



# Security Policy

rev 05/03

## Security Officer

Karl Graham, Senior Accountant

[KGraham@alternatives.org](mailto:KGraham@alternatives.org)

607-273-4611 Ext. 822

## Overview

This policy was developed to comply with the security program requirements of section 205(e) of the Federal Credit Union Act and part 748 of the regulations of the NCUA. This policy establishes security procedures and devices to discourage robberies, burglaries, larcenies and embezzlements; to assist in identification and prosecution of persons who commit such crimes; to provide for the safety of staff and members; and to prevent the destruction of vital records at the credit union.

## Board of Directors Approval

This policy has been approved by the Board of Directors at its meeting on \*\*\*\*\*and supersedes all previously adopted security policies.

## I. Program Administration

The Board of Directors has designated the CEO of Alternatives FCU with responsibility for credit union security. The CEO has delegated responsibility for administering this policy to the security officer. The security officer's duties include:

- 1) Development and modification of the written security policy as needed.
- 2) Implementation of security procedures and controls as described in this policy.

- 3) Training of staff in security procedures and policy, and conduct during and after a robbery or burglary.
- 4) Oversight or assistance in security equipment selection, testing, maintenance, and operation.
- 5) Consultation and coordination with local law enforcement agencies to develop robbery and burglary alarm response plans.
- 6) Other responsibilities as assigned by management and the board of directors.

## II. Internal Controls

The CU has adopted plans of organization and operation to safeguard its assets, check the reliability and accuracy of its accounting data, promote operational efficiency, and to encourage adherence to CU policies and procedures. Many of the internal controls are designed to protect the CU against embezzlement.

### **Accounting Controls**

The CU's accounting system is in accordance with generally accepted accounting principles and the Accounting Manual for Federal Credit Unions. Internal controls are designed to provide reasonable assurance that:

- 1) Transactions are executed in accordance with management's general or specific authorization;
- 2) Transactions are documented and recorded promptly to permit accurate preparation of financial statements and to maintain accountability for assets;
- 3) Access to assets is permitted only with management's authorization; and
- 4) The recorded accountability of assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences

### **Audit Policy**

The Supervisory Committee of the Board of Directors shall oversee a periodic program of internal auditing to include, but not limited to, bank reconciliation's, random cash counts, review of officials' and employees' loans, and verifications of accounts. The committee will also oversee an annual audit by an independent public accounting firm.

### **Control of Currency Levels**

A maximum amount of currency to be held in the vault will be determined by CU

management. It is the responsibility of the MSR Manager to ensure that currency is maintained at or below the maximum. The currency level should be checked weekly.

A maximum currency level for individual MSR's will be determined by management. It is the responsibility of the MSR Manager or vault manager to ensure that excess currency is shipped to the vault at the earliest possible time.

It is the responsibility of each MSR to ensure the security of the cash placed in their care. It is the responsibility of the vault manager to ensure the security of all vault cash.

### **Dual Controls and Segregation of Duties**

It is CU policy that no one employee dominate any transaction from inception to completion. In addition, when operationally practical, teams of at least two employees will exercise dual control over part or all of procedures involving cash, traveler's checks, and other negotiable instruments.

### **Key and Combination Control**

Management will ensure that the number of exterior door keys and entry cards supplied to staff or vendors are kept to a minimum. A log shall be maintained listing name and affiliation of key recipient, date of receipt of key, and date key returned. Excess keys will be kept in a locked location.

Lost or stolen employee entry cards should be reported to the security officer immediately. Said entry cards will be blocked (de-activated) at the earliest possible opportunity. The entry cards of ex-employee's, if not turned over to supervisors or the security officer, shall also be blocked at the earliest possible time.

Access to the software that controls entry card and code maintenance shall be strictly regulated to authorized personnel only.

