



CU*Answers Policy Manual

FY2018-FY2019

CU*ANSWERS
A CREDIT UNION SERVICE ORGANIZATION

Table of Contents

1	CYBERSECURITY POLICY	4
2	INFORMATION SECURITY POLICY AND PROGRAM	8
3	ACCEPTABLE USE POLICY	16
4	AUDIT POLICY AND EXAMINATION PROTOCOL	19
5	BUILDING SECURITY POLICY	24
6	CLIENT SUPPORT POLICY	29
7	LARGE SCALE ABSENCE POLICY	31
8	RECORDS AND INFORMATION MANAGEMENT POLICY	34
9	VEHICLE POLICY	37
10	VENDOR MANAGEMENT AND PROCUREMENT POLICY	40



CU*ANSWERS Policy Manual Overview

*Policies Approved by the
CU*Answers Board of Directors*

This Policy Manual is intended to provide requirements for continued employment with CU*Answers. These policies are dynamic and under constant review. Policies currently in effect may be revised, suspended, or eliminated by CU*Answers in response to changing marketplace and/or legal requirements.

Any changes to this manual will be communicated to staff. Some policies are necessary due to company compliance requirements with federal or state laws. If a question ever arises about the nature and extent of CU*Answers policies and any conflicts with regulations, the requirements of the specific laws or regulations govern.

WARNING

Violations of policies will be recorded by the Internal Auditor and reported to executive management and the board of directors. Failure to adhere to policies may result in discipline up to and including termination. Willful violations of policies which are also violations of law may result in fines, imprisonment, or both.

None of the policies included in this manual are intended to, nor do the policies grant, any contractual rights. This policy manual may be amended or revised from time to time as the need arises. The policies in this manual supersede any contrary or previous versions.

1 CYBERSECURITY POLICY

The Cybersecurity Policy defines the duties employees and contractors of CU*Answers must fulfill in securing sensitive information. The Cybersecurity Policy is part of and incorporated into the Information Security Program and Policy, as well as the Acceptable Use Policy.

Policy Owner: Network Services

1.1 POLICY PURPOSE AND OVERVIEW

Employees and contractors have a duty to safeguard sensitive information. Sensitive information includes trade secrets, confidential or proprietary information of CU*Answers, its partners or clients, and the non-public personally identifiable financial information of credit union consumers or members, as well as the employees and contractors of CU*Answers.

Every CU*Answers employee and contractor is responsible for ensuring that use of Computer Resources, as well as outside computers and networks, such as the Internet, does not compromise the security of CU*Answers. This duty includes taking reasonable precautions to prevent intruders from accessing the company's network without authorization, preventing introduction and spread of malware, and the use of other reasonable means to protect sensitive information.

Employees and contractors must take reasonable steps to ensure sensitive information is maintained and transmitted securely. Employees and contractors must not disclose sensitive information unless authorized by job description or by an officer of CU*Answers.

WARNING

In addition to discipline up to and including termination, willful violations of policies that are also violations of law may result in fines, imprisonment, or both.

1.2 SENSITIVE INFORMATION DEFINED

1.2.1 NON-PUBLIC PERSONALLY IDENTIFIABLE INFORMATION (PIFI)

This includes information that can be linked, directly or indirectly, to individual consumers of financial products, per Regulation P (Sections 502–509 of Title V of the Gramm-Leach-Bliley Act). Examples include, but are not limited to, Social Security numbers, credit union account numbers, and credit and debit card numbers that can be identified to a financial consumer.

1.2.2 SENSITIVE EMPLOYEE OR CONTRACTOR INFORMATION

This includes, but is not limited to, health records, payroll records and other non-public personal records of CU*Answers employees and contractors.

1.2.3 CONFIDENTIAL CLIENT AND VENDOR DATA

CU*Answers has agreements with our clients and vendors promising to secure their confidential information. Generally speaking, confidential client or vendor data is any data regarding client or vendor business that is not known or available to the public.

