications (data, voice)
- Loss of skilled personnel (injury, illness, pandemic)
- Breach of security (network/system compromise)
- Anticipated disaster (forewarned, severe weather, etc.)

It's important to recognize that each incident is unique and requires careful assessment and an appropriate and coordinated response. Not every incident has the capacity to disrupt business functions but every incident has the potential to create an impact.

Stages of an Incident include:



Crisis – Any situation that is likely to attract or warrant the attention of interested parties (clients, vendors, media, etc.). Most crises are isolated and resolved before escalating into a disaster.

Disaster – Any accidental, natural, or malicious event that threatens or disrupts normal operations, or services and endangers the success of the organization.

Emergency – An ongoing state of abnormal operating conditions that result from a disaster. The state of emergency remains until normality is restored.

Key factors to consider when making decisions during a disruption include:

- Safety of all personnel (evacuation, shelter, etc.)
- Security of data
- Availability of core services, including timing, expected duration of outage, etc.
- Proactive monitoring and controls to detect potential additional disruptions and to alert recovery staff
- Accurate initial assessment to enact proper plans and minimize downtime
- Existing service level agreements with clients and vendors
- Client and vendor expectations
- Each plan's inherent lead time (preparation, chasing down tapes, travel, etc.)
- Importance of the first few minutes and hours of an event
- Potential FUD factor (fear, uncertainty, doubt) of recovery teams, chaos during initial stages, remain calm
- The status of the work in progress at the time of the disruption

Several controls have been implemented during day-to-day operations in an effort to prevent, manage, control, and mitigate the impact of identified risks. During a disruption, additional inherent security risks must be considered such as:

- Reduced fault tolerance during the recovery

- Reduced redundancy of data during the recovery
- Compounded failures (snowball/domino effect, uncontrolled events have a tendency to escalate)
- Physical/network security at alternate sites
- Recovery team fatigue during lengthy recovery efforts

Additional financial considerations include:

- Lost revenue from service outage
- Need for temporary (skilled) staffing
- Equipment rental during the recovery efforts
- Extra shipping costs for moving equipment and materials
- Travel/lodging expenses for recovery teams and displaced staff
- Legal obligations for deadlines missed and service level agreements not met
- Overtime costs (labor) for staff and vendors
- Reputation/brand image (potential future revenue)

Recovery Timeline

This timeline provides a summary of the reaction and recovery process to a disaster. It is designed to help management keep perspective amid the crush of details and problems that occur during the disaster and to educate staff and volunteers who are not regularly involved in the disaster planning process.

The “Emergency Response Team” is responsible to coordinate an assessment of the situation as quickly as possible. The purpose of this assessment is to identify the scope of the disaster and to provide the basis for a declaration of disaster. Specific areas that must be evaluated are the condition and availability of staff members, condition and availability of facilities and the condition of key computer and business systems

1. Incident detected

- Invoke Emergency Response Plan is required
- Perform initial response to mitigate risk (fire extinguisher, fire alarm, power down, etc.).
- Evacuate premise or seek safe shelter if necessary.
- Call local authorities (911 or as appropriate).
- Alert recovery site (alternate branch or reciprocal arrangement) if necessary.

2. Establish chain of command

- A clear chain of command strategy should be determined prior to a disaster to anticipate scenarios where communication channels and/or select Management Team members are not available. It is important that this does not create a delay in key decision making, especially during the early stages of a recovery.

3. Assess situation

- A quick and accurate assessment is required. Consider elements of the incident such as:
 - The availability and condition of staff members
 - The condition and availability of facilities, and
 - The condition of key computer and business systems and vital records.
- Engage additional Emergency Response Units if needed (Fire, Police, EMT, etc.).
- Escalate the incident if necessary.
- Alert outsourced service providers if necessary (Site-Four, CU*Answers, Xtend, etc.).

4. Declare crisis severity based on assessment (escalate)

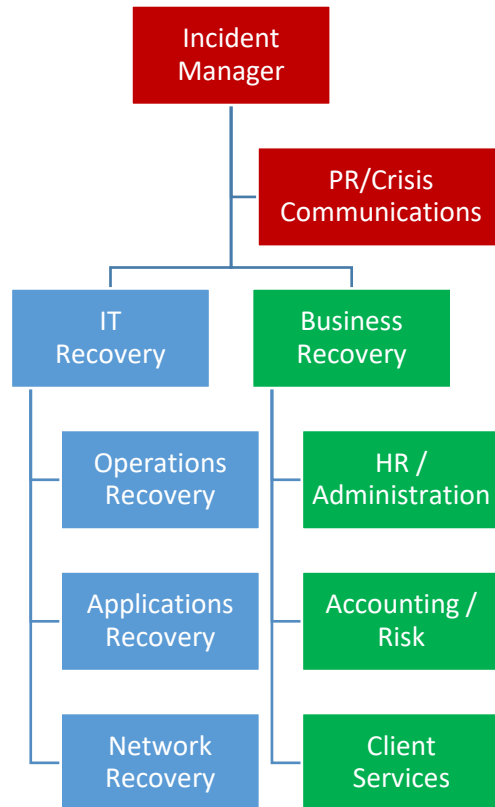
- Consider scope and duration of disruption based on the results of the assessment.

- b. Escalate based on scope and expected duration of outage (examples shown below):
 - i. 0-24 hours (Disruption)
 - ii. 24-96 hours (Emergency)
 - iii. 96+ hours (Disaster)
- 5. Establish command and control of incident and recovery effort**
 - a. Setup command post (alternate branch or other designated location).
 - b. Determine appropriate response to contain incident and initiate recovery plan both during and after business hours.
- 6. Notify recovery team members**
 - a. Communicate to recovery team members the description of the incident, extent of damage, recovery location, and prioritized action plan based on the circumstances of the incident.
 - b. Invoke HA rollover procedures if conditions warrant
 - c. Invoke IT Contingency Plan if conditions warrant
 - d. See "Emergency Response Team" section for recovery team leaders' contact information.
 - e. See "Appendix" for all-staff contact information.
 - f. Mobilize teams to alternate recovery location(s) if required.
- 7. Notify key stakeholders (members, vendors, media, etc.)**
 - a. See "Crisis Communications" section of Plan.
 - i. Send CU*BASE Alert and Announcement (or request CU*Answers to issue)
- 8. Recover core processing business functions**
 - a. Consider alternate recovery strategies based on circumstances of disruption.
 - b. Document and log recovery efforts including personnel hours worked.
 - c. Monitor and control all disaster recovery related expenses.
 - d. Provide status report to all recovery teams
- 9. Notify Insurance Claims Adjustor**
 - a. Notify CUNA Mutual for Insurance purposes.
- 10. Recover remaining business functions**
 - a. See "Recovery at a Glance" section of Plan.
 - b. Provide status report to all recovery teams and key stakeholders.
- 11. Repair/replace facilities and systems**
 - a. Direct and control all salvage efforts related to facilities and vital records.
 - b. Coordinate the restoration / building of permanent location.
 - c. Procure replacement equipment and supplies as necessary.
 - d. Schedule move back to main location.
- 12. Return to permanent location**
 - a. Resume normal operations.
 - b. Provide status report to all key stakeholders.
- 13. Assessment of response and recovery efforts**
 - a. Schedule debriefing meeting to evaluate the effectiveness of the disaster response.
 - b. Identify required modifications for Recovery Plan.
 - c. Prepare gap analysis report based on findings.

Roles and Responsibilities

Recovery teams are divided among two recovery paths (Technology and Business). The next several pages show recovery team hierarchy and each team's primary and secondary responsibilities. The Incident Manager has the authority to make changes as needed based on the circumstances of the event.

Perhaps the most important factor to ensure timely recovery is the quality and frequency of communication between recovery teams and management. It is critical that information is fed upstream to keep the decision-making team up to date on the status of the recovery efforts.



Staff emergency contact information is available in the "Appendix" section.

The following pages you will find specific responsibilities for each recovery team identified above. Each incident or crisis has its own unique set of circumstances and may require individuals and teams to perform multiple roles. It is important that each team is knowledgeable and trained to perform these and other tasks assigned to ensure a timely recovery.