Dual control will be maintained over vault and safe access. Knowledge of combinations and possession of keys to access vaults and safes shall be such so that no one person is capable of accessing the vault or safe alone. Employees assigned the vault and safe combination or keys will be changed at regular intervals, determined by management. At the same time, vault and safe combinations will be changed. Lost or stolen vault or cash drawer keys shall be reported to the supervisor immediately.

Vault and safe access will be limited to the minimum number of staff possible to maintain

effective operations.

### **Personnel Policies**

Prospective employees of the CU will be screened for criminal history, bond ability, and credit history . This screening will include asking appropriate questions on application forms, pulling a credit history, and checking the employee's history through the CU's bonding company.

Employees responsible for currency or negotiable instruments must telephone their supervisor to explain absences from work. If an employee doesn't phone to explain an absence, the employee's home will called to determine the reason for the employee's absence.

If telephone verification of an employee's absence cannot be made, the employee's cash or negotiable instruments will be counted immediately.

## **III. Security Policies and Procedures**

### **General Safekeeping Policy**

Management will implement security procedures for the CU (and any branches including ATM's) to provide for the safekeeping of currency, negotiable instruments, and vital records. All employees will be familiar with security procedures.

### **Safekeeping of Currency, Valuables, and Vital Records**

All currency, negotiable instruments, and other valuables will be stored in a locked, burglar resistant vault or safe during non-business hours.

During business hours, only the amount of currency, negotiable instruments, and other valuables needed to meet operating needs will be removed from the vault or safe. Said valuables will be kept in a secure location with access limited to specific, appropriate staff.

Vital records or copies of vital records on disk or fiche, will be stored in a fire resistant vault, safe, or file. Backup copies of member share and loan system full backups will be kept off site.

Blueprints or specification plans for CU offices, vaults, or other areas where valuables are stored will be kept in a secure location. A record of all such documents shall be maintained by the security officer.

### **Opening and Closing Procedures**

All employees shall be familiar with and follow the prescribed opening and closing

procedures set by management. If there is any suspicion that the building is unsafe to enter, the employee shall not enter or exit immediately and call the police.

### **Opening Procedures**

The first staff person to arrive at work in the morning shall, after turning off the alarm system, obtain and keep with them a remote alarm button. If there two staff in the building, working in different areas of the building, both people will wear a remote alarm. The remote will be kept at hand and all access doors will remain locked, until the majority of staff (on each floor) arrive (usually 8:45am, weekdays, 9:30am, Saturdays). No unknown person(s) should be allowed into the CU prior to opening.

The employee entrance door will remain locked and closed at all times unless the door is being used for maintenance or delivery purposes, in which case the door will be monitored by an authorized person.

### **Closing Procedures**

Once the lobby area is closed to the public (3pm weekdays, 1pm Saturdays), access doors and gates will be closed. Entrance will be restricted to authorized persons. Once the reception lobby is closed to the public (5pm weekdays, 1pm Saturdays) the front entrance door shall be locked. Staff shall not exit or enter through this entrance unless servicing the vestibule area, in which case the door will be unlocked only to allow their exit and re-entrance.

All currency, negotiable securities, and similar valuables will be secured in the office safe at the earliest practicable time. Member Service Staff should recheck work stations to ensure that all valuables are secured.

It is the responsibility of the last staff person to leave the building to ensure that the entire building is secured. This includes ensuring vault and safe doors, exterior doors, and appropriate interior doors are securely closed. In addition, all areas of the CU should be investigated to ensure 1) no staff people are still in the building, and 2) no unauthorized person(s) are in the building. All unnecessary lights should be turned off.

A remote alarm shall be carried while the final closing inspection is held. After insuring the building is secured, the last person out shall turn on the alarm system and exit the building.

### **Non-Business Hours Procedures**

Staff entering the building during non-business hours shall, after turning off the alarm, obtain

and keep on their person at all times a remote alarm button. If applicable, access doors should also be kept locked, ie, when moving from one floor to another within the building, the staff person should lock doors behind them.

If the alarm system is already off, the reason why must be immediately investigated. There may be a staff person or cleaning contractors already in the building who should be located and informed that another staff person is present.

