**Disclaimer**

This sample policy provides a guide or a place to begin. Credit union policies should always be structured to meet the specific needs of the credit union and its membership. Efforts are made to update the material to reflect applicable changes in the law. This sample should not be considered legal advice nor relied upon as a substitute for professional services.Credit unions are encouraged to contact legal counsel for legal advice. The Kansas Credit Union Association will not be liable for any direct, indirect or consequential damages resulting from the use of this policy.

**Disaster Recovery Plan**

**A Guide for Developing Your Credit Union**

**Disaster Recovery Plan**

TABLE OF CONTENTS

Important Contact Numbers..................................................................................... 3

General Overview

Purpose.................................................................................................................... 4

Planning................................................................................................................... 4

Implementation........................................................................................................ 4

Training.................................................................................................................... 4

General Public Relations......................................................................................... 6

Elements of the Plan................................................................................................ 7

Risk Assessment

Risks........................................................................................................................ 8

Evaluation................................................................................................................ 8

Insurance Coverage................................................................................................. 8

Security

Physical Protection.................................................................................................. 9

Cash Protection....................................................................................................... 9

Internal Controls....................................................................................................... 10

Record Retention and Off-Site Storage

Record Retention Guidelines................................................................................... 11

Off-Site Storage Requirements................................................................................ 15

Expenses

Disaster Recovery Planning for Expenses............................................................... 17

Alternative Disaster Recovery Strategies

Data Processing System.......................................................................................... 18

Reciprocal Agreements............................................................................................ 18

Hot Sites.................................................................................................................. 18

The Disaster Recovery Period

Management Team Duties....................................................................................... 19

Disaster Recovery Team......................................................................................... 19

Evacuation Plan....................................................................................................... 20

Damage Assessment............................................................................................... 22

Notifying the Authorities........................................................................................... 23

Critical Operations Restoration................................................................................ 24

Testing

Types of Testing...................................................................................................... 27

Parallel Testing........................................................................................................ 28

Disaster Recovery Plans for Specific Disasters

Natural Disasters......................................................................................................30

Fire........................................................................................................................... 30

Tornado.................................................................................................................... 30

Snow........................................................................................................................ 31

Flood........................................................................................................................ 31

Human Activity......................................................................................................... 32

Medical Emergencies............................................................................................... 33

Conflicts of Interest.................................................................................................. 34

Employee Theft........................................................................................................ 34

Embezzlement......................................................................................................... 35

Robbery................................................................................................................... 35

Suspicious Activity................................................................................................... 37

Bomb Threats.......................................................................................................... 38

Extortion/Kidnapping................................................................................................ 39

Management Succession Policy.............................................................................. 40

Financial Threats..................................................................................................... 42

Liquidity.................................................................................................................... 42

Insolvency................................................................................................................ 42

Legal Action Against the Credit Union......................................................................43

Sponsor Company Related Actions......................................................................... 43

Utility Failure............................................................................................................ 45



IMPORTANT CONTACT NUMBERS

Police/Fire Department/Medical Emergency 911

Name of credit union \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Physical Location \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Hospital \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Police Station \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Poison Control Center \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

American Red Cross \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

FBI

Kansas Bureau of Investigations

Kansas Credit Union Association - 800-362-2076

Kansas Department of Credit Unions - 785-296-3021

Kansas Corporate Credit Union – 800-721-2677

CUNA Mutual Insurance Society (CUMIS) 800-637-2676

NCUA - 678-443-3000

Data Processor

Disaster Response \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Power Company \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Telephone Company\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

GENERAL OVERVIEW

#### Purpose

Disruption of a credit union’s operations for an extended period of time could be disastrous for the credit union and its members. It is imperative that plans be developed to minimize disruptions of service to members, to minimize financial loss, and to ensure timely resumption of operations.

# Planning

The first step in creating a Disaster Recovery Plan is commitment from the Board and credit union management to develop the plan. The credit union leadership should appoint a group to oversee the development of the plan.

The next step in developing a Disaster Recovery Plan is assessing each risk to the credit union and the impact on its services. Risks to the credit union are divided into four types of events: natural, technical, economic, and people-based events. Disaster Recovery Planning identifies potential causes of loss and designs a plan of action to minimize disruptions from those events. The proper preparation of a Disaster Recovery Plan will require the analysis of every aspect of the credit union’s operation. Each critical service that the credit union offers should have alternative means of delivery. This requires an inventory of credit union assets and human resources to determine what is necessary to support those critical operations. Some of the credit union’s critical operations include administrative, personnel, automated clearing house transactions, share draft processing, teller operations, loans, accounting, and data processing.

# Implementation

The strategies and procedures for the Disaster Recovery Plan should be documented. The different recovery procedures should also have pre-established priorities to separate critical from lesser priority operations. The Disaster Recovery Plan should be presented to the credit union’s Board of Directors for approval after it passes review by senior management.

There should be an appointment by credit union management of a Disaster Recovery Team, alternate Disaster Recovery Team members, a Disaster Recovery Team Coordinator, and a backup Disaster Recovery Team Coordinator. The alternative methods of providing the credit union’s services should be established through written back-up agreements. There should be off-site storage of vital records and credit union policies and procedures (including a copy of the Disaster Recovery Plan). The Board of Directors should also authorize a Disaster Recovery Budget.

**Training**

The proper training of the credit union’s staff and those who will be involved in the execution of the Disaster Recovery Plan is essential. Training will prepare each employee for their specific tasks. Practice will enable them to perform efficiently, especially in the more technical areas such as data processing.

# Testing

The Disaster Recovery Plan must be tested annually. This test must be as realistic as possible so that the disaster simulation will locate any shortfalls. It will be much easier and less costly to locate shortfalls of the Disaster Recovery Plan during the testing phase rather than actual implementation of the plan.

# Updating

The Disaster Recovery Plan should be updated with any new corrective measures after testing. Each update of the Disaster Recovery Plan should be approved by the Board of Directors and noted in the minutes. In addition, the Board of Directors should delegate the responsibility for semi-annually reviewing and updating the Disaster Recovery Plan to an appropriate volunteer or credit union employee, to assure that the plan is maintained.

# Confidentiality

CUMIS Risk Management recommends that a “confidentiality warning” and a “statement of confidentiality” be included on the cover page of any Disaster Recovery Plan. This is due to the sensitive nature of the information contained in Disaster Recovery Plan.

**Elements of the Plan**

1. Purpose
2. Risk Assessment
3. Disaster Recovery Team
4. Team Assignments
5. Notification Process
6. Procedures
7. Testing
8. Staff Training

**General Public Relations Information**

The following outline will assist management and the Board in developing a public relations plan for handling a crisis.

1. List all problem situations that could occur.
2. Problem situations could include, for example:
3. Sudden death of key employee
4. Financial failure
5. Robbery, kidnapping, embezzlement, bomb threat
6. Fire, flood, tornado
7. Sponsor going out of business
8. Legal action against the credit union
9. General economic crisis
10. List all potential solutions to the problem.
11. Prepare a plan of action for each crisis.
12. Determine general response to media about the problem.
13. Evaluate general response and method of communication to the membership.
14. Keep your staff informed.
15. Adopt a general script for simple inquiries to staff and volunteers. Appoint one person as an official credit union spokesperson for all other (more complicated) inquiries.

###### Media Contact List

Keep a list of current media contacts within the credit union’s membership area.

#### Local Newspaper

#### Radio

#### Television

**General Information Sheet**

A general information sheet that contains vital statistics and information about the credit union should be prepared and updated periodically. At the time of a crisis, or inquiries from the media, the information will be available.

#### Handling Rumors

The nature of a rumor and its potential impact on the credit union will determine the appropriate response. Sometimes a rumor may be handled without a lot of attention or focus drawn upon it. The individual(s) making the statements may be approached in a diplomatic manner and presented with the real facts concerning the situation. If other members or staff overheard the rumor, they may be reassured that the statement did not accurately reflect the situation. Diplomacy is the key. It is unwise to attempt to diffuse a rumor with accusations or negative statements made about an individual who started the rumor.

#### Widespread Rumors

If many people have access to the rumor, it will only be a matter of time before members, staff, and the credit union’s officials become aware of it. You can use memos, direct mail letters, newsletters, and staff briefings to communicate positive and truthful information. Another positive method of minimizing rumors is to emphasize the positive aspects of credit union membership.

These are:

1. Ownership by the members

2. Democratic control by the members

1. The credit union exists to serve the financial needs of its members
2. The credit union is safe, strong, and insured
3. The credit union movement is a worldwide credit union network

#### Assistance

Contact the Kansas Credit Union Association for assistance.

**RISK ASSESSMENTS**

#### Risks

The various risks that can cause a disaster should be examined by the credit union. Once these risks have been identified, the credit union can plan how to effectively manage each crisis event. The severity of the event would determine the amount of the damage to the credit union. The amount of damage can range from total destruction to a minor inconvenience. Massive destruction may necessitate implementation of the entire Disaster Recovery Plan, but a lesser percentage of destruction may necessitate the implementation of only a portion of the Disaster Recovery Plan. Risks to the credit union are divided into four types of events: natural, technical, economic, and people-based events.