Incident Manager	Responsibilities
<p>★ [CONFIDENTIAL] ★ [CONFIDENTIAL]</p>	<ul style="list-style-type: none"> • Oversee the global efforts of all resumption teams and ensure that recovery goals and timelines are met • Establish command/control center for management of incident/crisis from top level • Primary decision maker on the invocation of the Emergency Response and Recovery plans (including HA Rollover activation if necessary) • Serve as liaison to the Board of Directors to get approval for the acquisition of major purchases and for strategic direction • Communicate with department heads to inform them of strategic direction and the status of the recovery efforts • Resolve issues of priority based on evolving circumstances • Determine message communicated to external media (with Public Relations/Communications Team) • Oversee initial damage assessment and approve major equipment purchases • Offer guidance to local authorities, utilities, services, etc. • Locate and confirm alternate site selection and availability • Oversee, review, and approve any facility's renovation and construction • Inform and update Executive Team on recovery status

PR/Crisis Communications	Responsibilities
<p>★ [CONFIDENTIAL] ★ [CONFIDENTIAL]</p> <p><i>CU*Answers as needed (Writing Team)</i></p>	<ul style="list-style-type: none"> • Serve as communications point of contact for the entire organization with external media relations (TV, print, web, etc.), public affairs, etc. • Serve as a conduit for all internal communications to and from executive and technical teams, alert staff, clients, major vendors, etc. • Message content creation and distribution (official company holding statements to minimize adverse publicity) • Organize internal meetings/briefings on recovery status (distribute recovery plans as needed) • Organize external meetings/briefings on recovery status (press conferences, etc.) • Inform and update Executive Team on recovery status • Assist Human Resources Team in communications with personnel and families • Assist other teams as directed by Incident Manager • Assist in post-recovery cleanup

HR/Administration	Responsibilities
<p>★ [CONFIDENTIAL] ★ [CONFIDENTIAL] <i>CU*Answers as needed (ORD Team)</i></p>	<ul style="list-style-type: none"> • Arrange travel, lodging, meals, and miscellaneous purchases for recovery staff as decided • Ensure proper office working environment for recovery staff at all facilities • Ensure injured/ill personnel receive prompt medical attention, families notified, etc. • Ensure all personnel/family issues are resolved (attendance, payroll, insurance/benefits, legal, etc.) • Answer questions about payroll continuation, employment, or securing temporary personnel during the recovery operation • Explain benefits programs such as medical insurance coverage • Ensure proper (safe/secure) working environment at all locations • Ensure workers compensation claims are properly filed and processed • Verify hours worked for staff and schedule sufficient time off • Hire temporary personnel as required • Assist PR/Communications Team to organize internal meetings/briefings on recovery status (distribute recovery plans as needed) • Inform and update Executive Team on recovery status • Assist other teams as directed by Incident Manager • Assist in post-recovery cleanup

Accounting/Risk/Security	Responsibilities
<p>★ [CONFIDENTIAL] <i>CU*Answers as needed (Accounting Team)</i></p>	<ul style="list-style-type: none"> • Ensure adequate cash flow for expenses during recovery • Contact supply vendors to increase credit limits and expedite shipping due to nature of event • Establish emergency accounting and purchasing procedures • Aid in all monetary details associated with the recovery operations, recording of expenses, post recovery cleanup, intermediate emergency credit arrangements, petty cash, travel advances, etc. • Act as liaison with insurance agency to document, file and settle claims Inform and update Executive Team • Ensure the safety and security of corporate and employee assets including employee and customer information during recovery • Verify that control mechanisms are in place to ensure data integrity regardless of the emergency or circumstances • Review procedures used in recovery efforts to ensure security/compliance policies are followed • Determine recovery status of vital records • Assist in the investigation of cause during the recovery • Assist in documenting and logging recovery efforts • Purchase, receive, store, distribute all software, equipment and supplies, etc. • Maintain interface with supply channel vendors

	<ul style="list-style-type: none"> • Establish mail services area to handle mail for recovery personnel and express-shipping functions at all locations • Verify and maintain all receipts and paperwork • Notify external auditors, if necessary • Inform and update Executive Team on recovery status • Assist other teams as directed by Incident Manager • Assist in post-recovery cleanup
--	--

Network Recovery	Responsibilities
<p>★ [CONFIDENTIAL]</p> <p>CU*Answers as needed (Network Services Team)</p>	<ul style="list-style-type: none"> • Recover network infrastructure (LAN/WAN, etc.) including data and voice communications • Ensure network/data security and availability • Order, install, and configure networking equipment as needed • Confirm recovery-site data-communications lines specifications • Recover archived data environment and restore data from media for server and application recovery • Ensure the archiving of data during recovery efforts to protect against loss in disruption reoccurrence • Recover/restore servers and appliances for critical business applications and services • Inventory damaged and undamaged items, determine salvageable status of equipment • Identify and inventory damaged or destroyed equipment for insurance and replacement purposes • Repair, replace, install, configure all internal network user hardware (workstations, printers, etc.) • Make repair/replacement recommendations • Mitigate damage to remaining equipment and facilities • Oversee cleanup and restoration of damaged equipment and supplies • Coordinate ordering/receipt of replace • Organize the transportation of supplies, data, equipment, and personnel • Assist in establishing/preparing temporary facilities during recovery efforts • Coordinate movement and storage of salvageable items • Inform and update executive team on recovery status • Assist other teams as directed by Incident Manager • Assist in post-recovery cleanup

Operations Recovery	Responsibilities
★ [CONFIDENTIAL] ★ [CONFIDENTIAL] <i>CU*Answers as needed (iSeries Team)</i>	<ul style="list-style-type: none"> • Recover and support iSeries environment hosts, applications, and services • Ensure host security and availability • Recover/restore core data processing daily operations and support • Perform daily operations throughout recovery effort • Secure/retrieve/deliver the correct tapes, documentation, equipment, media etc. to/from storage or alternate site • Ensure the security/inventory of all stored media at all facilities • Manage all backup tapes off- or on-site • Establish secure storage at off-site locations • Assist in receiving and storing needed equipment and supplies • Inform and update Executive Team on recovery status • Assist other teams as directed by Incident Manager • Assist in post-recovery cleanup

Applications Recovery	Responsibilities
★ [CONFIDENTIAL] ★ [CONFIDENTIAL] ★ [CONFIDENTIAL] ★ [CONFIDENTIAL] ★ [CONFIDENTIAL] ★ [CONFIDENTIAL] <i>CU*Answers as needed (Operations Programming)</i>	<ul style="list-style-type: none"> • Recover/restore/support critical business applications and services throughout the organization • Conduct quality control testing for recovered applications and services • Ensure application/service security and availability • Inform and update Executive Team on recovery status • Assist other teams as directed by Incident Manager • Assist in post-recovery cleanup

Client Services	Responsibilities
★ [CONFIDENTIAL] ★ [CONFIDENTIAL] ★ [CONFIDENTIAL] <i>CU*Answers as needed (Client Services Team)</i>	<ul style="list-style-type: none"> • Receive and attend to all incoming client-support calls, route calls to appropriate departments if needed. • Assist PR/Communications Team and Human Resources Team in notifying staff, families, clients, vendors, partners, etc. • Inform and update Executive Team on recovery status • Assist/support network end users including the installation and troubleshooting of all hardware and software issues (workstations, printers, etc.) • Assist other teams as directed by Incident Manager • Assist in post-recovery cleanup

Emergency Response Plan

Initial response to a (potential) incident is key to an effective recovery

No document can contain all of the practical responses for the wide variety of circumstances related to all potential incidents. The emergency response Plan provides critical information and a prioritized list of procedures to be performed for a variety of scenarios with the common goals of:

- Safety of personnel (staff and guests)
- Security of data
- Protection of assets

The “**Emergency Response Team**” is a group of people who are prepared for and respond to any emergency incident, such as a fire and explosion or an interruption of business operations. An accurate and prompt Initial assessment and response during the first few minutes are critical to minimize impact and injury.

A disaster may be declared and this Plan activated by the Incident Manager of any member of the Emergency Response Team.

Emergency Response Team

Name	Position	Cell Phone	Alt. Phone	Recovery Role
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	Incident Manager
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	IT Recovery Manager
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	Business Recovery Manager

*See “Appendix” for staff emergency contact information

Responsibilities of Emergency Response Team include (or delegation of):

- Identify the disruption.
- Assess the damage (facilities, equipment, services, etc.).
- Decide whether a disaster is to be declared.
- Alert recovery teams (keep track of mobilized personnel).
- Locate and confirm alternate site selection and availability.
- Adapt the Plan to account for prevailing circumstances.
- Prioritize recovery steps.
- Initiate, control and coordinate recovery operations.
- Initiate communications with internal and external stakeholders.
- Approve expenditures related to the recovery process.
- Procure the replacement of destroyed or damaged equipment.
- Offer guidance to local authorities, utilities, services, etc.
- Review critical milestones during the recovery process.
- Document and log events as they occur.
- Provide recovery status information to management and board of directors.
- Assemble and verify information for the Crisis Communications Team, who will control its release to stakeholders.

Characteristics and variables of threats to consider when taking action include:

- Speed of onset (some instant, others prolonged)
- Forewarning (some none, others tremors felt)
- Duration (early decisions can shorten or lengthen duration)
- Probability (doesn’t only happen to others)
- Impact on functional areas (isolated, wide-spread, domino effect, etc.)

Emergency Responders

Fire/Police/EMT:	911
Power Company:	[CONFIDENTIAL]
Gas Company:	[CONFIDENTIAL]
Water/Sewer Company:	[CONFIDENTIAL]
Heating/Cooling:	[CONFIDENTIAL]
Greenstone:	[CONFIDENTIAL]
	[CONFIDENTIAL]
	[CONFIDENTIAL]

Establishing Command and Control

Most incidents are relatively small in impact and have a short duration period. For example, a power outage, though somewhat frequent in occurrence (once or twice each year) is short lived (90% less than one hour) with an impact that has been dampened with the deployment of controls such as redundant power sources (UPS and generator). Other incidents can have a much greater impact but may be less frequent (building fire or explosion) however, they still require immediate action to limit and prevent injury and damages. With each incident, our response may be different but the priorities are still the same.