### **Visitor Identification and Access to Restricted Areas**

Identification of visitors should be verified unless the visitor and reason for visit are known to CU personnel. A log book will be maintained to document all visitors to the CU (visitors include vendors and repair technicians). The log book will record the date of visit, visitor's name and company, purpose of visit, time of arrival and departure, and CU employee assigned to escort the visitor. Visitors are required to wear a visitors badge while on premises.

Visiting family members or personnel friends of employees, desiring to visit areas of the building normally off limits to the public, shall also log in. Said visitors shall wait at the reception desk until the employee is notified. The employee should then meet their guest at the reception desk. Exceptions are allowed in the case of regular family visitors who are well known to staff.

Access to nonpublic areas of the CU will be restricted:

Visitors must be accompanied by staff during business hours

After banking hours, access to the teller area will be restricted by locked gates and doors.

Access to the mechanical room, electrical panels, and office supply areas of the CU will be restricted by locked doors.

### **Transportation of Currency by Armored Car**

All currency to be shipped will be counted and strapped under dual control. Currency received in bulk will be counted in the presence of the armored car employee unless the delivery is guaranteed by the armored car company. A signed receipt will be obtained for all shipments and receipts of currency. Shipments should be secured in the vault immediately.

### **Servicing of ATMs: Remote and on location**

Management will develop and implement ATM servicing procedures. All employees servicing ATMs will be familiar with and follow the prescribed servicing procedures.

#### IV. Policy for the Identification, Apprehension, and Prosecution of Criminals

In order to assist in the identification, apprehension, and prosecution of persons who commit or who attempt to commit crimes against Alternatives FCU and/or its employees, CU management or its designee(s) will be responsible for implementing the procedures in this security policy.

##### **Procedures For Maintaining Records of Crimes**

A copy of the police report, CUNA Mutual Insurance forms, or other detailed records of any robbery, burglary, or larceny at any credit union owned property will be kept at the credit union by the security officer.

A Criminal Referral Form will be filed anytime an officer, director, employee, or agent of the CU is suspected of crime. The security officer or other officer will promptly report all such incidents to the CEO, unless the offending party is the CEO, in which case a report shall be made to the Supervisory Committee of the Board of Directors. If a member of the Board is suspected of committing a crime, then the report will be made to the CEO or another officer of the Board.

Records of any crimes and supporting documents will be kept on file at the CU for at least 7 years from the date of the report.

##### **Procedures for the Operation of Surveillance Systems**

Closed Circuit cameras will continuously monitor and record activity at the teller line and other areas as determined by management. Access to the digital records will be restricted to authorized staff persons. To ensure cameras are operating properly, the security officer or computer specialist will view recorded images weekly at a minimum.

##### **Procedures for Maintenance of Bait Money**

Bait money will be kept at each teller station in their working drawer. Bait money will consist of used Federal Reserve Notes with no obvious markings. A photocopy record of bait money listing in which teller drawer the bills are located will be maintained by the Member Service Manager. All employees will be trained in the proper use and maintenance of bait money.

##### **Height Reference Markers**

Height reference markers or visible strips of tape at a five and six foot height will be installed on door frames at all office exterior entrances. All employees will be trained to use these markers to estimate a suspect's height.

## V. Security Training Policy

The security of the membership, employees, and assets of the Alternatives FCU is the responsibility of all employees. It is the policy of the Credit Union to provide a program of initial and periodic security training for each employee.

### **Security Officer Training**

The security officer will receive initial and periodic training designed to foster effective administration of this security program. This training program will keep the security officer appraised of current industry standards for security devices and procedures, criminal activity in the area and security related compliance issues. This training will include, but not be limited to:  
Periodic consultation with law enforcement officials.

Subscription to trade journals dealing with security and compliance.

Periodic consultation with security consultants or security equipment vendors regarding current industry standards for security devices and procedures.

Attendance at security training seminars or classes.