1.2.4 TRADE SECRETS AND CONFIDENTIAL EMPLOYER DATA

Trade secrets and confidential employer information includes information protected from disclosure through CU*Answers reasonable efforts to maintain its status as a “secret.” CU*Answers confidential data and trade secrets may include but is not limited to: proprietary computer software programs; proprietary databases, business processes and methods; information pertaining to overhead, costs, pricing and margins; strategic plans; and marketing programs.

1.2.5 CONSUMER PRIVACY

CU*Answers is required to have a high standard of care regarding the confidential information of our clients and their consumers or members. This policy describes CU*Answers policies towards both confidential client information and the nonpublic personal information of credit union member and non-member customers.

1.2.6 CONFIDENTIAL CLIENT INFORMATION

CU*Answers will not use or disclose to any third party any information concerning the trade secrets, methods, process or procedures or any other confidential, financial or business information of a client which it learns during the course of service. CU*Answers will treat client information with the same degree of care that it treats its own most confidential information and shall disclose such information only to employees or representatives who require such in the ordinary course and scope of their employment.

1.3 PRIVATE INFORMATION OF MEMBERS AND NON-MEMBER CUSTOMERS OF CLIENTS

CU*Answers intends to protect the privacy and confidentiality of the Nonpublic Personal Information of the members and non-member customers of any Credit Union CU*Answers has an agreement with. CU*Answers is prohibited from disclosing or using Nonpublic Personal Information about the Credit Union's members other than to carry out the purposes for which the Credit Union disclosed the members' non-public personal information.

CU*Answers shall disclose to the Credit Union any breach in the security resulting in unauthorized intrusions into CU*Answers' systems that may materially affect the Credit Union or its members.

1.4 NO OBLIGATION TO PROTECT PUBLICALLY AVAILABLE INFORMATION

CU*Answers has no obligation to protect information which (i) was publicly available or in the public domain at the time of disclosure, (ii) becomes publicly available or in the public domain subsequent disclosure through no fault of CU*Answers, (iii) is in the CU*Answers possession free of any obligation of confidence to the disclosing party at the time of disclosure, or (iv) is disclosed to CU*Answers from another source rightfully possessing it.

1.5 EMPLOYEE BOND

CU*Answers agrees that any of its employees who have access to internal information or Credit Union information will be sufficiently bondable against fraud or other dishonesty.

1.6 MINIMUM REQUIREMENTS FOR DATA SECURITY

The following are the core rules with respect to the use and protection of sensitive information:

1.6.1 USE ENCRYPTION

Employees and contractors are required to use secure and/or encrypted methods authorized by CU*Answers before sending confidential information to parties outside of the organization.

1.6.2 ENSURE AUTHORIZATION

Employees and contractors are required to have reasonable assurance that the recipient of confidential information is authorized to receive the sensitive information prior to sending.

1.6.3 DO NOT DISCLOSE UNLESS AUTHORIZED

Employees and contractors are allowed to disclose sensitive information only when authorized to do so. Employees and contractors should never disclose information if they have any doubt they have authority to do so.

1.6.4 STORE SENSITIVE INFORMATION SECURELY

Employees and contractors are forbidden to store sensitive information insecurely, either in hardcopy form or electronically where accessible to unauthorized personnel. In addition, users are not allowed to store sensitive information to their local machine or mobile device.

1.6.5 DATA LEAKAGE

Employees and contractors are forbidden to transfer sensitive information to mobile storage devices (such as to CDs or DVDs, or USB Flash Drives), unless such transfer is permitted by the organization to do so.

1.6.6 NOTIFY WHEN SUSPECTED SECURITY INCIDENT OCCURS

Employees and contractors are required to notify the organization through Security Incident Reports when a breach of sensitive data is known or suspected.

1.6.7 DESTROY SENSITIVE INFORMATION SECURELY

Sensitive information, especially in hardcopy form, should be destroyed when not used. Sensitive information in hardcopy form must be shredded in an authorized bin.

1.6.8 PRODUCTION DATA CHANGES

CU*Answers employees and contractors are not permitted to make changes to production data without appropriate authorization (e.g. Data File Utility changes (“DFU”)).