Priorities:

1. Safety of personnel (staff and guests)
2. Security of data
3. Protection of assets

Once an incident is detected, it is important to establish command and control early in the recovery effort. Normal reaction may be that of confusion and chaos in an emergency situation. Therefore, coordination of personnel and resources during emergencies is a critical function of the **Emergency Response Team**.

The Emergency Response Team will establish a Command Center upon declaration of a disaster event. Alternative locations to the main branch include surviving branches, nearby home or building equipped to accommodate the recovery efforts, or a reciprocal credit union site. The location will be disseminated to staff via established call tree processes and as specified in the Crisis Communications section.

Typical items necessary at a command center may include:

- Office supplies (pens, paper, paperclips, envelopes, files, folders, staplers, etc.)
- Fax/printer/copier (with supplies – paper/toner)
- Folding tables and chairs
- Whiteboard and dry-erase markers
- Check stock and specialized forms

Emergency Response Checklist

- Conduct initial status meeting with Recovery Team leaders.
- Determine the extent of response and recovery actions to be performed.
- Establish frequency of communications to provide support and on-going status of current response and recovery activities.
- Observe all staff behaviors and as needed provide periods of rest and relief to relieve stress and correct inappropriate behavior.
- Maintain a log of recovery activities (problems encountered, suggestions for improvements to the plan) of each business function affected.
- Conduct an initial assessment.

- ❑ Determine the status of the work in progress at the time of the disruption and provide a status update to the stakeholders and management.
- ❑ Perform damage assessment.
- ❑ Determine criticality of damaged/destroyed items or components (salvage).
- ❑ Cell phone cameras can be used to document disaster area damage.

Incident Assessment

The purpose of the assessment is to gain relevant information and to determine the best strategies for recovering each system and/or critical business function.

System Outage Assessment Report to include:

- Cause of the system disruption, including type, scope, location, and time of disruption
- Location of failing components and those users without service
- Impact of the disruption or components damaged
- Functional status of all system components (fully, partially, nonfunctional)
- Potential for additional disruption or system damage
- Identification of a single point of failure
- Items to be replaced (hardware, software, firmware, supporting materials)
- Anticipated downtime of the system (i.e., longer than two days?)
- Classification of system failure as minor or major.

Post-Incident Assessment

- What was learned?
- What happened that we did not expect?
- What worked, didn't work and why?
- What needs to be done to improve our preparedness?

Securing Corporate Assets

Once recovery procedures are underway the team will be responsible for making sure that sensitive data is protected from public access in accordance with CU*NORTHWEST current circle of security policy. This responsibility will revolve around the recovery of the firewall systems and encryption requirements currently in place for the storage of data, transmission of data to third parties and clients, and the proper configuration of access points into the CU*NORTHWEST network. This will require a constant communication with the I.S. Recovery Team on the design and implementation of the new network infrastructure. In the event that specific IT Systems are designed outside the scope the original system configuration the team will be responsible to perform an assessment of risk and give recommendations to the specific team leaders requiring such assessment.

Securing Assets in Existing Facility

In the event of partial destruction of one the CU*NORTHWEST main facilities the Security Team will be responsible for the security of corporate assets which remain in tack or are partially destroyed. The following outlines the procedures to be followed:

Computer Equipment

A full inventory listing of the facilities hardware equipment will be maintained at the offsite storage facility. This list will be used to account for the equipment at the original facility. Once accounted for, the equipment will be transported to the new facility for use in the resumption plan. Equipment that is damaged will be moved to a facility with proper physical security and destroyed in accordance with CU*NORTHWEST existing policies.

Corporate Written Documentation

All paperwork remaining in the original building will be inventoried, crated, and either shipped to the new facility if required or shipped to a facility which meets minimum-security requirements. Such paperwork includes:

Client Contracts and correspondence

Information found in file cabinets, office furniture, and other storage locations which contain confidential client/member information. If possible CU*NORTHWEST personnel will be responsible for the gathering of information found within desks and other cabinets. In the event that it is not possible for CU*NORTHWEST personnel to gain access to the destroyed facility items will be boxed and label with the appropriate offices listed on the boxes.

Magnetic Media

All magnetic media found within the damaged facility, which may have value at the new site, will also be evaluated for usefulness and sensitivity. Useful data will be transported to the new facility and the remaining will be transported to a secure facility

Transportation of Vital Assets

The security team will manage transportation of vital assets. When applicable the transportation will be completed by CU*NORTHWEST staff. In the event that transportation is a contracted third party, proper bonding will be required and all contracts must be reviewed by the CFO.

Relocation of Corporate Assets

Once assets are relocated to the new facility the security team will be responsible for the evaluation of the new facilities physical security. Proper perimeter alarm and fire systems will be evaluated by the team to ensure that corporate assets are properly protected from theft and other anticipated risks. In the event the team finds defaults in the nature of the security systems, arrangements will be made to upgrade the facility and provide alternative security methods in the interim period.

Disposition of Corporate Assets

When the asset inventory is completed the team will compile a list of items to be disposed of. This list will contain the following information:

1. Method of disposition
2. Detail if back-ups of the data or information exist and where they are stored
3. The disposition methodology used for each type of asset listed

The accounting department to ensure that all items have been properly accounted for will complete a reconciliation of hardware.

Systems/Applications Outage Assessment Report

SYSTEM / APPLICATIONS OUTAGE ASSESSMENT REPORT	
Recovery Team(s):	
Event Information	
Date:	Time of Disruption:
Location:	Type of Event:
Impact to System:	Facility Damage:
Personnel Injuries:	Disruptions Classification (Minor or Major)
System Information	
Point of Contact:	Est. Duration of Disruption:
Impact on Components:	
Component Resources Affected:	
Type of Damage to Resource:	
Estimated Equipment Needs:	
Recovery Information	
Suggested Recovery Strategy:	
Administration	
Completed by:	Date:
Reviewed by:	Date:
Notes:	

Declaration of Disaster

For incidents where long-term outages and high impact are expected, engaging and mobilizing recovery teams and invoking the proper recovery plan quickly is imperative. This decision is most likely performed by the Incident Manager or action member of the senior management team.

Considerations for making rollover/recovery decisions include:

- Knowing what is involved and the time it takes for performing a rollover is key.
 - Also, knowing the amount of time to roll-back if necessary.
- The scope of the incident (list of critical products/services/functions that are disrupted).
- Timing of incident (day, night, weekday, weekend, proximity to open of business day, etc.)
- Status of daily processing (what needs to be completed before credit unions can access data, expected duration, etc.)
- Expected volume (holidays, etc.)
- Impact of disruption (who does it affect, which applications/services, etc.)
- Is the incident contained or is there the potential for it to expand in scope?
- Integrity of data (production and HA replication status)
 - Is rolling over even an option in this circumstance?
 - If we roll, what is the inherent risk?
 - If we don't roll, what is the impact?
- What's plan B if rolling is not an option (know your options)?
 - Recovering from tape?
 - If so, what data is at risk (does it meet RPO)?
 - What is the anticipated recovery time (does it meet RTO)?
- Can we suspend rolling until a more convenient time?
- What is the availability of recovery personnel (how does this impact our recovery effort)?

Continuity Insurance

Insurance allows for the organization to recover losses that cannot be completely prevented and expenses related to recovering from a disaster. Insurance coverage is obtained for risks that cannot be entirely controlled, yet represent a potential for financial loss or other disastrous consequences.

Evaluation of Insurance Options

To offset potential losses, CU*NorthWest has purchased insurance coverage for identified perils. This coverage is referred to as business-interruption or additional-expense insurance. Exposures not addressed by insurance will be taken into account in the Business Recovery Plan. There are two basic types of insurance: property coverage and time-element coverage. Property coverage covers buildings, personal property, and equipment and machinery. Time-element coverage covers such items as business income, extra expenses, leasehold interest, and rental value.

CU*NorthWest maintains both types of insurance coverage.

Covered Perils:

- Explosions
- Fire or lightning
- Leakage
- Mine subsidence
- Riot or civil commotion
- Sinkhole or collapse
- Smoke

- Vandalism
- Volcanic action
- Wind or hail

Extensions to Normal Coverage:

- Electrical arcing
- Falling objects
- Glass breakage
- Mechanical breakdown
- Steam explosion
- Water damage
- Weight of ice, snow, or sleet

Property Coverage:

The value of insured assets is generally determined by a combination of methods including actual cash value, replacement-cost value, functional-replacement value, and book value.

Time Element Coverage:

The expenses incurred during the recovery of critical functions. Examples include: business income - the loss suffered because we cannot provide our services.

Extra Expenses:

Coverage for those expenses that are beyond the normal operating expenses required to continue operations when premises are damaged during an interruption. The damage must be caused by an insured peril. Examples include:

- Disaster-declaration fees
- Rent for alternative office site
- Rent for fixtures, machinery, and equipment
- Light, heat, and power at temporary locations
- Insurance at temporary locations
- Moving and hauling
- Installation of operation at temporary location
- Employee expenses
- Administrative expenses
- Emergency command-post expenses
- Operating expenses

Common Policy Provisions

This section includes policy ground rules, duties under the policy and duties after a loss. These provisions apply to the coverage in the Property, Expense/Income, Lending and Liability sections of the Policy.