The risk from the human element should be reviewed as well. The risk to the credit union from people ranges from threat of war, riots, robbery, sabotage, hostage taking, strikes, oil or toxic substance spill, and medical emergencies.

# Risk Measurement and Evaluation

The risk assessment process begins with identification, measurement, evaluation, and control or reduction of potential risks. The risks should be analyzed on two different levels: the frequency of occurrence and severity of damage this event would have on the credit union. NCUA requires that each risk to the credit union have a Disaster Recovery Plan set forth in case of a disastrous event. Since risk assessment is a subjective process it is exceptable to categorize the likelihood of occurrence and the severity of specific events as approximations.

The risk assessment process may identify material risks that are not covered under present insurance protection. For any probable uninsured risk of material severity, it would be prudent to obtain additional insurance coverage to avoid financial risk to the credit union.

# Review of Insurance Coverage

Insurance coverage should be extensively reviewed for adequacy during a possible disaster recovery period. Extra expenses, data processing, flood, and personal property are examples of what should be discussed with the credit union’s insurance agent. Another frequent insurance coverage shortfall is the credit union failing to increase insurance coverage after the purchase of major items (such as computers, equipment, or ATMs) or after opening a new branch office. The insurance coverage should always be maintained for changing internal and external conditions.

**CREDIT UNION SECURITY**

#### Security

The most important purpose of any security program is the prevention of a loss or to minimize any foreseeable loss. All credit unions should already have a written security program as required by Section 748 of the NCUA Rules and Regulations. The written security program provides for the protection of the credit union’s assets. A security officer should be appointed to oversee the security program.

The premises of the credit union should be adequately protected from the probable hazards identified earlier in the risk analysis. The protective measures should be subjected to a cost-benefit analysis for cost effectiveness. The protective measures should be especially targeted to the human-based threats identified earlier in the risk analysis. This includes risks such as data entry errors, robbery, embezzlement, sabotage, and other crimes that must be safeguarded by adequate security and internal control measures.

# Physical Protection

1. The credit union should be well illuminated and patrolled during hours of darkness.
2. Records should be stored in a fireproof storage area or cabinet.
3. The credit union should have an adequate alarm system, surveillance system, and secure locks.
4. The credit union should have an adequate number of fire extinguishers that are properly maintained.

#### Cash Protection

1. Reasonable minimum and maximum currency needs should be established.
2. The vault should not be visible from outside the credit union office.
3. Funds should be transported between the credit union and the bank using two employees, security guards, or security personnel.
4. Negotiable securities should be under dual-access control and stored in the vault.
5. Each teller and vault should have bait money and bait money records must be accurate.
6. Surprise cash counts should be conducted by credit union management and/or supervisory committee.
7. Each teller should have sole access to the cash and negotiable item supply assigned to him.
8. Bank account reconcilement(s) should be accurate and current.

**Internal Controls**

1. More than one employee should be utilized in a transaction when possible.
2. It should be a policy to have annual vacations and require all employees to take at least 5 consecutive days each year.
3. Closed and dormant accounts must be properly controlled.
4. Insurance proceeds disbursed to members should be verified during audits.
5. Account verifications should be accomplished on an annual basis.
6. General ledger accounts should be reconciled to statements generated outside the credit union on a monthly basis.
7. Adequate audit trails must be available for follow-up activity.

# Computer Controls

1. Access to the computer area should be restricted.
2. Computer’s data should be backed-up on a timely basis (at least daily).
3. The data processing procedures should be well documented in a manual.
4. The confidentiality of access codes and passwords should be adequately protected.
5. Unapplied exceptions and other suspense items (such as data entry errors) should be promptly investigated and corrected.

**RECORD RETENTION AND OFF-SITE STORAGE**

The vital records of the credit union must survive a disaster for the Disaster Recovery Plan and recovery process to be workable. Backup copies of records must be made and transferred to off-site storage on a timely basis.

# Record Retention Requirements

Record retention for credit unions is required by Section 749 of the NCUA Rules and Regulations, the Kansas Credit Union Act, the Bank Secrecy Act, Regulation CC (Funds Availability Act), Regulation C (Home Mortgage Disclosure Act), Regulation E (Electronic Funds Transfer Act), Regulation B (Equal Credit Opportunity), and Regulation Z (Truth-In-Lending).

The chief financial officer (usually the treasurer) of the credit union is responsible for storing duplicate vital records at a vital records center. This responsibility may be delegated by the chief financial officer to another person.

Summary of Record Retention Periods – Revised 12/2006

**The following Record Retention and Disposal Guideline is provided by the Kansas Department of Credit Unions to assist credit unions in determining minimum retention periods for certain types of books and records. However, if a credit union is required by other applicable law, rule, or regulation to retain a record for a longer period of time, the credit union must comply with that longer retention period. t should be recognized that this Guideline is not all-inclusive. Where additional records and retention periods are required by other applicable law, rule or regulation, the credit union must comply with that requirement and retention period.**

**I. GENERAL RECORDS**

***A. ADMINISTRATION***

|  |  |
| --- | --- |
| 1. Charter, By Laws and amendments | \*Permanent |
| 1. Minutes of Annual meetings | Permanent |
| 1. Minutes of Director’s meetings | Permanent |
| 1. Minutes of Credit Committee meetings | Permanent |
| 1. Deeds, Abstracts, Title Insurance etc. to credit union property | \*Permanent |
| 1. Certificate of Share Insurance | \*Permanent |
| 1. Certificates or licenses to operate from government agencies (HUD, Savings Bonds, IRA, etc.) | \*Permanent |
| 1. Lists of officers and oath of office | 7 Years |
| 1. Abandoned property: escheat reports | Permanent |
| 1. Lists of all records destroyed | Permanent |
| 1. Off premises record preservation log | Until superseded |
| 1. Current manuals, circular letters and other official instructions of a permanent nature received from KDCU or other appropriate government agencies | Until superseded |
| 1. Copy of each 5300 Call Report | 5 years |
| 1. Reports of Examination | 5 years |
| 1. 1099 listing, summary | 3 Years |
| 1. Security program and log | Until superseded |
| 1. Audit reports and record of account verification | Permanent |
| 1. W-9 Form | 4 Years |
| 1. Suspicious Activity Report (NCUA 2362) | 5 Years from date of report |
| 1. Court Orders | 7 Years |
| 1. Power of Attorney | 15 Years after expiration |

***B. INSURANCE, INVENTORY AND PROPERTY***

|  |  |
| --- | --- |
| 1. Inventory of furniture and equipment and depreciation schedule | 2 Years after disposal of furniture and equipment or fully depreciated |
| 1. Bond (premium receipts and Dec. page) | Current and last years |
| 1. Insurance policies | 2 Years after expiration of coverage |
| 1. Insurance coverage report | Current and last years |

***C. COMPLIANCE REGULATIONS***

|  |  |
| --- | --- |
| 1. Evidence of Reg. B compliance | 25 Months |
| 1. Evidence of Reg. E compliance | 2 Years |
| 1. Evidence of Reg. Z compliance | 2 Years |
| 1. Evidence of Reg. CC compliance | 2 Years |
| 1. Evidence of Reg. DD compliance | 2 Years |
| a. Civil Actions | 7 Years |
| 1. Evidence of Reg. C compliance (HMDA) |  |
| a. Complete register | 2 Years |
| b. Public disclosure statement | 5 Years |
| 1. Evidence of Fair Credit Reporting Act compliance | 7 Years |
| 1. Evidence of Reg. X (RESPA) compliance | 2 Years |
| 1. Large currency transaction form 4789 | 5 Years |
| 1. Management certification of compliance with Bank Protection Act | 3 Years |
| 1. Evidence of BSA/OFAC policies and compliance | Yearly |
| 1. IT – 748 Compliance | Yearly |

**II. MEMBERSHIP RECORDS**

|  |  |
| --- | --- |
| 1a. Open account  Signature and beneficiary cards | Retain revised signature and beneficiary cards 7 Years from date of revision |
| 1b. Closed account  Signature and beneficiary cards | 7 Years from date account closed |
| 1. Individual share and loan ledgers | 7 Years |
| 1. Periodic statements (data) | 7 Years |
| 1. Payroll deduction authorization | 5 Years after expiration |
| 1. Court orders, judgments & releases of member's accounts | 5 Years |
| 1. Membership lists (data) | Until superseded |