### **Employee Security Training**

The security officer or designee will develop and implement a program to provide initial and periodic training of employees, interns, and volunteers in their responsibilities under this security program, including the operation of security devices, and in proper conduct during and after a robbery, burglary or larceny. The security office will maintain a log of all training provided. To include: staff persons name(s), date, and topic of training.

## VI. Burglary or Robbery Policy

The following guidelines for employee conduct during and after a robbery, burglary, or larceny will be followed.

### **Employee Response to a Burglary or Larceny-Alarm Not Sounded**

Each employee will be trained to follow this procedure upon the discovery of an apparent burglary or larceny:

Immediately report the apparent crime to the security officer (or other designated credit union official), local law enforcement officials and the FBI.

To protect the physical evidence, avoid disturbing or handling any object the criminal may have

touched.

Cooperate with the police investigation.

Discuss the crime only with designated credit union and law enforcement officials.

### **After Hours Burglar Alarm Response**

The security officer will prepare a list of employees who meet the criteria for after hours alarm response (see Alarm Response Policy). This list will include the alarm cell phone number, the primary and backup responders for each month, and the responder's home telephone numbers. A copy of this list will be forwarded to each responder, and posted at the employee entrance. The alarm monitoring service and the Ithaca Police Department will be provided the alarm cell phone number and as backup, the security officer's home phone number.

When an alarm is detected, the monitoring service will contact the after hours alarm responder to assist in the alarm investigation. The responding employee will be trained to follow this procedure.

- 1) When contacted by the monitoring service (or police), proceed to the credit union office. If the police have not arrived, wait in a locked vehicle a safe distance from the office for their arrival.
- 2) After the police have surveyed the exterior of the office for signs of forced entry, permit their access to the facility, disarm the alarm system, and assist in their investigation when they indicate it is safe to do so. Use extreme caution because an intruder may be hiding in the office. Conduct an interior inspection of the office with the police. Thoroughly examine all vaults for signs of forced entry.
- 3) If a burglary has been attempted or committed, immediately notify the security officer and the CEO. The police will notify the FBI. The following day, the security officer or CEO will notify the NCUA and CUNA Mutual Insurance.
- 4) If any physical damage to the building has occurred, broken window(s) for example, refer to the After hours Alarm Response Schedule or Policy for the phone numbers of repair companies.
- 5) Cooperate with the police investigation. To protect evidence, avoid disturbing or handling any object the burglar may have touched.
- 6) Discuss the crime only with designated credit union and law enforcement officials. Only the CEO and COO are authorized to speak to the press about events occurring at the CU.

## **Employee Conduct during a Robbery**

In the event of a robbery, the safety of members and employees is of primary importance. The objective is to get the robber out of the CU as fast as possible

All employees will be trained to follow this procedure during a robbery.

Remain composed - try not to panic.

Follow the robber's commands exactly without hesitation or resistance. Avoid taking any overt actions other than those ordered by the robber. Tell the robber what you are about to do, before making any movement to avoid misinterpretation of your action.

Actuate the silent alarm only after the robber has exited the building, unless the situation demands immediate police response.

If the robber demands a certain amount of money, surrender the exact amount. Do not volunteer additional currency or information about where additional funds are stored. Include bait money with the amount given to the robber.

If a note is passed, handle it carefully. Hold it near the edges to preserve fingerprints. Set the note aside; return it only if the robber asks for it.

Be observant, but not obviously so. Do Not Stare! Note features and characteristics that stand out: eye color, voice, scars, tattoos, moles, clothing. Note the weapon: handgun or long gun, any visible words or symbols, is the color all black or different colors.

Note where the robber's body meets the teller counter: at the waist, lower chest, etc.

Try and observe the robber's height relative to the height markers as the robber exits the building.

Remember everything the robber touches and report it later to the police. If more than one robber is present, concentrate on the nearest one.