The following steps must be done in the event of loss or damage to Covered Property:

- Notify the police if a law may have been broken
- Give CUNA Mutual Group prompt notice of the loss or damage. Include a description of the property involved. But, failure to furnish such notice or proof of loss as soon as reasonably possible will not invalidate or reduce a claim unless CUNA Mutual Group rights are jeopardized.

- As soon as possible, give CUNA Mutual Group a description of how, when and where the loss or damage occurred.
- Take all reasonable steps to protect the Covered Property from further damage. If feasible, set the damaged property aside and in the best possible order for examination. Also, keep a record of your expenses, for consideration in the settlement of the claim.
- CUNA Mutual Group may request the following procedures:
- If requested, give a complete inventory of the damaged and undamaged property. Include quantities, costs, values and amount of loss claimed.
- Permit CUNA Mutual Group to inspect the Covered Property and records proving the loss or damage.
- If requested, permit CUNA Mutual Group to question you under oath at such times as may be reasonably required about any matter relating to this insurance or your claim, including your books and records. In such event, your Answers must be signed.
- If requested, send a signed, sworn statement of loss containing the information requested to settle the claim. You must do this within 60 days after CUNA Mutual Group's request. CUNA Mutual Group will supply you with the necessary forms.
- Cooperate with CUNA Mutual Group in the investigation or settlement of the claim.
- Promptly send any legal papers or notices received concerning the loss.
- Make no statement that will assume any obligation or admit any liability, for any loss for which CUNA Mutual Group may be liable, without consent.
- In case of loss to "valuable information" make every reasonable effort to collect amounts owed to you.

Insurance Agency:

CUNA Mutual
[CONFIDENTIAL]

Policy # [CONFIDENTIAL]

Emergency Response Procedures

Response procedures are identified below for the following scenarios:

- Fire/Explosion (requiring building evacuation)
- Severe Weather (requiring seeking safe shelter)
- Flood and Water Damage
- Power Outage
- Injury/Illness/Mass Absence (Pandemic)



Fire/Explosion

When a fire is discovered:

- A member of the Emergency Management Team is to notify the authorities and follow any instructions given.

Fire Departments

Spokane Dial 911 or 534-7377

Liberty Lake Dial 911 or 928-2462

- Make the following statement:

*"This is CU*NORTHWEST. We are located at 1421 N. Meadowwood Lane, Suite 130. We have a fire."*

- Do not hang up until instructed. Be as accurate as you can about details.
- In the event of a minor fire, a fire extinguisher should be activated. Fire extinguishers are located by the door next to the operations room, next to the back door and in the hallway outside the office near the women's restroom.
- Alert other tenants in the building if the fire cannot be extinguished.
- The Emergency Management Team will calmly evacuate all employees and clients to the parking lot of the shopping center directly behind the building.
- The CEO is to notify the Board of Directors of the situation.

Post-Fire Procedures

- A member of the Emergency Management Team will obtain permission to re-enter the building from the Fire Department.
- The Accounting Department is to notify the insurance company:
- Employees are not to re-enter the building until authorized by management.
- Employees are not to open drawers, cabinets, or move any documents until instructed by management.
- Containers holding records should be completely cooled before opening.
- When preparing to open containers, it is advisable to have a fire extinguisher and/or water available in the event of flash ignition.
- Records, which have become brittle or charred, may be placed between glass sheets for further protection until reconstruction begins.

- If necessary, the Emergency Management Team will proceed with Step 2 of the Disaster Recovery Plan, including activating backup sites.

Building Evacuation

Upon instruction to evacuate the building, all employees should do the following, **providing time permits and in no way will endanger the employee:**

1. Log off your terminal.
2. Power down terminals, personal computers and printers, time permitting.
3. Log out of phone system.
4. Close and lock file cabinets containing sensitive data in the accounting office.
5. Notify CU*Answers CSR and Site-Four that we are under an emergency situation (time permitting).
6. All personnel assigned laptops should make every effort to take their laptops out of the building with them as long as this will not affect their personal safety.
7. A member of the Emergency Management Team will escort all employees and visitors from the building and have them go to the parking lot directly behind the building and wait for further instructions from a member of the Emergency Management Team.
 - a. **Under no circumstances shall employees or visitors leave the property without notifying a member of the Emergency Management Team.**
8. A member of the Emergency Management Team will ensure that all windows are closed, and that interior doors are closed but NOT LOCKED so as to allow easy access to fire personnel.
9. Management will determine if and when the iSeries systems and all power will be shut down. If necessary, the **Client Services** department will notify clients of the situation via phone or fax.
10. A member of the Emergency Management Team will stand as close as possible to the main entrance in order to direct police and fire personnel.
11. Members of the Emergency Management Team will keep non-essential personnel out of the building, if possible.
12. The above procedures will be reviewed annually with all staff in coordination with the annual fire extinguisher training session.

Severe Weather / Shelter-in-Place

In case of tornado, flood, or other severe weather condition endangering the safety of CU*NORTHWEST employees and property, the following steps should be taken:

Tornado

A tornado watch is a forecast of weather conditions, which are ripe for the development of a tornado. Normal CU*NORTHWEST activities will continue, but management should be kept informed of weather conditions.

- If the watch is upgraded to a tornado warning, management will execute shelter plan, relocating all customers and employees to the following location:

Liberty Lake: Basement of Greenstone building

- No employee shall be permitted to leave the shelter area or the building until directed by management.
- In the event of damage due to tornado, management shall notify the authorities and follow any instructions given.

Fire Departments

Spokane Valley Dial 911 or 534-7377

- Make the following statement: “This is CU*NORTHWEST. We are located at <building location>. We have been hit by a tornado.” Do not hang up until instructed. Be as accurate as you can about details.
- The CEO is to notify the Board of Directors of the situation. (See the “Appendix” for contact information.)
- The Accounting Department is to notify the insurance company:

CUNA Mutual

[CONFIDENTIAL]

- If necessary, the Emergency Management Team will proceed to activate the necessary backup sites.

Flood/Water Damage

Excess water and flooding can cause damage to multiple areas in the building, including the computer rooms. Repairs for structural damage can prevent staff from returning to their work areas. In severe cases, where large areas of flooring and drywall are in need of replacing, renovation can take up to 30 days or more.

Sources of water can include:

- Restroom (sink, toilet, water feeds, etc.)
- Kitchen (sink, dishwasher, etc.)
- Ceiling (water source and drain pipes, roof leaks, AC unit condensation leaks, etc.)
- Exterior doors, windows and walls where water retention is possible
- Floor drains (failed sump pump)
- Fire rescue efforts (sprinkler system or fire hoses)

Damage can occur to:

- Electrical systems (building and computer room)
- Structure (weakening walls, floors, etc.)
- Paper documents
- Electronic media (tapes, hard drives, etc.)

In the event of flooding or other water damage:

- Determine if the Building Evacuation plan needs to be activated.
- Determine proximity/risk to computer room (power off equipment as necessary).
- Cover equipment with plastic tarps to protect from roof leaks (warning about humidity and corrosion on computer equipment).
- Determine source of water (roof, pipe, drain, wall, floor, etc.) and location of water-source shut off.
- Determine if sump-pump is functioning properly (between elevator and computer room on west side of building).

During the recovery efforts:

- Ensure that any hardware that is determined to be unsafe to operate is properly labeled. If determined to be safe, unplug equipment from the power source.
- Do not simply power equipment up until you are sure that that any moisture has been removed.

- Visually inspect equipment for external and internal damage. Do not power up any equipment prior to passing this inspection.
- Secure media in dry storage area.

In the event of a flood or threat of flood, the following procedures should be followed:

- Management will monitor weather conditions and determine whether or not evacuation is warranted.

If evacuation is necessary, use the same procedures as outlined for fire evacuation on Page 19. If necessary, employees should evacuate to higher ground located at the Liberty Lake golf course.

- Management will determine possible relocation of materials, such as records, time permitting.
- Management will determine if and when the iSeries systems and all power will be shut down. If necessary, the Client Services department will notify clients of the situation via phone or fax.
- Management is to notify the authorities and follow any instructions given.

Fire Department

Spokane Valley Dial 911 or 534-7377

- Make the following statement:

*“This is CU*NORTHWEST. We are located at <building location>. We have a flood.”*

- Do not hang up until instructed. Be as accurate as you can about details.
- The CEO is to notify the Board of Directors of the situation. (See the “Appendix” for contact information.)
- The Client Services department will notify clients of the situation via phone or fax.
- The Accounting Department is to notify the insurance company:

CUNA Mutual

[CONFIDENTIAL]

- If necessary, the Emergency Control Team will proceed with Step 2 of the Disaster Recovery Plan, including activating backup sites.

Power Outage

The Greenstone Office location has UPS units to power critical LAN appliances and devices for short-term power outages. For power outages exceeding 4-6 hours, actions must be taken to gracefully power down equipment. That decision will be made by a member of the Emergency Management Team based on the circumstances of the event.

Systems and appliances at Site-Four and CU*Answers are provided redundant power sources for short and long-term outages. Equipment at both Site-Four and CU*Answers production datacenters are monitored 24x7, tested weekly, and are part of a regular maintenance program.