**III. LOAN RECORDS**

|  |  |
| --- | --- |
| 1. Loan applications approved or denied | 25 Months or until loan is paid, whichever is greater |
| 1. Loan application denial notice | 25 Months from date of member notification |
| 1. Disclosure statements | 2 Years after date disclosures are required to be made |
| 1. Security agreement | Until loan is paid or collateral is released |
| 1. Financing (UCC-1) statement or verification of vehicle lien | Until loan is paid or collateral is released |
| 1. Real estate mortgage | Until loan is paid, then release |
| 1. Notice of rescission | Until loan is paid |
| 1. Abstracts, deeds, title insurance, insurance policies, etc. | Until loan is paid |
| 9a. Security agreement for property held by the credit union | Until loan is repaid and property returned |
| 9b. Receipt for Return of Property | 7 Years from date of return of property |
| 1. Collateral held by the credit union (stock, C.D.'s, insurance policies, jewelry, guns, etc.) | Until loan is paid or until released. Return to borrower and obtain receipt. |
| 1. Insurance loss payable notices | Until superseded or until collateral is released |
| 1. Borrower's and comaker's credit reports and financial statements | Until loan is paid |
| 1. Credit disability insurance forms | Until loan is paid |
| 1. Home mortgage disclosure register | 2 Years |
| 1. Open End Agreement to Pay | \*Permanent |
| 15a. Canceled open end agreements | 7 Years after canceled |
| 1. Credit committee minutes | Permanent |
| 1. Charged off loans and records | 10 Years |
| 1. Flood insurance certificates | Life of loan |
| 1. Good faith estimates | 6 Years |
| 1. Hazard insurance policies | Life of loan |
| 1. Credit card stop list | 1 Year |
| 1. 1098 data | 5 Years |

**IV. ACCOUNTING FORMS AND RECORDS**

|  |  |
| --- | --- |
| 1. General ledger | Permanent |
| 1. Journal and cash record, and EDP daily proof listing | Permanent |
| 1. Cash received, cash disbursement, and journal vouchers | 5 Years |
| 1. Withdrawal slips | 5 Years |
| 1. Bank statements | 5 Years |
| 1. Canceled checks, void checks, money orders | 5 Years |
| 1. Financial and statistical reports | 5 Years |
| 1. Dividend records | Until next audit and examination |
| 1. Schedule of delinquent loans | 5 Years |
| 1. Expense records and vouchers (paid bills, statements and invoices) | 5 Years |
| 1. Share & loan tapes, EDP trial balance | Until next audit and examination |
| 1. Original of credit union share certificates and certificates of debenture | 5 Years after redemption |
| 1. Bank reconcilements | 5 Years |
| 1. Records pertaining to discrepancies or shortages | 2 Years or until discrepancy or shortage is cleared |
| 1. Charged off asset records | 10 Years |
| 1. Money order registers | 2 Years |

**V. ELECTRONIC RECORDS**

|  |  |
| --- | --- |
| 1. EDP daily proof listing | 5 Years |
| 1. EDP trial balance | Until next audit and examination |
| 1. Year end application back ups | Until replaced |
| 1. System Back ups | 5 cycles + 7 days |

**VI. MEMBER SHARE ACCOUNTS**

|  |  |
| --- | --- |
| 1. Withdrawals | 5 Years |
| 1. Deposits | 5 Years |
| 1. Journal | 1 Year |
| 1. Trial balances, automated or non-automated |  |
| a. If statement or account history  retained | Optional |
| b. If no alternate record | 5 Years |
| 1. Form 1099   a. 1099 listing, summary | 5 Years  3 Years |
| 1. IRA account records | 10 Years after close |

**VII. MEMBER SHARE DRAFT ACCOUNTS**

**U8**

|  |  |
| --- | --- |
| 1. Checks paid (microfilm copy front and back) | 7 Years |
| 1. Stop payment orders | 1 Year after expiration |
| 1. Undelivered statements | 5 Years |
| 1. Daily record of overdrafts | Optional |
| 1. Copies of advices of deposits | 1 Year |
| 6a. Open account  Signature and beneficiary cards | Retain revised signature and beneficiary cards for 7 Years from date of revision |
| 6b. Closed account  Signature and beneficiary cards | 7 Years from date account closed |
| 1. Statement - microfilm | 7 Years |
| 1. Trail balances, automated or non-automated |  |
| a. If statement or account history record retained | Optional |
| b. If no alternate record | 5 Years |
| 1. New and closed accounts | 3 Months |
| 1. Zero balance report | 1 Month |
| 1. Change of Address records | 1 Year |
| 1. Dormant account | Permanent |
| 1. Return item record | 5 Years |

**VIII. SAFE DEPOSIT VAULT**

|  |  |
| --- | --- |
| 1. Access tickets | 2 Years |
| 1. Canceled signature cards | 2 Years after close |
| 1. Copies of rent receipts | 2 Years |
| 1. Leases or contracts, closed accounts | 2 Years after close |
| 1. Correspondence | 2 Years after close |
| 1. Court orders | 7 Years |
| 1. Forced entry records | 6 Years |
| 1. Records and/or contents of drilled box | 6 Years |

**IX. INVESTMENTS**

|  |  |
| --- | --- |
| 1. Documents evidencing investment of funds | 3 Years after close |
| 1. Safekeeping records and receipts | 5 Years after close |
| 1. Broker confirmations | 2 Years |
| 1. Broker invoices | 2 Years |
| 1. Broker statements | 3 Years |
| 1. Descriptive literature on securities disposed of | 2 Years |
| 1. Buy and sell agreement: mortgage backed securities | 2 Years after maturity or sale |

**X. ATM**

|  |  |
| --- | --- |
| 1. Audit tape or Network tape | Permanent |
| 1. Deposit envelopes | 5 Years |
| 1. ATM machine settlement | 3 Years |

**XI. ELECTRONIC FUNDS TRANSFER**

|  |  |
| --- | --- |
| 1. Wire copies or advices | 5 Years |
| 1. Wire transfer debit and credit entries | 5 Years |
| 1. Wire transfer logs | 5 Years |

**XII. PERSONNEL**

|  |  |
| --- | --- |
| 1. Personnel records | 6 Years after termination |
| 1. Affirmative action plan (EEOC) | Permanent |
| 1. Application and resumes approved | 3 Years |
| 1. Application and resumes declined | 6 Years |
| 1. Attendance records | 3 Years |
| 1. Profit sharing plan and records | Permanent |

**XIII. ACCOUNTING CHECKS**

|  |  |
| --- | --- |
| 1. Receipts of cosigned traveler’s checks | 2 Years |
| 1. Reconciliations: traveler’s checks | 2 Years |
| 1. Traveler’s checks sales and inventory registers | 2 Years |
| 1. Stop payments: traveler’s checks | 5 Years |
| 1. Traveler’s checks: agency purchase | 2 Years |

\* **Must be maintained in original form. Other records may be converted to other media for storage after the next examination and audit.**

**Off-Site Storage Requirements**

The vital records center is defined as any location far enough from the credit union’s office to avoid the simultaneous loss of both sets of records (the credit union’s on-site records and vital record storage facility) in the event of a disaster. Caution is urged on not having the off-site storage too far away because the vital records need to be close enough to the credit union to retrieve on a timely basis for the disaster recovery process. An inventory of all credit union records on inventory control cards (with the retention period for each record noted on the card along with the location of each inventory item) should be maintained. These records should also have a timetable for removal from active to inactive storage, date for microfilming, and date of planned destruction. A detailed records transfer list should be maintained for the transfer of these records to off-site storage. The transfer log should contain information on what records were sent, when they were sent, and by which employee. These transfers must be made at a minimum of once every 3 months, within 30 days after the end of the 3 month period. More frequent transfers of vital records are suggested for planning purposes.

In the off-site storage vault, there should be lists of members’ account numbers, addresses, share account and loan (listing multiple loans separately) balances, monthly financial/statistical reports, bank statements, bank reconciliations, insurance policies, and investment records. A copy of the general ledger (and subsidiary records, such as charge-offs and recoveries, accounts payable, escheats, etc.) should be maintained to offer a reconstruction of the credit union’s general ledger activity. Stored records may be in any format that can be used to reconstruct the credit union’s records. Acceptable formats include paper originals, machine originals, microfilm, microfiche, magnetic tape, computer diskette, CD-ROM, etc.

Disaster recovery will necessitate the storage of more information than listed by Section 749 of the Rules and Regulations. An employee list with home telephone numbers should be maintained in case of any emergency. The credit union’s administrative and personnel records should be duplicated and periodically transferred to off-site storage. Complete and current copies of all the credit union’s policies and procedure manuals (including a copy of the Disaster Recovery Plan) should be maintained off-site. Automated clearing house transactions, share draft processing, and automated teller machine records should also be duplicated and transferred off-site. Backups of personal computer data and program files should be made and transferred off-site on a timely basis. Lists of suppliers of materials and services that the credit union uses and other organizational contacts should be compiled.

E**XPENSES DURING DISASTER RECOVERY**

# Need for Extra Expenses

The disaster recovery process can be an expensive period for any credit union. The costs of repairing and replacement of damaged assets could be enormous, even with insurance coverage. The credit union may have to obtain replacements for crucial assets in as short as time as possible, leaving little negotiating time. To aid in the cost containment of these replacement assets, it is recommended that agreements and contracts be pre-negotiated with suppliers of critical assets. A copy of each of the negotiated contracts should be transferred to the off-site storage facility.

# Increased Cash Needs

The extra expenses during the recovery period will increase the cash needs of the credit union. The increased cash needs can be provided for by a line-of-credit at Kansas Corporate Credit Union.

# Furniture, Fixtures, & Equipment Purchase &/or Rental

Since these needs are unknown, the planning process should concentrate on a list of the suppliers of the items on a purchase and/or rental basis.

# Data Processing

The repair, replacement, or possible rental of computers and related equipment should be discussed with the credit union’s supplier of data processing needs. Agreements should be negotiated and a copy of those agreements retained at an off-site storage facility.