1.6.9 PASSPHRASES AND PASSWORDS

Employees and contractors are responsible for safeguarding their passphrases and passwords for access to CU*Answers Computer Resources. Individual passphrases and passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passphrases and passwords. No Employees and contractors may access Computer Resources with another employee’s or contractor’s password or account, except in a support role with accompanying documentation. Employees and contractors should follow any passphrase or password guidelines as established by CU*Answers.

Passphrases and passwords do not imply privacy. CU*Answers has global passwords that permit access to all material stored on its Computer Resources regardless of whether that material has been encoded with a particular employee’s or contractor’s passphrase or password.

A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, The Traffic On The 101 Was &@< This Morning!). Passphrases are preferred whenever possible.

*CU*Answers offers management-approved Password Management software for generating and securely storing strong passphrases.*

1.7 SOCIAL ENGINEERING AVOIDANCE

CU*Answers employees and contractors should always be aware that criminals have interest in using social engineering techniques to gain access to sensitive information. The awareness and integrity of an employee is the best line of defense for protecting sensitive information.

Employees and contractors must be aware of the types of social engineering attacks. These may include, but not be limited to telephone, email, letter, personal contact or other electronic means (instant messenger, text messaging, etc.). In addition, social engineering may include any attempt by any individual (including internal employees or in-person contact) to gain information via pressure techniques - i.e. social pressure, social encouragement or simply being tricked or deceived. Employees should always avoid clicking on links or opening attachments from unknown or suspicious sources. If any employee or contractor encounters a social engineering attempt, the employee should contact the Security Incident Response team. For in-person social engineering attempts, the employee or contractor should contact a member of the Security Incident Response team or the employee’s immediate manager.

WHAT IS “CYBERSECURITY?”

Legally, cybersecurity refers to the regulatory laws governing computer (or information) security. These laws cover compliance requirements, penalties for non-compliance, and victim remedies.

In addition, victims may have a right to sue due to negligence in handing sensitive information, unfair or deceptive practices, breach of contract, or privacy violations.



TOP 10 THINGS TO KNOW ABOUT SECURITY AT CU*ANSWERS

ALWAYS USE A STRONG PASSPHRASE: Passphrases are stronger than passwords. *I want to go to Jupiter!* is better and easier to remember than *Jup!t3r!*. A best practice is for network passwords to be at least 12 characters. Passphrases and passwords must include two of the following three: special character, capital, or number. Spaces are considered special characters and are useful!

NEVER GIVE OUT YOUR PASSPHRASE: No employee should give out his or her password to anyone. If anyone ever asks for your password credentials over the phone or email, assume you are being social engineered. Contact the help desk at x266 and file a Security Incident Report.

USE SEPARATE PASSPHRASES FOR SEPARATE SYSTEMS: Never duplicate your password for the various systems. CU*Answers uses Password Safe to help our employees manage their passwords. If you have access to multiple systems, call our technology teams at x266 to have password management software set up for you.

NEVER SEND SENSITIVE INFORMATION INSECURELY: Personally Identifiable Financial Information (PIFI) is data that includes a person's name plus additional sensitive information such as the person's social security number, account number, or credit card number. This information can be used to compromise the person's identity or steal their funds. Any email that must contain PIFI going outside our network must be encrypted through approved technology. Our technology teams can show you how.

SHRED SENSITIVE INFORMATION: Documents containing PIFI should never be thrown in the trash. CU*Answers has several shred bins located throughout the organization. Ripping documents up is not sufficient. If there is any doubt about the sensitivity of the information in a document, use the shred bins. Documents with sensitive data should not be left unattended and should be locked in desk drawers when not in use.

KNOW THE BADGE RULES: There are three simple rules to follow regarding badges. Red badge visitors must be escorted when in a secure area. Individuals without badges must sign in and obtain a badge before entering a secure area. Never allow an unescorted visitor into a secure area. See the Building Security Policy for more information.