Injury/Illness/Mass Absenteeism (Pandemic Policy)

In the event of injury to personnel (staff or guest):

- Determine if medical help is required.
- Ask for CPR qualified individuals if necessary.
- First aid supplies kits (including AED) are located in the break room.
- Contact the Human Resources department, who will contact family members if needed.
- Record identity of eyewitnesses and notes from event.

CU*NorthWest Pandemic Policy

In June of 2009, the NCUA issued a letter to credit unions, Letter No.: 09-CU-13, requiring credit unions to augment their disaster recovery plans. The letter specifically speaks to the potential operational problems associated with a large-scale pandemic or hurricane. The letter requires credit unions to adopt a response to these events and evaluate the potential risk to the organization including an evaluation of critical-service-provider plans for operating during a large-scale absence event.

This document describes the procedures and controls implemented by CU*NorthWest to provide for continuation of business operations necessary to support our clients and partners should a large scale-absence impact our staff.

Definition

A large-scale absence, for purposes of this document, is defined by CU*NorthWest as missing 50% or more of the employee population for a period of up to two consecutive weeks.

Method

Team leaders were asked to assess specific needs and concerns that they would face in a large-scale absence event for their area(s) within the company. These needs and concerns, the response or reaction to those concerns, and any preventative measures that can be taken have been used in the development of this planning document.

Client Service

Possible Delays in Service (longer than normal wait before the phone is answered, longer than normal responses to questions that require research, etc.)

Delays in servicing our clients should be expected. However, we would want to communicate this to the client appropriately by sending out a scripted message using our Alert procedures. Management would be key in assisting the employees in prioritizing the workload.

Coverage of All Shifts

Cross training and management involvement will help the client service areas to make sure all necessary shifts are covered across all areas of the company. Employees and managers who have the capability to work from home would be encouraged to do so, if the situation allows.

Prioritizing Daily and Pending Duties

Consider the time of the month—there might be things that must be done as they are time sensitive. For instance, is it end of month? If so, divert team members across departments.

Management would make decisions on readjusting the priority list and delay of non-critical project travel.

Programming

Impact Pending Projects and Other Departments

The projects to be worked on will be prioritized by management; inevitably some projects will need to be delayed or put on hold for a short period of time. We would want to communicate this to the clients appropriately by sending out a scripted message using our Alert procedures.

Managing Project Timelines

Management will adjust these timelines and workloads (i.e. briefly delay CU*BASE releases, CU*BASE prototypes and demos if necessary.)

Responsibility for resulting GOLD issues

Cross training and updated documentation will be an important preventative measure to take in making sure a greater number of employees can be responsible for any GOLD issues. Employees and managers who have access will be encouraged to work from home, if the situation allows.

Delivery

Delivering Quality Service to the Clients

For services that require travel, employees will be expected to be aware of their ability to complete their responsibilities without negative effects on clients. If necessary (i.e. in a conversion situation), CU*NorthWest management may need to make a decision regarding whether or not more employees will need to be sent to supplement for the incapacitated employees.

For services delivered from our offices, cross-training and up to date documentation will be necessary to be able to continue to provide quality service. In some cases, CU*NorthWest may need to contact staffing agencies if additional staff is needed.

Handling Time Essential Duties

Essential duties will still need to be completed; other team members will be assigned these tasks by management as necessary. If possible management will adjust these timelines and workloads by reprioritizing duties.

At the Client Site

Scenario #1: The entire conversion team is "down for the count". What happens at the client site?

Until additional staff can arrive on site, web and phone conferences would have to be utilized for training, support, sign-off etc. Several concurrent sessions could be scheduled to facilitate training by department.

Depending on the location of the credit union, the VP of Delivery Services may tap other CU*NorthWest credit union employees as support staff.

Scenario # 2: What if the Credit Union is going through an event? What would we do for sign offs?

Past experience does give us some guidance in this situation; we can use CPAs and Board members as alternatives to a CEO for sign-off authorization.

Additional support may have to be rescheduled for a particular department. For example, 'live week' may be postponed if several credit union employees are unavailable for the necessary training.

Operations

Shift Coverage and General Department Responsibilities

Primary operations are performed by Site Four. If necessary, adjust schedules of remaining team members to cover all shifts and run with reduced staff per shift. Managers will provide additional coverage as needed. Beginning of Day, End of Day, and File Transmissions must be delegated to other trained team members in the absence of operators from the shift on which the processes are carried out. Operations cross-trains team members

on an ongoing basis to ensure delivery of time-sensitive items. An email/call chain is in place in order to contact the Operations Team to let them know of any changes in shift and duties they must fulfill as the situation changes.

Communication

The determination that CU*NorthWest is experiencing a large-scale absence event will happen at the management level. In such an emergency, staff at CU*Answers and CU*South will be alerted for support call coverage.

Should senior CU*NorthWest management determine that conditions warrant informing and alerting clients, the following script may be used as a template to create the email message:

Dear Credit Unions,

*We are notifying you via our Alert system that CU*NorthWest is experiencing a large-scale absence of staff due to extenuating circumstances. As a result of this, you may experience delays. If the person you are trying to contact cannot be reached or you need immediate assistance, please call the CU*NorthWest operator and they will be able to help you or direct you to someone who can in a timely manner. Thank you for your patience.*

CU*NorthWest' Management Team

Managers will be responsible for communicating to their staff members any new priorities or changes in responsibilities resulting from the event.

Travel during a Management Declared Event

The travel expectations during an event will be decided upon by CU*NorthWest Senior Executive Team and communicated to the employees by the Human Resources department. Depending on the circumstances surrounding the event, any decision could be made up to and including the suspension of ALL travel.

Staff Interaction during an Event

The staff interactions during an event will be decided upon by CU*NorthWest Senior Executive Team and communicated to the employees by the Human Resources department. Depending on the circumstances surrounding the event, decisions will be made regarding:

- Severely discouraging or disallowing large assemblies of employees (on or off work premises)
- Closing all meeting rooms
- Limiting all staff interactions as much as possible
- Encouraging or forcing employees to work at home or at other CU*NorthWest offices
- Offering masks and setting up for cleaning stations around the office
- Specifically Addressing the Flu Season: Controlling the spread of infection

With the news of the H1N1 virus currently spreading across the nation, we are all a little more aware of methods to limit the spread of infection. This is not the only virus that could create an event to be proactive about, but we will use it as a stepping stone to understand how we will handle a pandemic event if one does occur in the future.

- Infected staff should defer coming to work for the length of the incubation period of the virus.
- Staff should utilize the hand-sanitizing stations provided around the office and wash hands often.
- Clean keyboards and other equipment, especially if workstations are shared between staff members.
- A certain degree of social distancing could be practiced; reducing frequency, proximity, and duration of contact can also help reduce the spread.

Planning, then, is essential. This large-scale planning document outlines how the different areas of operation will handle mass absences.

NCUA LETTER TO CREDIT UNIONS
NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA 22314

DATE: June 2009 **LETTER No.:** 09-CU-13

TO: Federally Insured Credit Unions

SUBJ: Hurricane Preparedness and Pandemic Planning

Dear Board of Directors:

The purpose of this letter is to inform credit union management to update their Business Continuity and Disaster Recovery Plans because of recent announcements by the National Hurricane Center (NHC) and Pandemic events related to the H1N1 virus (swine flu).

On May 21, 2009, the NHC predicted a near-normal Atlantic hurricane season for 2009. Forecasters predicted a seventy percent chance of nine to fourteen named storms, of which four to seven could become hurricanes, with one to three major hurricanes. The outlook provided by the NHC is not only a guide to the expected seasonal activity, it is also a warning it is time to take action.

NCUA urges all federally-insured credit unions, in recognition of National Hurricane Preparedness week and the seasonal outlook provided by the NHC, to perform a review of their disaster preparedness and response plans. These plans should be commensurate with the complexity of operations and focus on minimizing interruptions of service to members and maintaining member confidence in times of an emergency. Previous disasters have provided many “lessons learned” in working through a disaster. Following are the principle “lessons learned”:

- Implement pre-disaster actions to ensure a constant state of readiness and take steps to safeguard assets and vital records if an early warning is received;
- Communicate disaster preparedness and response efforts before, during, and after an emergency to keep members, volunteers, employees, and regulators fully aware of the situation;
- Utilize a cross-section of people to develop, test, and implement disaster preparedness and response plans;
- Ensure back-ups are available for not only data but also personnel, worksites, equipment, vendors, and other resources; and
- Treat disaster preparedness and response plans as “living documents” to be updated as circumstance change.

The recent events pertaining to the H1N1 virus (swine flu) highlight the importance of credit union disaster preparedness and response plans including provisions for a Pandemic event. While the recent flu epidemic was mild in the United States, the World Health Organization and Center for Disease Control are cautious about predictions the H1N1 virus will have on the normal flu season this fall and winter.

Pandemic planning, unlike most natural or technical disasters and malicious acts, presents unique challenges to credit unions. The impact of a pandemic is much more difficult to determine. As experience with the recent H1N1 flu, pandemics can be focused to specific regions of the world or the United States, but can spread quickly and cause health officials to close schools and other public gathering facilities or events. Experts believe the most significant challenge may be the severe staffing shortages likely to result from a pandemic outbreak.