# Repairs

Costs of repairs are potentially the total destruction of the credit union’s building site and all its contents. The credit union may have to rebuild its entire operations.

# Incidental Costs

The costs may be individually small but can total to a large material amount for the credit union’s recovery expenses.

# Authorization for Greater Expenses

The Board of Directors should authorize an adequate Disaster Recovery Budget. It should be substantially larger than a budget designed for normal operating conditions. The larger budget gives the credit union the flexibility to restore credit union operations.

**ALTERNATIVE DISASTER RECOVERY STRATEGIES**

Alternative Disaster Recovery strategies for each critical function should be developed. One strategy is to switch to a manual system of operation. Another strategy is to have a critical operation completed by an outside service (such as bookkeeping, payroll, or data processing). Other alternatives, mostly applicable for data processing (but adaptable to other critical operations), are listed below.

1. **Owned-Backup Facility**

The total data processing system would be duplicated, as a “mirror image”, at a distant area from the present system. This could be a branch operation that would otherwise be equipped with terminals. This option is a low risk but high cost solution.

When transferring to the alternate location care should be taken to protect the equipment at the location of the damage. Determine which team member will be responsible to:

* Unplug all equipment
* Move items from the floor whenever possible to avoid water damage
* Cover equipment and computers with large trash bags to protect from water damage

1. **Reciprocal Agreements**

This is an arrangement between two or more credit unions, in which, all have the same computer system hardware and software. The agreement states that if one credit union’s system fails the agreeing parties use the surviving system. This agreement must be in writing. The computer systems must be maintained as “mirror images,” with each utilizing identical hardware and software. The credit unions should be certain that one surviving computer could handle the processing of all agreeing parties transactions. The unaffected credit union could process their transactions in the usual manner, while the disaster affected party could process their transactions at night (in the usual “on-line” manner or a “batch” process mode). One advantage of reciprocal agreements is that multiple agreements can be signed. Multiple reciprocal agreements would better assure that there would be a surviving computer system in a widespread disaster.

#### Hot Sites

This is a service offered by a computer vendor for a fee to all who choose to subscribe. The subscribing customers have the right to use the “hot site” within 24 hours notice, usually for a period up to 3 months. If there was a widespread disaster or if the “hot site” is needed over 3 months, there could be a problem. A widespread disaster could create too many users that would overload the system or leave some without service. If a credit union needs more than 3 months to recover on their data processing system, other data processing system alternatives may have to be located.

**THE DISASTERY RECOVERY PERIOD**

#### Management Team Duties

The management team has the responsibility of directing disaster recovery efforts through the disaster recovery team. The management team provides the ability of the credit union to rapidly respond with the various components of the Disaster Recovery Plan.

The management team has the following duties:

1. Selecting the disaster recovery coordinator, team, and any sub-committees.
2. Implementing and updating the Disaster Recovery Plan.
3. Maintaining record retention and off-site storage.
4. Deciding on implementing the Disaster Recovery Plan (part or whole).
5. Directing the coordination of business resumption activities.
6. Filing any insurance claims and completing any documentation required.
7. Keeping the members informed.

#### Disaster Recovery Team

The disaster recovery team’s organization is largely determined by the credit union’s complexity of operations and size. In a smaller credit union, one disaster recovery coordinator may be all that is required. In a larger credit union, a disaster recovery team will be required with each member of that team responsible for a critical operation coordinated by the disaster recovery coordinator. Member services (teller and loan operations), accounting, and data processing would all be critical operational areas needing to be coordinated in the recovery process. The disaster recovery coordinator and disaster recovery team should have an alternate or back-up person(s) appointed should the original appointed person be unavailable for their duties. The credit union’s operation may be so complex that a disaster recovery team would be overburdened. In such a case, a sub-committee approach for each critical operation may be necessary. The disaster recovery coordinator while having the key responsibility for disaster recovery should report all activities to the credit union’s management team.

The disaster recovery coordinator will have the following duties should a disaster occur:

1. Determine the scope of the disaster.
2. Report recommendations to the management team.
3. Activate all or part of the Disaster Recovery Plan upon approval of the management team.
4. Evacuate, if needed.
5. Shut down operations, if needed.
6. Coordinate alternate site operations, as required.
7. Oversee business resumption activities.
8. Report all recovery activities to the management team.

###### Evacuation Plan

Each credit union needs to develop an evacuation plan based upon the credit union’s layout and floor plan. Evacuation may be necessary for a number of reasons ranging from bomb threats to fire. The purpose of any evacuation is the timely emptying of the building and safeguarding life and property.

An evacuation plan involves:

1. Pre-evacuation planning.

a. Determine exit routes.

b. Provide well-placed and visible exit signs.

2. Designation of authority to order evacuation.

3. Actual building evacuation.

4. Established security measures.

5. Protect assets.

6. Re-entry to building and resuming normal operations.

7. Training of staff.

#### Protection of Assets

Time is a critical element for determining which procedures to follow prior to an evacuation. A sudden event, such as a tornado, requires the use of common sense in attempting to protect property.

In the case of prior notice in a potential emergency, such as a hurricane, assets can be protected to a much greater extent or moved off-site.

If time does not permit removal of cash, the tellers should be instructed to lock their cash drawer and keep their keys until instructed to release their keys to a supervisor or return to their station.

#### Priorities

The credit union should establish a priority of items to be removed from or properly stored at the credit union’s site prior to the arrival of an impending threat.

*First Priority*: Cash, money orders, traveler’s checks, and securities

*Second Priority:* Essential computer tapes and accounting records

*Third Priority:*  Blank checks and signature stamps

*Fourth Priority:* Loan records, signature and payroll deduction cards, microfilm and microfiche records, management and official credit union records

*Fifth Priority:*  Business equipment, furniture, and fixtures

**Emergency Closing Procedures**

Emergency closing procedures are vital to protect both employees and credit union property.

Emergency Closing procedures include:

1. Designate authority to shutdown operations.
2. Notify staff.
3. Notify members.
4. Specify shutdown procedures for each department.
5. Take adequate security measures.
6. Set-up procedures for re-opening the credit union.

#### Emergency Closure CHECKLIST

An example of a shutdown checklist is provided below:

* Put cash and other negotiable items in vault.
* Place teller transaction records in the vault.
* Put deposit bags in the vault.
* Place loan files in vault.
* Put membership records in vault.
* Place microfiche in vault.
* Shutdown computer system and other electrical devices.
* Turn down the heat.
* Turn lights off.
* Open all drapes and blinds.
* Remove the keys from the check protector.
* Lock vault.
* Set alarm system.
* Exit.

**Damage Assesment**

The assessment of the disaster damage begins with the assembly of the disaster recovery coordinator and other members of the disaster recovery team that are available. It is desirable for the Damage Assessment Team to live nearby the credit union site. The Damage Assessment Team should have a preselected “command post” nearby from which to conduct their operations. The “command post” should be supplied with items such as a copy of the Disaster Recovery Plan, phone service, cleaning supplies, pens and paper, a radio, flashlight, repair tools, and other material deemed necessary. The Damage Assessment Team once they approach the disaster site should first have clearance to enter the damaged credit union building from the local authorities (the building structure may be unsafe). After permission is given, the actual damage assessment can begin, in the steps that follow:

1. A close inspection of the credit union’s premises (building and contents).
2. A precise listing of the damages should be recorded for later reports.
3. Assess the severity of damages. Are damages enough to warrant activation of all or part of the Disaster Recovery Plan?
4. Determine if the damages are repairable.
5. Judge how long the repairs will take.
6. Evaluate how long it will take to resume normal operations.
7. Estimate the cost of the damages.
8. Appraise the condition of the credit union’s records.
9. Report these findings to the appropriate parties.
10. Decide whether a news release is necessary.
11. Evaluate if there are other items warranted by the situation.
12. Tighten security to control the tide of people flowing in and out of the damaged building.

If the credit union has to move, notify:

1. The Post Office.
2. Telephone company and other utilities.
3. The members
4. Kansas Corporate Credit Union
5. State/Federal Regulators.
6. Kansas Credit Union Association
7. Vendors and Suppliers.
8. Insurance Carrier.
9. Bank, if applicable.

#### Notifying the Authorities

The local authorities should be first in the line of those who should be informed about catastrophic events. Police (in the event of kidnapping, robbery, embezzlement, etc.), Fire Department (in the event of fire, oil, chemical, or toxic substance spill), and Rescue (in the event of hurricane, earthquake, tornado, etc.) are a few of the local authorities that would need to be involved in a disastrous situation.

# Federal Authorities

Section 748.1(c) of the NCUA Rules and Regulations states “each ***federally-insured***  credit union will notify the NCUA regional director, the US Attorney, and the Federal Bureau of Investigation within 7 business days of crimes or suspected crimes that occur at its office(s), utilizing NCUA form 2362, Criminal Referral Form. The federally-insured credit union should follow the instructions and reporting requirements set forth on the Criminal Referral Form. Copies of this form have been distributed to all federally-insured credit unions. Additional copies may be obtained by contacting the NCUA Regional Office.”