## **Employee Conduct after a Robbery**

Certain actions must be taken immediately after a robbery. In some cases (e.g., a robbery involving a lone note passer) the victim may be the only person aware that the robbery has taken place. All employees will be trained to follow this procedure.

Activate the silent alarm as the robber is leaving the office, even if it has been actuated once before.

Notify management that a robbery has occurred as soon as it is safe to do so.

The MSR Manager, Assistant MSR Manager, or MSR in charge should direct staff to take the following actions simultaneously:

All Tellers lock cash drawers to secure any remaining cash or valuables.

Call the police and give any relevant information, including the designated staff person who will meet the responding officers outside.

After staff is positive the robber has left the building, carefully approach a window or door to observe the direction of escape. Observe any accomplices or witnesses outside. If a vehicle is used, try to obtain its description and license plate number.

Block off all area's the robber may have touched.

Inform members in the lobby and other staff that a robbery has occurred. Ask members to remain until the police arrive. If a member insists on leaving, verify his identity and record his name, address, and telephone number.

Ask anyone who was in the area and may have observed the robber to fill out a robbery description form. Witnesses, including the victim teller should be separated and not discuss their memories of the robber so as not to contaminate each other's memory.

Each teller review their previous 2 or 3 transactions and write down the member's names for the police, in case they may have witnessed the robber.

Discuss the robbery only with designated law enforcement and credit union officials. Only the CEO and COO are authorized to discuss the robbery with the media.

As soon as feasible, the security officer or CEO will notify the NCUA and CUNA Mutual Insurance. The FBI will also be notified if the local police have not done so already.

Staff not appointed to specific duties by management should remain away from the lobby area.

## VII. Security Devices

The security officer shall provide for selecting, testing, operating, and maintaining security devices.

Safes, overnight depositories, ATM vaults, envelope depositories, and any other container meant for the storage of negotiable instruments shall at a minimum meet CUNA Mutual Insurance Company and/or NCUA guidelines.

The alarm system providing entrance, area, vault, depository, ATM, and silent detection is maintained by Brown Security and monitored continuously by Sentry Alarms.

A lighting system will be in place for illuminating the parking lots, walkways, the drive through/ATM area, and outer lobby and night depository.

Back-up power is provided by a generator. This backup power is minimal and meant primarily to provide for the security and phone systems.

Cameras providing digital coverage of the teller line, front vestibule, drive through ATM, and staff entrance are supplied and maintained by Danica Computers.

### **Procedure for Selecting Security Devices**

The security officer is charged by management with soliciting bids for security devices.

The following factors will be considered in the selection of devices for purchase:

Whether the device meets or exceeds current industry standards. (Consult with law enforcement officers, security specialists, our bonding company and vendors of security devices).

The incidence of crimes in the area in which the credit union office is located.

The location of the nearest law enforcement offices, guards or security personnel and the time required for such personnel to arrive at the office.

The amount of currency or other valuables exposed to robbery, burglary, or larceny.

Other security measures in effect at the credit union office or within the surrounding area.

The physical characteristics of the credit union office structure and its surroundings, including the physical vulnerability of the office itself and visual obstructions nearby caused by architectural or landscaping features which might provide places for criminals to hide.

The size of the credit union office and number of employees.

### **Operation of Security Devices**

The security officer shall establish procedures to ensure that security devices are operated properly at the credit union office. Such procedures shall include:

Training on the operation of (relevant) security devices for all office personnel.

Visual and operational inspection of security device controls to ensure they are working properly.

Immediate notification of the security officer when any security device fails.

### **Procedures for Testing and Maintaining Security Devices**

The security officer, working with the security device vendors, will schedule tests and preventive maintenance inspections for all security devices. A written record of each test or inspection and its result will be retained at the office. The tests and inspections will include, but not be limited to those listed below.

All robbery alarms will be tested semi-annually.

All actuating devices will be included in the tests and all office personnel will participate in the procedure.

Preventive maintenance inspections of all security devices will be conducted at least once every year by an authorized service contractor.