Federally-insured credit unions need to review their disaster preparedness and response plans to ensure their pandemic plan is appropriate for their operation. The plan should include:

- A preventative program to reduce the likelihood the operations will be significantly affected by a pandemic event;
- A documented strategy which provides for scaling pandemic events including provisions for a possible second and third wave of a pandemic;
- A comprehensive listing of facilities, systems, or procedures to continue critical operations if a large number of staff are unavailable for prolonged periods;
- A testing program to ensure the pandemic planning practices and capabilities are effective;
- An evaluation of critical service provider plans for operating during a pandemic; and
- An oversight program to ensure ongoing review and updates are made to the pandemic plan.

NCUA provides the enclosed resources to assist you in reviewing your own disaster preparedness and response plans related to hurricane and pandemic preparedness.

If you have any questions or concerns, please contact your NCUA Regional Office or State Supervisory Authority.

Sincerely,
Michael E. Fryzel,
Chairman

Resources

NCUA Resources:

- [Letter to Credit Unions 08-CU-01, Guidance on Pandemic Planning](#)
- [Letter to Credit Unions 06-CU-12, Disaster Preparedness and Response Examination Procedures](#)
- [Letter to Credit Unions 06-CU-11, Interagency Guidance Lessons Learned by Institutions Affected by Hurricane Katrina](#)
- [Letter to Credit Unions 06-CU-06, Influenza Pandemic Preparedness](#)
- [Risk Alert 06-CU-01, Disaster Planning and Response](#)
- [Letter to Credit Unions 01-CU-21, Disaster Recovery and Business Resumption Contingency Plans](#)

Interagency Resources:

- [FFIEC IT Handbook Booklet: Business Continuity Planning on FFIEC web site](#)

REFERENCES

In addition to resources included above, credit unions may find these web sites helpful in their planning activities:

- [Ready.Gov - Business Emergency Planning Guidance](#)
- [The National Strategy for Pandemic Influenza](#)
- [National Hurricane Center](#)
- [Department of Health and Human Services \(DHHS\)](#)
- [Business Pandemic Influenza Planning Checklist \(DHSS\)](#)
- [Avian Flu Website \(DOD\)](#)
- [Centers for Disease Control \(CDC\)](#)
- [World Health Organization \(WHO\)](#)
- [Department of Agriculture \(USDA\)](#)
- [Department of Labor Occupational Safety and Health Administration \(OSHA\)](#)
- [Department of State](#)

Distributed Denial of Service Attack Response

A number of critical products and services provided to CU*NorthWest clients require access to public-facing devices on the Internet that are exposed to the threats of a Distributed Denial of Service Attack (DDoS). These devices are hosted and provided by CU*Answers. For the purpose of this recovery plan, CU*Answers has provided the following:

*“Distributed Denial of Service attacks are just one type of threat faced by organizations that depend on the Internet for business transactions and communications. A description of DDoS attacks can be found in the CU*Answers April 2013 Whitepaper titled "Assessing DDoS Risk". In response to the heightened awareness surrounding the recent activity from these types of attacks, CU*Answers is providing this overview of the documented DDoS Incident Response Plan.*

PREPARATION

The best defense against such security attacks begins with a layered security strategy starting at each hardened host and expanding to security appliances at and beyond the network perimeter. Key to an effective incident response are the skilled and knowledgeable personnel that make up the Incident Response Team.

*The roles and responsibilities of the Incident Response Team are described in the “CU*Answers Incident Response Policy”.*

COMMUNICATION

*A critical component of any incident response is timely, accurate and consistent communications at all points within the response phase to all internal and external stakeholders including senior management, affected clients and partners, legal counsel, vendors, and agencies including law enforcement (if appropriate). For use with all incidents and disruptions, CU*Answers has deployed the CU*BASE Alerts Notification Site, (accessible to CU*BASE on-line and in-house clients only) for posting current alert status information in conjunction with broadcast alert email notifications. All affected non-client stakeholders will be contacted using methods identified in the “Crisis Communications” section of the “CU*Answers Business Continuity Plan”.*

DETECTION

*Proper detection of potential incidents begins with 24x7 network and host monitoring from multiple presence points within the network. With these monitoring and alerting tools in place, IRT members are notified around the clock of potential incidents that may require prompt response. Personnel are trained and skilled to take immediate measures to identify the type and scope of the incident and to accurately assess the risk to the organization (particularly the security, integrity, and availability of data on the CU*Answers networks).*

MITIGATION

*Once an incident is detected, mobilized IRT members may determine that mitigating steps are required, ranging from the limiting of access to/from specific hosts and networks to the complete protection of assets by prohibiting all traffic to/from specific hosts and networks. The Incident Response Team has been granted the "Authority to Act" as described in the “CU*Answers Incident Response Policy”. Depending on the circumstances of the attack, the Incident Response Team may engage the cooperation of upstream service providers and security vendors if necessary.*

REMEDICATION AND RECOVERY

Once it has been determined that the incident/attack has elapsed and/or the risk has been reduced, the Incident Response Team will reintroduce services to the network until all have been restored. At the conclusion of the response effort, post-attack procedures include the collection of logs and potential forensic evidence (if applicable) and documenting response and mitigation procedure gaps, weaknesses and lessons learned.”

Continuity and Recovery Strategies

Those products and services provided by CU*NorthWest to credit union clients that have the greatest impact are categorized as “core-processing”. This includes CU*BASE/GOLD and supporting applications. The limited tolerance for downtime for CU*BASE/GOLD core-processing applications requires the implementation of real-time data replication on hosts located in geographically disperse datacenters with redundant power and communication resources.

To accomplish this, CU*NorthWest has contracted with Site-Four for providing CU*BASE/GOLD core-processing services in an ASP environment to meet these strict availability and security requirements.

“High Availability” refers to a multiprocessing system that can quickly recover from a failure with minimal downtime. A “highly available” system or component is continuously operational for a desirably long length of time. Availability can be measured relative to “100% operational”.

For those products and services identified as “(non)core-processing”, alternate continuity recovery strategies have been implemented and plans developed and tested to ensure an effective and efficient recovery. Where possible and feasible, redundant components have been included in host and network configuration (i.e. redundant power supplies, hard drives, etc.) to eliminate or reduce single points of failure and to mitigate identified risk.

*See “IT Recovery” section for more information.

Overview of HA strategy

Owned and managed by Site-Four, IBM hosts are located at state-of-the-art datacenters in Yankton, SD and Kentwood, MI. Vision Solutions’ iTERA software is used to replicate member data between the hosts in real-time. Client credit unions connect to both primary (Yankton) and secondary (Kentwood) datacenters through Internet VPN communications. Third party EFT vendor communications are also located at both primary and secondary datacenters. ACH transmissions are available through FedLine VPN appliances at both datacenters. Both datacenters include redundant communications, redundant firewalls, redundant power (utility, UPS, generator) and are monitored 24x7. An independent CRAC (Computer Room Air Conditioner) is provided to maintain optimal temperature and humidity. Physical access security and video surveillance is also provided.

In the event the host (PROD) at the primary datacenter is not available, a manual process is initiated to “rolover” or “swing” production to the host (HA) at the secondary datacenter. This manual process includes several data integrity checks and audits and a carefully orchestrated sequential process to bring subsystems up on the stand-by host. The rolover process also includes procedures to redirect client credit unions to the secondary datacenter and to backup EFT vendor communications if necessary.

Performing a core-processing rolover involves several teams. The rolover technical process is primarily managed and performed by staff at Site-Four with the assistance from CU*NorthWest and CU*Answers Network Services for DNS, routing, and firewall modifications. *See “HA Rollover Procedures” section below.

Communications to affected third party vendors is handled by Site-Four while communications to clients and affected stakeholders is handled by staff at CU*NorthWest (see “Crisis Communications” section).

The rolover process may require up to 3 hours or more (to ensure data integrity, system stability, and vendor availability) depending on the circumstance of the incident. For short-term disruptions or those during non-business hours, the Incident Manager may determine that a rolover is not a practical solution.

The following identifies the procedures required to perform a typical rolover process. Circumstance involved in any particular incident may require modifications to the procedure list. High Availability rollovers are performed regularly offline and online to validate procedures and test our capabilities for successful completion.

Reports published following scheduled rolover events can be viewed at:

<http://cunorthwest.com/disaster-recovery-and-audits/> for content and additional information

HA Rollover Test Procedures:

One week prior to rollover test: (procedures performed by Site-Four unless otherwise noted)

[PROCEDURES - CONFIDENTIAL]

HA Rollover Test Procedures: (procedures performed by Site-Four unless otherwise noted)

[PROCEDURES - CONFIDENTIAL]

Verify Third-Party Connections/Subsystems: (procedures performed by Site-Four unless otherwise noted)

[PROCEDURES – CONFIDENTIAL]

<u>ROLL OVER</u>			<u>SPOT CHECK #1</u>			<u>SPOT CHECK #2</u>			<u>ROLL BACK</u>		
3rd Party	Time	Init	3rd Party	Time	Init	3rd Party	Time	Init	3rd Party	Time	Init
COP			COP			COP			COP		
FIS			FIS			FIS			FIS		
FSV			FSV			FSV			FSV		
FTH			FTH			FTH			FTH		
STR			STR			STR			STR		
VIS			VIS			VIS			VIS		
LAN			LAN			LAN			LAN		
PEM			PEM			PEM			PEM		

Vendor Contacts for Third Party EFT Rollover Support

[CONTACTS – CONFIDENTIAL]

Overview of DR strategy (in case HA is not an option)

In the event the host (PROD) at the primary datacenter is not available, a manual process is initiated to “rollover” or “swing” production to the host (HA) at the secondary datacenter. If the rollover process is unsuccessful or if circumstances of the incident are such that the rollover process is impossible or induces increased risk, a host recovery from tape may be necessary. Note that a recovery from tape may require 24-48 hours or more before services are restored. This would be considered a disaster scenario.