# NCUA

Section 748.1(b) of the NCUA Rules and Regulations states “each ***federally-insured*** credit union will notify the regional director within 5 business days of any catastrophic act that occurs at its office(s). A catastrophic act is any natural disaster such as a flood, tornado, earthquake, etc. or major fire or other disaster resulting in some physical destruction or damage to the credit union. Within a reasonable time after a catastrophic act occurs, the credit union shall insure that a record of the incident is prepared and filed at its main office. In the preparation of such record, the credit union should include information sufficient to indicate the office where it took place; the amount loss, if any; whether any operational or mechanical deficiency(ies) might have contributed to the catastrophic act; and what has been done or is planning to be done to correct the deficiency(ies).”

# Kansas Department of Credit Unions

The state-chartered credit unions should notify the state credit union division about any catastrophic act.

# Insurance Carrier

The credit union’s insurance agent should be notified as soon as possible about any potential insurance claim, especially those of catastrophic proportions. Before repairs are started, the expenditures have to be authorized by the insurance company. Do not let employees or cleaners throw anything away before the insurance adjusters make their evaluations.

# Credit Union’s Board of Directors

The President of the Board of Directors should be notified about any material disaster to alert the other Directors about possible future Board of Directors action.

# Credit Union Management Team

The credit union’s management team should be alerted because of their role in authorizing and directing the activities of the disaster recovery team.

Note: Depending upon the nature of the catastrophic event, others may need to be notified.

For example:

* The Post Office
* Telephone and other utility companies
* First Carolina Corporate Credit Union
* North Carolina Credit Union League
* The Bank

#### Critical Operations Restoration

The various critical operations identified in the analysis of the credit union’s operation should each be broken down into a separate process with one disaster recovery team member or sub-committee responsible for that operation. The choices for alternate forms of delivery for most of the critical operations are falling back to a manual system, having an “outside service” perform the function (such as bookkeeping or payroll), or establishing an alternate “fully functional” site (such as a “hot site” or reciprocal agreement). A credit union may decide on a combination of several or all of the alternatives (manual, outside service, owned-backup facility, reciprocal agreement, or hot site) in their Disaster Recovery Plan.

# Member Services

Member Services will be dependent upon the progress of the data processing recovery, if data processing is effected. Member Services operation may be required to be put on a manual or batch processing (if available) mode until regular computer operation is restored. Tellers should move to an off-line transaction mode. Extended periods of being down could force the decision to temporally use a manual accounting system until computer operations are restored. The anticipation of the emergency use of a manual accounting system means that the credit union should look into the availability of the manual accounting supplies in their area. Credit unions may decide to store a day or two (or possibly more) supply of manual accounting system supplies at their off-site storage facility.

Tellers will have to use the most current records available to determine availability of the members funds (with guidance from management). The timely transfers of vital records to off-site storage is most important due to the material amounts of member’s balances involved. The tellers should make notations of withdrawal amounts on their hard copy of the account balances. All the tellers’ activity can later be compiled and updated totals computed by the temporary data processing system (or manually). The tellers should obtain authorization on large withdrawals, whose dollar value is to be determined by management, as a means of internal control during the period of computer “down time”. The credit union’s management may consider the use of a dollar limit of teller transactions in case of manual operation. For the credit unions with more than one branch of operation, the coordination of teller transactions may involve calling the main office for approval of each transaction (controls that would normally be automatic on the credit union’s computers). In the case of automatic clearinghouse transactions, automated teller machines, share drafts, and credit cards, the vendor should be contacted in the case of an interruption of each service.

Loans can still be made providing that the disaster has not depleted the credit union’s liquidity. The preservation of loan documents is crucial. Critical operation restoration for loans would depend upon the nature of the disaster and what damage was sustained. The loan documents should be stored in a fireproof cabinet or vault. If original loan documentation is destroyed, copies can be ordered for records such as titles, deeds of trust, and insurance policies of collateral. To calculate loan payments and payback periods during the restoration period, manual calculations with tables or equivalent means can be used.

# Data Processing

The procedures for data restoration differ according to the computer system that the credit union is utilizing. The credit unions utilizing “out-of-house” computer services should develop a Disaster Recovery Plan for data processing should a disaster strike the provider of the “out-of-house” computer service. The credit union should contact the “out-of-house” computer service to inquire about the supplier’s Disaster Recovery Plan. The credit union can then coordinate their Disaster Recovery Plan to the “out-of-house” vendor’s plan. A credit union with an “out-of-house” computer service must have a Disaster Recovery Plan compatible with their computer service vendor’s plan.

The credit unions with “in-house” computer systems should contact their supplier about the effects of a disaster on their system. The possibilities include large-scale repairs, system replacement, and restoration of data. Computer maintenance contracts should be reviewed for adequacy of disaster recovery coverage. Larger credit unions may consider back-up power supplies for the continuation of computer service during a power interruption. Back-up data processing means should be established by one or more methods. An alternate fully functional data processing unit that is not in the same geographical area could be one answer (called a “hot site”) for the credit union. Another method of alternate processing of data during a recovery period is reciprocal agreements. The credit union could set-up a reciprocal agreement (or several reciprocal agreements – for more than one alternative processing site) with a credit union(s) with the same computer system but not in the same geographical area. Copies of these alternate delivery agreements should be retained for examiners and auditors to review for regulatory compliance.

# Accounting

The first step of record restoration is to take the stored records for each specific function and up-date the information. The maintaining of the most current records at the off-site storage facility of the credit union is crucial (such as the member’s accounts). The daily balancing of teller transactions, automated clearing house, share drafts, credit cards, payroll deductions, general ledger and other accounting activity must be continued (even if on a manual basis). Any subsidiary records of accounts such as charge-offs and recoveries, escheats, accounts payable, etc. should be maintained as current as possible during the recovery period. If the credit union’s data processing system is down for an extended period, the use of a manual accounting system may be required. The transfer of the data from printouts to a manual system could be time consuming and should not be attempted if the computer is down only for a short time. The automated clearinghouse, share draft, and credit card activity should be followed-up and reconciled daily. The cost of not reconciling daily could be very high to the credit union. The specific procedure for obtaining the automated clearing house, share draft, or credit card information from the vendor during system problems will have to be handled on a case by case basis with each vendor. Make sure these procedures are in writing and agreed upon by all parties. Accounts payable can be processed through manual means during the restoration process. If suppliers are not paid on a timely basis, the needed equipment and supplies for restoration may be delayed.

**TESTING**

#### Annual Testing

The goal of the test of the Disaster Recovery Plan is to see if it works. The credit union should conduct a “hard test” of their entire Disaster Recovery Plan, at least once a year. This test should “simulate a disaster” so that the credit union may implement the disaster recovery process. Later, after the test, the test results should be appraised for any amendments to the Disaster Recovery Plan.

#### Types of Testing

There are two different types of testing, passive and active. Passive testing is a test conducted by observation, inspection, reviewing checklists, or “walk through”. Active testing is completed by drills and simulation. In the instance of Disaster Recovery Plan testing, passive testing is applicable in reviewing the staffs’ completeness of being prepared for the initiation of an active “hard test.”

#### Simulated Disaster

The test should be conducted on a surprise basis, at a time to be determined by the Board of Directors, who may delegate this duty (i.e. to the credit union’s manager).

#### Minimizing Disaster Testing Impact

The idea of a Disaster Recovery Plan is to minimize the impact of a disaster on the credit union operation. There is a possibility of the test disrupting member services. The disaster planning and testing process should strive to minimize disruption to member service. Planning of the disaster recovery test should be undertaken with caution.

#### Off-Hours/Off-Line Tests

The credit union may elect to conduct the test of a simulated disaster on the weekend or an evening to minimize the impact on member services. The test would not utilize data but “test data” that would be prepared in advance (or be portion of an actual days transactions). ***This test should be conducted in a manner so that the test data is not input into the live “on-line” system.***

If “test data” is used:

1. Develop various types of transactions.
2. Assign distinctive names to the test data to facilitate identification.
3. Run a total on the “test” data to compare to the running of the disaster recovery test total.
4. Acquire alternative computer hardware, as appropriate.
5. Acquire compatible software, or use back-up copy sorted for disaster recovery purposes.
6. Install software and test.
7. Install member account data from stored back-ups.
8. Simulated disaster begins.
9. Input “test” data.
10. Observe test carefully for weaknesses.
11. Identify cause and corrective action for any weaknesses.
12. Amend Disaster Recovery Plan, if necessary.

If historical data is used:

1. Determine which daily work (or portion of day) is to be used for test.
2. Run a total of data to compare to running of disaster recovery test total.
3. Acquire hardware.
4. Acquire software.
5. Install software and test.
6. Install member account information.
7. Simulated disaster begins.
8. Input “test” data.
9. Observe and record weaknesses.
10. Identify causes and corrective action for weaknesses.
11. Amend Disaster Recovery Plan, if necessary.

#### Parallel Tests

A parallel test is a method that the credit union may use to minimize the disruptive effects of Disaster Recovery Plan testing on member service during normal business operating hours. In a parallel test, the credit union utilizes their current computer system during the testing phase along with their planned emergency system. The testing of the alternate computer system is achieved by comparing the output of the two systems (the credit union’s and test system) and following-up on any of the differences, what caused the differences, and how to resolve the differences.

If parallel resting is used:

1. Acquire alternate computer hardware.

2. Acquire alternate computer software.

3. Install software and test.

4. Install from back-up media the members’ account data.

5. Simulated disaster begins.

6. All transactions on credit union’s computer system are also input on the “simulated disaster” computer.

7. At the end of the test, the two sets of printouts are compared for any differences.

8. Any difference(s) must be followed-up and explained.

9. Corrective actions proposed for any difference(s).  
10. Amendment(s) made to Disaster Recovery Plan.

The credit union should retain copies of the testing procedures, results, and evaluation for later review by authorized outside parties (i.e. examiners and auditors).

**DISASTER RECOVERY PLANS FOR SPECIFIC DISASTERS**

#### Natural Disasters

**Fire**

**In the case of a fire:**

1. Sound the fire alarm.
2. Know the location of all fire exits.
3. Leave the area via designated exits when the fire alarm goes off.
4. Follow your supervisor’s instructions once outside the building.
5. Assist your supervisor in determining if all the staff and members have evacuated the building.
6. When evacuating, do not touch or open any door that appears “hot”, proceed to another exit.
7. Cover your mouth and nose with a cloth to reduce damage through smoke inhalation.

**In the case of a minor fire:**

1. Locate the nearest fire extinguisher to put out the fire.
2. If the fire cannot be put out rapidly, call fire department.

#### Protective Measures

1. Install an automatic sprinkler system.
2. Install heat and smoke detectors at strategic points throughout the credit union.
3. Install fire extinguishers at strategic points throughout the credit union.
4. Place visible exit signs and instructions of where exits are located at appropriate locations in the credit union.
5. Ground the building for protection against lightning and related electrical damage.
6. Limit smoking to a specific area of the credit union. Prohibit extinguishing cigarettes in waster paper baskets. Provide for appropriate disposal of cigarette butts (sand-filled containers). Check waste paper baskets for cigarettes each night.
7. Call local fire department for other useful fire prevention measures.
8. Post local fire department number on emergency number list.
9. Close all doors at night, so that if a fire starts it will be contained.

#### Tornadoes

Although tornadoes are relatively short-lived storms, they are extremely violent. They are most destructive over a small area.

The National Weather Service is responsible for issuing Weather Warnings. Television and radio stations in the area will broadcast two types of tornado warnings, tornado watches and tornado warnings. Local cities may use sirens or other audio warnings.

#### Tornado Watch

In the issuance of a tornado watch, the weather service is warning that the weather conditions are favorable for the development of a tornado.

The credit union’s response should be:

1. Alert appropriate staff to weather conditions.
2. Monitor weather reports.
3. Management should be kept informed of changing weather conditions.

#### Tornado Warning

A tornado warning means there has been a sighting of a tornado.

The credit union’s response should be:

1. Evacuate to shelter.
2. Monitor weather reports in shelter.
3. Inform management.
4. Activate shutdown procedures.
5. Notify workers to return to work after the danger has subsided.

#### Tornado Strike

If a tornado actually strikes the credit union causing damage and/or injury, the following procedures should be implemented.

1. Medical attention to injured.
2. Rescue of trapped individuals.
3. Fire control.
4. Assessment of damage.
5. Contact insurance representative.
6. Debris clearance.
7. Liaison with local disaster response group.

#### Flooding

#### Security Measures

1. Select a flood protected credit union site.
2. Proper drainage system.
3. Periodic inspection of credit union facilities for water damage.

#### Flood Response

1. The credit union receives the news of flood conditions from the weather service.
2. Notification of employees.
3. Activation of evacuation plan.
4. Activation of shelter plan.
5. Rescue.

#### Snow/Ice Storms

Snow/ice storm watches, warnings, and travel advisories are issued by the National Weather Service.

#### Pre-Storm Preparation

1. Purchase sand, salt, snow removal equipment (snow shovels, blowers, etc.) and arrange for snow removal service.
2. Establish a system of notification to employees.
3. Provide for emergency supplies (food, etc.).

#### Storm Response

1. Issue snow/ice emergency notification. Notification of employees and the public may be accomplished by two methods. First, each supervisor, or designated person, may call his employees at home. The other method is the manager may notify a local TV and/or radio station(s) about a closing announcement.
2. Implement shutdown procedures, if necessary.
3. Start snow/ice removal for reducing legal liabilities.

#### Salvage Operations After Natural Disaster

After a natural disaster, salvage operations are likely to be required. The following steps are recommended:

1. Determine who is to be in charge of the operation.
2. Assemble supplies for salvage operation off-site.

absorbent papers, drop cloths, blotting paper, flashlights, chemicals (alcohol and disinfectants), rubber gloves, tools (shovels, scrapers, etc.), nails, and other supplies.

1. Obtain temporary help.
2. Consider vacuum/freeze facilities for preservation of records.
3. Determine which records should be preserved.
4. Contact insurance company.

#### Human Activity

All financial institutions are targets for a wide variety of medical or criminal activities. Policies, procedures, training, and a thorough audit trail will reduce the likelihood of your credit union becoming a target. This section covers a broad cross-section of crimes and offers suggestions to protect both life and property:

* Medical emergency
* Insider dealings/conflicts of interest
* Employee theft
* Embezzlement
* Robbery
* Suspicious activity
* Bomb threats
* Civil disorder
* Extortion
* Kidnapping
* Check kiting
* Management secession

**Safety Tip:** Badges may be issued to all employees, officials, and visitors at a credit union. Laminated badges with photographs for employees and officials provide an easy and rapid means of identification. Visitors to the credit union may be issued temporary badges for security purposes.

# Medical Emergencies

Medical emergencies can occur with one or more persons at the credit union. Employees, volunteers, members, suppliers, and other visitors to the credit union could experience a medical emergency.

# First Aid Kit

The credit union should have at each branch a fully equipped first aid kit in case of a medical emergency. A handbook of first aid and emergency care for reference purposes for minor medical emergencies can be obtained from the local Red Cross.

# First Aid Training

The credit union should encourage employees to train for medical emergencies (consider offering a CPR class as part of employee training) through classes offered through the Red Cross. Once employees have become certified through the Red Cross, the credit union should keep an updated list of these person(s).

# Employees

Updated information should be retained on vital medical data for each person. The name, relationship, address, and phone number for next of kin should be maintained. Any employee injuries should be reported to credit union management so that the insurance company and any other necessity are completed. Disability claims involving workmen’s compensation claims would need reports completed in special cases. The credit union’s attorney should be notified of any accident, which may create potential liability for the credit union.

The staff of the credit union should be informed about the location of first aid kits in the credit union and have a list of emergency numbers at each phone.

# Handling a Medical Emergency

When a medical emergency occurs you need to:

1. Inform your supervisor.
2. Follow the supervisor’s instructions.
3. Know where the first aid kit is located.
4. Know the person(s) who are trained in life saving procedures.

# Insider Dealing and Conflict of Interest

Insider dealings and conflicts of interest do present a threat to credit unions. Although the percentage of credit unions actively involved in such illegal activities is small.

# Preventative Measures

1. Do not give special treatment to officials, management, or employees.
2. Follow NCUA guidelines for loans to officials, management, and employees. Develop written policies and procedures for granting such loans. Include thorough documentation.
3. Conduct a thorough audit of all loans to officials, management, employees, and family members.
4. Review any lease or purchase agreements between the credit union and officials or management to assure an “arm’s length transaction.”
5. Provide education to newly elected officials about duties and liabilities of directors.
6. Provide officials with information on director and officer’s liability and conflict of interest material.

# Types of Insider Dealings and Conflicts of Interest

1. Embezzlement.
2. Preferential and substandard loans to officials and employees.
3. Business loans to management officials and their private business interests.
4. Conversion of credit union assets for personal use and benefit.
5. Ownership by credit union officials and management of fixed assets which are leased back to the credit union which are not an “arms-length transaction”.

# Employee Theft

Employee theft may be reduced, if not eliminated, by carefully screening potential applicants during the pre-employment process.

# Preventative Measures

1. Require all applicants to complete an employment application. Do not use a resume only. Check for discrepancies between a resume and the application.
2. Verify previous employment with former employers. To avoid potential litigation, many employers will only furnish dates of employment and titles of positions held. Therefore, careful screening is vital.
3. Perform a credit check. Employees of financial institutions should exhibit prudent personal money management skills.
4. Contact bonding company for information about applicant.
5. Require employees to sign a “Code of Conduct” which lists specific prohibited activities.

# Embezzlement

**Preventative Measures**

1. Conduct at least a monthly independent verification (control records to the actual count) of the teller’s fund, traveler’s checks, money orders, and credit union checks written.
2. Review dormant account activity.
3. Reconcile bank accounts on a timely basis.
4. Reconcile investments on a timely basis.
5. Use check protectors to imprint dollar amounts on the checks written by the credit union.
6. Try to have more than one employee involved in any operation. The other employees involved should check the accuracy and authenticity of each activity.