Host recovery from tape would include “wiping” one of the two hosts, installing the IBM operating system, CU*BASE environment and member libraries. This host recovery effort would be performed by staff at Site-Four with the assistance from technical staff at CU*NorthWest and CU*Answers.

Procedures for recovering PROD is maintained by Site-Four. Procedures for recovering IBM I on the same or different host is available from the IBM web site at: [*Systems Management: Recovering your System*] SC41-5304-10

<http://pic.dhe.ibm.com/infocenter/iserics/v7r1m0/topic/rzarm/sc415304.pdf>

During a recovery effort, it is important that all stakeholders involved in the recovery or affected by the disruption are notified. Please see “Crisis Communications” section for more information.

Third Party Vendor Communications

Primary data communications for third party EFT vendors are available through the network at Site-Four in Yankton, SD. In the event of an outage at Site-Four, backup data communications are available for most vendors through the network at the CU*Answers datacenter in Kentwood, MI.

Backup third party communications connectivity is tested during high-availability rollover exercises.

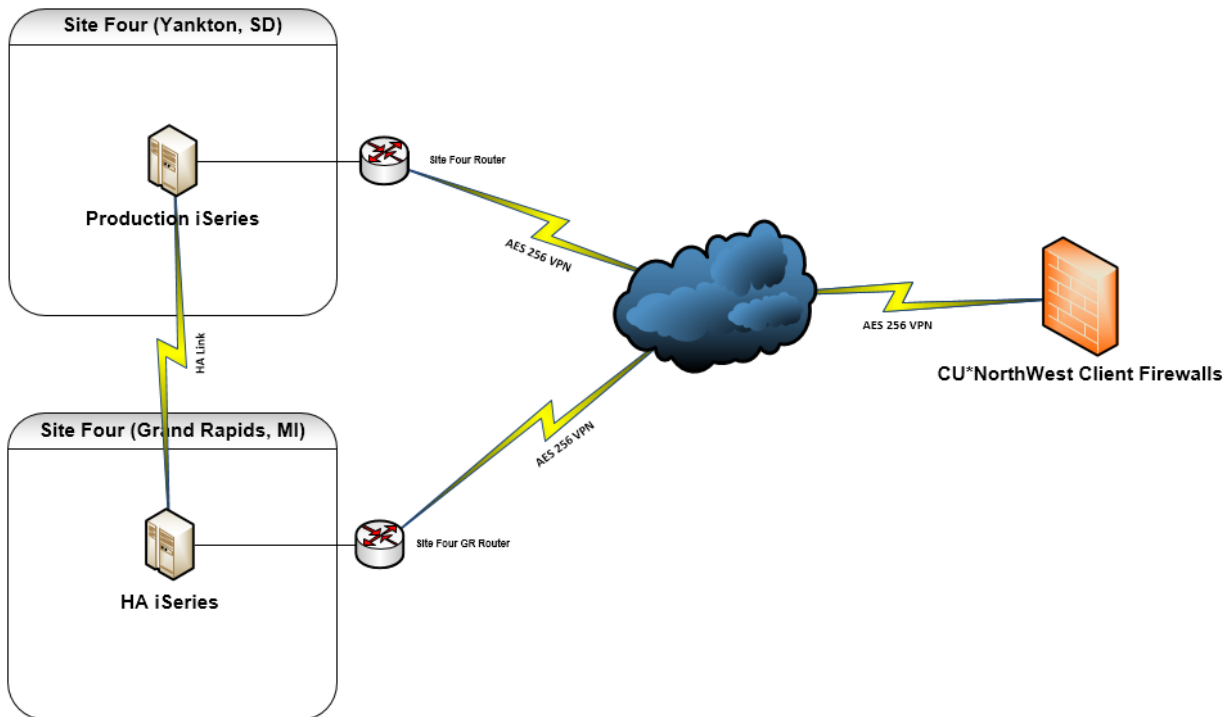
The table below lists the third-party EFT vendors and available data communications. Contact information for each is available in the “Appendix” and “HA Rollover Procedures” section of this plan.

Vendor	Client or Server	Primary Link (Yankton)	Secondary Link (Kentwood)
[CONFIDENTIAL]	Server	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	Server	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	Server	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	Server	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	Server	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	Server	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	Client	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	Server	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]		[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	Server	[CONFIDENTIAL]	[CONFIDENTIAL]



Client Network

Client credit unions have primary data communications through Internet VPNs to the Site-Four datacenter in Yankton, SD with backup VPN connections at the Kentwood datacenter. Several client credit unions have deployed redundant communications through multiple ISPs. Client connectivity is monitored and supported by CU*NorthWest and CU*Answers Network Services 24x7. Management of the ISP connections at each client site is the responsibility of the client. Clients with redundant ISP connections are configured for auto-failover in the event of a disruption.

During HA rolover events, clients are routed to the secondary datacenter through DNS configuration changes and firewall network address translation rules, implemented and maintained by Site-Four.



[The image above shows a typical client credit union VPN connection for the purpose of accessing CU*BASE/GOLD and complementary products provided by CU*NorthWest.]

Externally Monitored VPN-Concentrators (VPN-Concentrators-External)				Externally Monitored VPN-Concentrators (VPN-Concentrators-External)			
Host	Status	Services	Actions	Host	Status	Services	Actions
vpn-	UP	1 OK	 	vpn-	UP	1 OK	 
vpn-	UP	1 OK	 	vpn-	UP	1 OK	 
vpn-	UP	1 OK	 	vpn-	UP	1 OK	 
vpn-	UP	1 OK	 	vpn-	UP	1 OK	 
vpn-	UP	1 OK	 	vpn-	UP	1 OK	 
vpn-	UP	1 OK	 	vpn-	UP	1 OK	 
vpn-	UP	1 OK	 	vpn-	UP	1 OK	 
vpn-	UP	1 OK	 	vpn-	UP	1 OK	 
vpn-	UP	1 OK	 	vpn-	UP	1 OK	 
vpn-	UP	1 OK	 	vpn-	UP	1 OK	 
vpn-	UP	1 OK	 	vpn-	UP	1 OK	 
vpn-	UP	1 OK	 	vpn-	UP	1 OK	 
vpn-	UP	1 OK	 	vpn-	UP	1 OK	 
vpn-	UP	1 OK	 	vpn-	UP	1 OK	 
vpn-	UP	1 OK	 	vpn-	UP	1 OK	 
vpn-	UP	1 OK	 	vpn-	UP	1 OK	 

[The image above shows a sample screenshot of the 24x7 monitoring by CU*Answers Network Services.]

IT Recovery

Overview of IT environment

To provide the wide-range of products and services to client credit unions in a secure environment with optimal performance and availability, a complex arrangement of networks, communications, systems and appliances is required. The image below shows the relationships between the locations identified in previous sections including: Greenstone Office, Site-Four, and CU*Answers.

[NETWORK DIAGRAM – CONFIDENTIAL]

In addition to the High Availability and Disaster Recovery procedures identified earlier, the following highlights recovery of the remaining critical IT components including:

- Voice/Data Communications
- Non-core processing systems (file/print servers, etc.)
- LAN components (workstations, printers, etc.)

The CU*NorthWest network is monitored and managed by CU*Answers Network Services. Replacement equipment is available through CU*Answers.

Loss of Data Communications

ISP and MPLS communication lines at the Kentwood datacenter are owned and managed by Site-Four.

The following data communications lines are owned and managed by CU*NorthWest at the Greenstone office location:

Internet Service Provider: [CONFIDENTIAL]

- Bandwidth: [CONFIDENTIAL]
- Emergency Contact: [CONFIDENTIAL]

MPLS Provider: [CONFIDENTIAL]

- Bandwidth: [CONFIDENTIAL]
- Emergency Contact: [CONFIDENTIAL]
- Account# [CONFIDENTIAL]

Loss of Telephone Service

The loss of service may be attributed to several features of the CU*NORTHWEST Phone Network. Qwest provides all local service. The internal phone network, extensions, call transfer, voice mail, CU*TALK are controlled by redundant computers running the Interactive Intelligence IP Telephony software at the CU*Answers location in Michigan. Qwest supports the inbound 800 service.

Loss of Inbound 800 Service

All of the inbound calls coming into CU*NORTHWEST 866 number (866-922-7646), are routed through an inbound

connection from [CONFIDENTIAL], converted to SIP, and routed to our [CONFIDENTIAL] phone system. The service is supported by [CONFIDENTIAL], our contact when trouble shooting this type of problem or making changes or moves is listed below. In the event of a disaster, our numbers can be rerouted to CU*Answers. See the Appendix F for further information.