# Embezzlement Targets

1. Money order packets could be opened and money order(s) removed out of sequence. The discovery of this would take until the next verification of money orders or longer.
2. Traveler’s checks packets could be opened and traveler’s check(s) removed out of sequence. The discovery of this would be the next verification of traveler’s checks or longer.
3. Review checks for being altered on the amount area, payees and the authorizing signature being the same person, and checks listed as “void” being processed.
4. Review inactive account activity for illegal withdrawals by employees.
5. Review disbursement of insurance funds to the members for illegal activity.

# Robbery

Robbery has the potential for being a highly dangerous situation because it involves the possibility of the use of “deadly force”. A robbery prevention plan is the best method to reduce the possibility of your credit union becoming a victim.

# Preventative Measures

1. Keep marked money in teller drawers and record the serial numbers on suspect identification sheets that should be kept at each teller station.
2. Do not keep large sums of money at teller stations. An analysis of cash flow and needs should be done to determine how much actual cash tellers need on a daily basis. Control access to all cash items (currency, traveler’s checks, money orders) by locking these items in individually lockable containers at all times.
3. Keep excess cash in the safe.
4. Install television monitors in critical locations.
5. Do not clutter windows with displays or signs blocking the view. Keep the view clear both into and out of the credit union.
6. Instruct staff to be careful when strangers show an interest in the number of employees, alarm system, or in your cash flow.
7. Notice suspicious persons loitering around the building, particularly at opening and closing time.
8. Be alert to anyone seeking entry when you are closed.
9. Do not carry money in a typical canvas moneybag. A briefcase is also a target. Carry money in shopping bag, flight bag, etc.
10. Vary your hours when making bank deposits. Do not get into an obvious routine.
11. Place height markers at main entrance so that staff can note a robber’s height as he leaves.
12. Install an alarm system and advertise the fact that you have one. Regarding robbery type alarms, one of the most important factors to consider is the safety with which it can be activated.
13. Side and back doors should be kept locked at all times.
14. Storage rooms should be fitted with an inside lock and a key should be hidden inside. Robbers have been known to lock employees in storage rooms. It is also wise to install an alarm button in storage rooms.
15. Vault rooms should have an alarm button.
16. Require references from employees. A surprising number of robberies involve employees or former employees. All job applicants should be carefully screened, particularly tellers.

# Staff Training

Your local police department can provide valuable written material and assistance in training staff in the event of robbery. Staff should also be trained to become observant to identify robbers, weapons, and vehicles.

All training should begin by emphasizing that, once the robber enters the credit union, personnel safety should be the primary concern of everyone. At no time should anyone attempt to stop the robber. Only if it is absolutely safe, should anyone attempt to activate an alarm or surveillance system.

# The Robbery

1. Remain calm.
2. Obey the robber’s commands and do exactly as you are told.
3. Inform the robber of any move you intend to make, that he may not anticipate, and could mistaken as an aggressive one.
4. Do not be a hero.
5. Take a good look at the suspect unless you are instructed to lie on the floor or turn your back.
6. Notice any detail, which will aid you to describe the robber. Note the shape of head, shape of eyebrows, eye-lid folds, color of eyes, type of lips, also notice color and scars. Also note the hairline, ears, nose, chin, and speech.
7. When trying to determine age, height, weight, and appearance make a comparison between the robber and yourself or someone you know. Check height against door markers as the robber leaves the credit union.
8. Notice tattoos, scars, and deformities.
9. Describe the type, color, and size of the weapon.
10. Follow the robber’s instructions.
11. Direct staff not to discuss the crime among themselves or with witnesses prior to arrival of the police.
12. Suggest that all witnesses make notes while the information is still fresh in their minds.
13. Watch which way the robber leaves and describe the vehicle.

**Post-robbery**

1. Call the police.
2. Inform them that you have been held-up and provide your address, telephone number, and name.
3. Be as accurate as you can be about details of the robbery.
4. Do not hang up the phone until the police tell you.
5. Give descriptions of all suspects, vehicles, weapons, and direction of travel.
6. Do not touch anything yourself, stop all business, and lock your doors. Preserve any items the suspect may have touched.
7. Prevent anyone from going into the area where the robbery occurred.
8. Ask all witnesses to wait for the police.
9. If a note is used in the robbery, keep it unless the robber wants it back.
10. Sit down and make notes after the robbery.
11. Answer all police questions as accurately as possible.
12. Cooperate with police personnel by making yourself available for interviews and giving evidence in court when required to do so.
13. Schedule a staff meeting within 48 hours after the robbery to obtain each staff member’s opinion about the credit union’s current policies, procedures, and training program dealing with armed robbery. Request each person’s input as to what might have better prepared him for the robbery.
14. Analyze the benefits of appropriate security measures which could include bullet-resistant barriers, armed guards, armored car services, etc.
15. Offer post-robbery counseling for employees.

**Suspicious Activity**

Contact your supervisor of any suspicious activity in or around the credit union facility.

**What Should Be Reported**

1. Persons loitering in or around the credit union.
2. Persons requesting information about the credit union staff or members.
3. Persons requesting information about the building, vault, etc.
4. Abandoned parcels left in the lobby or building.
5. Strangers attempting to enter non-public areas of the credit union.

# Bomb Threats

In the event of a bomb threat, the following procedures should be followed to reduce risk:

1. Call the emergency telephone number of local police. The police will contact other authorities for bomb disposal assistance. Under no circumstances should anyone attempt to locate, remove, or disarm a bomb on the premises.
2. Inform them of the name of the credit union, location, and explain the situation.
3. Staff should note any “out of the ordinary circumstances” or actual bomb sightings within the area which may assist in locating the bomb.
4. Evacuate all members from the building.
5. Instruct all employees to immediately leave the building. Each supervisor will be responsible to determine that all persons under their supervision are accounted for in the evacuation.
6. A bomb threat could involve neighboring businesses. Notify neighbors after the evacuation.

# Bomb Threat Guidelines

1. Record date of threat.
2. Record time of threat.
3. Record how the threat was reported.
4. Record the exact words of the caller.
5. Questions to ask the caller:
   1. When is the bomb going to explode?
   2. Where is the bomb located?
   3. What type of bomb?
   4. What does it look like?
   5. Why did you place the bomb?
   6. What is the location from which you are calling?
6. Describe the caller’s voice:
   1. Male/Female/Young/Old/Accent/Tone.
   2. Background noise.

# Extortion

When you receive an extortion call, you should:

1. Write down the caller’s exact word.
2. Ask for the caller to speak to the supervisor.
3. If the caller will not speak to your supervisor, ask to speak to the hostage.
4. If the caller will not let you speak to the hostage, you should ask for the caller to describe the hostage.
5. Ask for time to arrange for ransom money.
6. Contact your supervisor.
7. The supervisor should contact the local police and FBI.

# Kidnapping/Extortion

Kidnapping and extortion are not common events because of the government’s excellent record of apprehension, conviction and punishment. It is sound policy to adopt procedures to cover extortion threats and kidnapping.

# Extortion Defense Procedures

Extortion defense procedures should include an action plan and a form for completing vital details. Upon notification of an alleged kidnapping, the following procedures are followed, as appropriate:

1. Immediately, telephone the FBI. The person calling the FBI should be ready to furnish all facts relating to the disappearance of the victim.
2. Maintain absolute secrecy and do not permit any of the facts about the kidnapping or demands for ransom to be known to anyone outside the immediate family, except for investigating officers.
3. Do not handle letters or communications demanding the payment of ransom. Turn these over to the police.
4. Do not touch or disturb anything at the scene of the crime.
5. Remain calm and strive to maintain a normal routine around the office.
6. Furnish the investigating officers with a complete description of the victim and photograph, if possible. Furnishing all known details about the personal habits and characteristics of the victim.

# Kidnapping/Extortion Defense Procedures

Upon notification of an alleged kidnapping, follow all procedures below, which are appropriate to the situation:

Step 1: Obtain information and write down extortionist’s exact words:

Name of person kidnapped

Action threatened by caller

Amount of money demanded

Denomination(s) of currency

Type of container required

Time of drop

Release time and place of hostage

Delivery route required

Time of call

Sex of caller

Voice mannerisms

Background noises

Other information

Step 2: While the extortionist/kidnapper is still on the phone, do the following:

Ask for an extension of time to get the money.

Ask to speak to the person kidnapped.

If direct contact is not permitted, demand proof that the threat is not a hoax. Ask the person to describe the color of eyes, hair style/color, other physical features, and clothing worn by the victim.

Step 3: Immediately contact the local police and FBI

All or part of ransom money should be bait money. List the serial number and series year.

# Management Succession

A written policy covering the credit union’s succession of command is essential to assure the orderly succession of management and to minimize any disruption of the credit union’s operation.

# Management Succession Policy of the Credit Union

In the event of a catastrophic event or other emergency involving the credit union, it is possible that the manager/CEO will not be available to direct recovery operations. In such an event, the following is a succession listing of authorized persons to assume the responsibility:

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Credit union operation procedures in the event of a disaster:

1. If a natural disaster is of sufficient severity to prevent the conduct of the business of the credit union by its elected directors, officers, and committees, any three available members of the then incumbent board shall constitute a quorum of the Board for full conduct and management of the affairs and business of the credit union including the approval of loans to members, if the regularly elected credit committee is not available. In the event of the unavailability of three members of the Board, the vacancies, in order to provide a quorum of three, shall be filled as follows:

A. If the regularly elected Chairman or a regularly elected Vice Chairman is not available, the available person who is highest on the succession list for Chairman last authorized by the Board shall automatically become an Acting Director if he is not a member of the Board and Acting Director.

NOTE: See the resolution below.

B. If the regularly elected Treasurer is not available, the available person who is highest on the succession list for Treasurer last authorized by the Board shall automatically become Acting Director is he is not a member of the Board and Acting Treasurer.

NOTE: See the resolution below.

* 1. If a third Director is necessary to make a quorum, he shall be the next highest on the succession list for Chairman or upon the exhaustion of such list, the next highest available person on the succession list for Treasurer.

NOTE: See the resolution below.

Resolutions covering credit union’s operation in the case of an attack on the United States or other widespread disaster must be kept current, with a copy forwarded to the NCUA regional office. A sample Board Resolution is provided below.

#### Sample Resolution

BE IT RESOLVED, that if an attack upon the United States or other widespread disaster, a quorum of \_\_\_\_\_ of the Board of Directors as provided in Article \_\_\_\_\_ of the bylaws is not available and among those unavailable are the Chairman and Vice Chairman, the highest available person in the following succession list shall automatically become Acting Director if he is not a member of the Board.

1. Second Vice-Chairman
2. Treasurer
3. Secretary

BE IT FURTHER RESOLVED, that if an attack upon the United States or other widespread disaster, a quorum of three directors as provided in Article \_\_\_\_\_ of the bylaws is not available and among those unavailable are the Treasurer, the highest available person in the following succession list shall automatically become Acting Treasurer and/or Acting Director if he is not a member of the Board.

1. Manager/Chief Executive Officer
2. Assistant Manager/Vice President
3. Controller
4. Supervisory Committee Chairman (if applicable)
5. Credit Committee Chairman (if applicable)

The following sample Resolution authorizes relocation of the credit union in the event of a widespread disaster.

**Sample Resolution**

BE IT RESOLVED, that if as the result of an attack upon the United States or other widespread disaster, the office of this credit union is unable to conduct its functions at its regularly designated location, the office location will be \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, until such time as the Board of Directors as then constituted shall designate another location.

The following sample policy covers situations, which involve the sudden departure of the Manager/CEO of the credit union.

Sample Policy

The following individual shall be appointed Acting Manager/CEO until a new Manager/CEO is hired by the credit union.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Financial Threats**

#### Liquidity

A liquidity crisis could arise for various reasons. A run on shares could occur because of the member's loss of confidence in the credit union. Excessive loan demand can also result in liquidity problems. The following areas should be reviewed by management and officials to formulate a plan to handle the crisis:

1. Appoint an official spokesperson to restore member confidence in the credit union. Generally, this person would also handle public relations for the credit union.
2. Determine your credit union’s line of credit with Kansas Corporate Credit Union.
3. Authorize individuals to obtain funds from Kansas Corporate Credit Union.
4. Determine the reason for the run-on shares.
   1. Internal – Was something done by the credit union? If necessary, institute immediate changes and inform members of the changes.
   2. External – Was some outside event responsible for the run? If the run was caused by external events contact your Association for assistance. It would also be wise to contact the National Credit Union Administration or Kansas Department of Credit Unions for advice.
5. Evaluate if the liquidity crisis is caused by a lack of credit with Kansas Corporate Credit Union.
6. Determine the reasons for excessive loan demand.
7. The credit committee, Board of Directors, and/or management should review and revise loan pollicies, if necessary.
8. Review the credit union’s policies with regard to shares and share promotional programs. Revise the pollicies, if necessary.

### Insolvency

A credit union does not become insolvent overnight. Generally, either the state or federal regulators will have issued warnings and targeted specific problem areas uncovered during the examination process. The regulators will insist upon immediate action to correct the problems. All available alternatives for correction of the causes must be considered by the credit union. If the cause of the insolvent condition cannot be corrected, merger becomes likely. The membership should be reassured about the credit union’s insured status and the protection of member accounts should be stressed.

The following suggestions apply to both liquidity and insolvency problems:

* + - 1. Examine options to increase membership or assets

1. Taking in select fields of membership
2. Merger
   * + 1. Contact the state, NCUA, or Kansas Credit Union Association for assistance.
       2. Prepare an annual financial forecast:
3. Spread analysis
4. Review of income and expenses
5. Review of credit and collection programs
6. Review of investments
   * + 1. Establish a timetable for resolving problems.
       2. Notify membership through a special letter, if applicable.
       3. If liquidation will occur, notify the membership and media to assure them that precautions are being taken to assure full return on all member assets.
       4. Assure members that their accounts are insured.
       5. Determine your delinquency ratio over the past five years. Develop strategies to lessen the ratio.
       6. Evaluate what procedures can be used to speed up collections.
       7. Review performance appraisal of credit union manger. Review the results and standards set for performance.
       8. Review qualifications and expectations of the Board of Directors.
       9. Review training programs for management and volunteers. Determine if additional training is necessary to strengthen capabilities.
       10. Conduct a survey of member usage of credit union services and review past surveys, if any.
       11. Review relationship with sponsor, if applicable. Determine if the relationship needs to be strengthened.
       12. Review methods of communicating with members about services.

### Legal Action Against the Credit Union

A credit union could become the defendant in a lawsuit for a variety of reasons ranging from an accident with a repossessed car to a class action suit. The following items will assist you in properly responding to the threat of legal action:

* + - 1. Contact your credit unions’ attorney.
      2. Review the credit union’s CUMIS insurance coverage for its premises, members, employees, and officials.

Name of CUNA Mutual representative

Telephone number of representative

Date of last review of coverage

* + - 1. Provide CUMIS with the name and telephone number of the credit union’s attorney. CUMIS may assign an attorney to handle the matter.

### Sponsor-Related Actions

Sponsor actions that affect the health and safety of your credit union include plant closings, layoffs, loss of field of membership, and labor relation problems among employees of the sponsor.

The following items need to be considered in relationship to sponsor actions:

1. Analyze under what circumstances a sponsor could go out of business, relocate, layoff personnel, or become involved in labor relations issues.
2. Determine the immediate impact on your credit union if:
3. Sponsor goes out of business
4. Sponsor layoffs
5. Labor relation problems
6. Evaluate methods to preserve the credit union and its membership in case of a crisis.
7. Determine the method to establish a dialogue with membership to communicate their thoughts on preserving the credit union.
8. Evaluate the sponsor’s services, which are used by the credit union.
9. Date processing system
10. Payroll deduction
11. Employees
12. Office space
13. Property
14. Phone system
15. Utilities
16. Determine who uses the credit union.
17. Employees
18. Family Members
19. Retired
20. Other
21. Determine the amount of credit available from Kansas Corporate Credit Union.
22. Review the credit union’s lending policies.
23. Consider or review current policy on extension agreements for displaced workers.
24. Consider a merger partner.
25. Proceed cautiously in the event of labor relation problems. Remain neutral.
26. Maintain communications with both union and management officials.
27. Prepare lending policies to be implemented in case of a strike. The Board should approve the policies. Review loan limits on unsecured loans and share secured loans.
28. Establish share withdrawal policy during a strike. The policy should address withdrawals for members who have loans and a policy to cover share draft account overdrafts.
29. A reduction in payroll deduction can create cash flow problems.
30. Establish how the credit union will transact business with members during a strike. Crossing picket lines can create a volatile situation.
31. Determine if it may be necessary to open a temporary office for the duration of the strike. Pre-select possible locations.
32. If possibility exists of damage to the credit union or risk to staff, consider security guards or move the office to a temporary location.

**Utility Failures**

**Power Interruption**

If a power failure should occur at the credit union, the following steps should be followed:

1. Manually secure facility.

2. Contact the power company preferably on the emergency number.

3. Obtain the reason for outage and estimated downtime.

3. Inform management.

4. If an internal wiring problem, contact an electrician.

# Phone Service Interruption

If telephone service is interrupted at the credit union, the following steps should be followed:

1. Contact the telephone company, preferably on the emergency number.

2. Obtain the reason for disruption and estimated downtime.

3. Inform management.

Telephone service is important to the credit union’s operation. The credit union should take measures to implement “alternative” telephone service as a critical operation.

These steps can aid the recovery of credit union operation until the restoration of normal telephone service:

1. Give your telephone number to others (vendors, etc.), so they can call you.
2. Use cellular telephones, CBs, and short-wave radios as alternatives for regular telephone service.
3. Form “reciprocal phone agreements” with the next-door businesses to act as a “phone-clearing house”. The next-door business could act as an emergency telephone system in case of a crisis.

# Water Interruption

If water is interrupted at the credit union, the following steps should be followed:

1. Contact water company, preferably on emergency number.

2. Obtain the reason for disruption and estimated downtime.

3. Inform management.

4. If an internal plumbing problem, contact plumber.

1. If long term, alternate means of supply should be obtained (such as bottled water or transporting water from outlying areas).