[CONTACT - CONFIDENTIAL]

To forward line remotely:

[PROCEDURES - CONFIDENTIAL]

Internal IT Contingency Plans (non-core-processing)

There are several servers and appliances installed on the LAN to perform daily business functions that are not categorized as “core-processing”.

Internal servers are monitored and managed by CU*Answers Network Services. Each server is backed up using the DataBP solution to a local appliance and replicated to an appliance at CU*Answers. In the event a server is unavailable; the server can be recovered as a virtual machine on the appliance until the hardware can be repaired or replaced.

Instructions for restoring file/print servers archived using the DataBP solution can be viewed at:

[PROCEDURES - CONFIDENTIAL]

Configuration files for critical network devices such as firewalls, routers, and switches are archived and managed by CU*Answers Network Services.

[PROCEDURES - CONFIDENTIAL]

[APPLICATION LIST - CONFIDENTIAL]

[NETOWRK DIAGRAM - CONFIDENTIAL]

[The image above shows the Greenstone Office LAN]

PC/Workstation Build Checklist

[PROCEDURES - CONFIDENTIAL]

Business Recovery

A disruption that imposes the relocation of IT systems and/or staff to another area within the facility or to an alternate/temporary facility can be the result of several scenarios such as:

- Loss of service (HVAC, communications, power) is expected to last several days
- Loss of access or physical damage to the structure (fire, water, flying debris, other)
- Large-scale renovation project (planned)
- Hazardous material spill (quarantine)

Recovery steps include:

- Conducting an initial assessment of outage to determine the duration and scope of the event and business functions to resume
- Identifying alternate facilities and arranging for operations
- Notifying employees and providing instructions on where to report and when
- Determining if alternate skilled staff is required for the recovery effort
- Swinging communications to an alternate site (if needed)
- Retrieving records, supplies and resources required to resume operations from off-site
- Determining the impact of the work in process at the time of the disaster
- Determining materials needed (Office and IT equipment)
- Approving and arranging for purchases
- Setting up shipping/receiving operations for the facility (UPS, FedEx, USPS, etc.)
- Ensuring security of assets and safety of staff at each location (physical access, video surveillance, lighted parking lot, etc.)
- Coordinating the repair and restoration of the disaster site

Office workspace recovery options include:

- Relocating to an alternate space/floor within the same building (if damage is contained to small area and access to building granted)
- Working remotely from home, a hotel or a conference room (assuming SSLVPN access is available)
- Leasing equipped work-recovery-area services (dedicated, shared, mobile)
- Working from client main or branch office (See Alternate "Recovery Locations" section below)
- Securing available commercial space from landlord (Greenstone)

Office workspace recovery requirements include:

- Workstations (monitor, mouse, keyboard, scanners)
- Power distribution units, lighting
- Desk, table, chair
- Printer, copier, fax, shredder, phone
- LAN, switch, cables
- Paper, envelopes, blank checks,
- Extra cell phone chargers
- Whiteboard, markers, easel, flipcharts
- Pens, pencils, staplers, paperclips

Alternate Recovery Locations

Alternate Emergency Operations Center (EOC) locations.

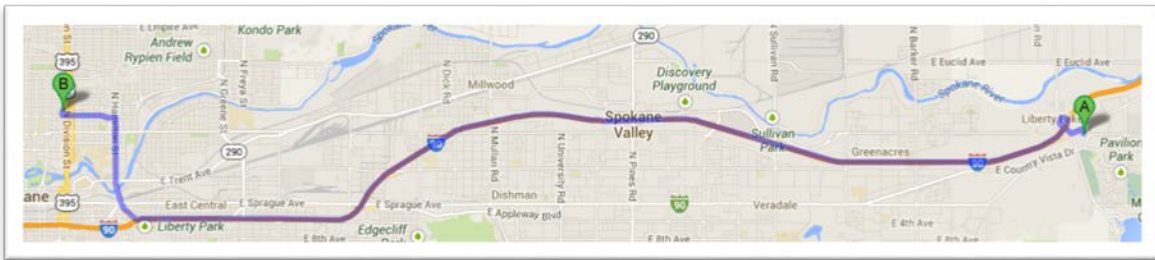
In the event that the Greenstone Offices are not available, an agreement has been made with Spokane Firefighters Credit Union to provide recovery workspace and resources to coordinate the recovery effort and perform critical business functions. The decision to send to alternate recovery location(s) will be determined by the Incident Manager or a member of the Emergency Management Team based on circumstances of the event.

*See "Establishing Command and Control" section for more information.

Several personnel have remote access capabilities to either SSLVPN appliances at the Greenstone Office or the CU*Answers location. In a disaster scenario, CU*Answers Network Services personnel can quickly activate any CU*NorthWest employee who does not currently have remote access capabilities.

CU*Answers Network Services: [CONFIDENTIAL]

Spokane Firefighters Credit Union (approx. 20-minute drive)
[CONFIDENTIAL]



[Directions from Greenstone Office to Spokane Firefighters Credit Union shown above]

This location provides [CONFIDENTIAL] with network access and a 12-person board room for an acting Emergency Operations Center.

In the event Spokane Firefighters Credit Union is not available, other optional recovery locations include:

- Cheney Federal Credit Union (approx. 35-minute drive)
 - [CONTACT - CONFIDENTIAL]
- Prime Source Credit Union (approx. 25-minute drive)
 - [CONTACT - CONFIDENTIAL]

Crisis Communications

In a crisis situation, communication can make or break a complex recovery effort. It is important that internal stakeholders are informed of the situation and know what is expected of them (where to report and when) and that external stakeholders are made aware of the (potential) disruption to business functions and services.

Crisis communications must begin early in the recovery process beginning with notification of recovery teams, and continue through the event until business has returned to normal.

Communications to external stakeholders during a crisis situation is best performed by a trained and/or experienced media spokesperson.

With effective crisis communications:

- Employees feel reassured
- Stakeholders feel confident in the response
- Media reports are accurate

Communications in a crisis is all about who, what, when and how.

- Who?
 - Staff (and their families), board of directors, members, vendors, service providers, emergency personnel, media, local/state/federal agencies, etc.
- What?
 - A carefully constructed message that generates confidence and assurance
- When?
 - Timing and frequency of the message throughout the disruption
- How?
 - Which communications channel to use for each group (email, phone, fax, web, etc.)

Key stakeholders

Circumstances with each crisis scenario will determine who needs to be contacted and when. Stakeholders can be categorized as internal and external, each requiring unique message content.

Key stakeholders include:

- Internal audiences such as
 - Employees, and family members
 - Corporate management
- External audiences such as
 - Credit union members,
 - Vendors,
 - Partners,
 - Regulators
 - Media including
 - Print,
 - TV,
 - Radio,
 - Web
- See “Appendix” for contact information

To internal stakeholders consider stating:

- Facts about the situation

- The response initiated by management
- Ways employees can report to their managers
- Employee assistance programs offered
- How the event might affect operations over subsequent days

To external stakeholders consider stating:

- Facts about the situation
- What the Credit Union is doing to resolve the incident and what each stakeholder can expect as a result of the incident (how it may affect them)
- Expected duration of the event
- Open issues that management continues to investigate

Communicating in a crisis

All questions from the news media or others regarding the Plan or any disaster should be directed to the Incident Manager or CEO.

Methods of communication include:

- Email (corporate or personal)
- Instant messaging or phone texting
- Credit Union corporate web site
- Social media tools such as Facebook, Twitter, LinkedIn, Skype, WebEx, etc.
- Phone (voice)
- Press conference
- Press release (print)
- Fax

Creating holding statements, which are pre-written statements for use in a variety of crises such as natural disaster, fire, explosion, public health emergency, and workplace violence incident, helps ensure that all relevant information is provided quickly and accurately.

Holding statements should identify the primary audience, the optimal delivery time, suggested method of delivery, as well as who should/should not deliver the message. Also, expect and be prepared for follow-up questions.

Key points to remember during and after the incident

- Remind employees that only media-trained personnel should speak to the media.
- Weigh the desire for information against the need to issue a statement.
- You will not know everything immediately.
- Give them what they need to know in the most appropriate method possible.
- Update the status often, even if there is no material development. This helps those connected feel they are in the loop on key details.
- Keep the information fresh and frequent (minimize waiting time between comments).
- Realize that the media is one of your best resources.

Publishing CU*BASE Alerts

[PROCEDURES - CONFIDENTIAL]

Appendix

CU*NorthWest Staff Emergency Contact Information

(Updated as of 02/06/2017) Staff Emergency Contact Numbers			
Please keep a copy accessible at home or on your cell.			
Name	Extension	Home Phone	Mobile
[CONTACTS - CONFIDENTIAL]			

Board of Directors

Board Member	Credit Union	Contact	Term
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]

Stockholders

[CONTACT LIST - CONFIDENTIAL]

Vendors and Service Providers

Vendor Name	Contact	Phone Number	Email Address
	[CONTACTS - CONFIDENTIAL]		

CUNW Voice and T1 Lines

[LIST and CONTACTS - CONFIDENTIAL]