DON'T DOWNLOAD UNAUTHORIZED SOFTWARE: Software downloaded from an un-trusted source may compromise your system or the entire network. If you need software installed on your system, fill out the appropriate form.

AVOID OPENING ATTACHMENTS OR CLICKING LINKS FROM UNKNOWN SOURCES: Because we handle sensitive information on a daily basis, our employees will regularly be attacked by individuals looking to steal this data. Be very cautious if you receive an unexpected link or attachment in your email. Contact the help desk at x266 if you are not sure.

IF YOU BELIEVE YOU HAVE BEEN COMPROMISED, CHANGE YOUR PASSPHRASE IMMEDIATELY: Everyone has the potential to be the victim of a social engineering attack. If you believe you have been compromised, the first thing to do is change your password. Immediately changing your password can prevent an attack. Do this even before contacting the help desk at x266.

REPORT ANYTHING SUSPICIOUS TO SECURITY OFFICERS: Anything that might be suspicious should be reported to the security officers. This would include the help desk at x266 (who will escalate the call), the Internal Audit department at x335, the Administration team at x104, or Facilities at x119.

2 INFORMATION SECURITY POLICY AND PROGRAM

*Under our contracts with our clients, CU*Answers agrees to adhere to the laws protecting consumer information, including an Information Security program.*

Policy Owner: Network Services

2.1 POLICY PURPOSE AND OVERVIEW

The Guidelines for Safeguarding Member Information (Guidelines) set forth standards pursuant to sections 501 and 505(b), codified at 15 U.S.C. 6801 and 6805(b), of the Gramm-Leach-Bliley Act. These Guidelines provide guidance standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of member information. These Guidelines also address standards with respect to the proper disposal of consumer information pursuant to sections 621(b) and 628 of the Fair Credit Reporting Act (15 U.S.C. 1681s(b) and 1681w).

This Information Security Policy and Program is designed to:

- ensure the security and confidentiality of member information;
- protect against any anticipated threats or hazards to the security or integrity of such information;
- protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any member; and
- ensure the proper disposal of member information and consumer information.

The CU*Answers Information Security Program is designed to provide clear guidance to all staff on the minimum standards of data protection. This Program also provides guidance on the regulatory and contractual obligations CU*Answers must fulfill to continue in business. CU*Answers aspires to the best possible security of sensitive information within the bounds of commercial reasonableness. CU*Answers enforces this program through technical controls and audits.

2.2 KEY TEAMS

2.2.1 CORPORATE OFFICERS

The corporate officers of CU*Answers are the CEO, the CFO, and the COO.

2.2.2 SECURITY OFFICERS

The security officers of CU*Answers are any corporate officers, the EVPs of Technology or Software Development, the Internal Auditor, and the Facilities Manager.

2.2.3 INCIDENT RESPONSE TEAM

The Incident Response Team (IRT) consists of the following positions: Corporate Officers, Executive VPs, technological Managers related to any Incidents, and the Internal Auditor.

2.3 DATA CLASSIFICATION

CU*Answers relies on just two categories of data classification: data is either sensitive or not sensitive. Sensitive data must be protected in accordance with this Information Security Program and all policies of CU*Answers. Data that is not sensitive does not require security controls, although employees are cautioned to use information in accordance with the Employee Handbook and Acceptable Use.

EXAMPLES OF SENSITIVE MEMBER DATA

Examples of sensitive information include but are not limited to: the fact that an individual is the customer of a particular financial institution; consumer's name, address, social security number, credit card number, or account number; any information a consumer provides on an application; information from a "cookie" obtained in using a website; and information on a consumer report obtained by a financial institution (NOTE: Such information may also be covered by the Fair Credit Reporting Act).

2.4 PROGRAM IMPLEMENTATION

This Policy and Program is implemented by the CU*Answers Board of Directors. Executive management is responsible for oversight and reviewing reports submitted by the Internal Audit Team. Implementation of the Program is the responsibility of the Security Officers.

Vendors must agree to meet the requirements of the law if they have access to sensitive member information.

2.5 RISK ASSESSMENT

The program will have a risk assessment performed by the Internal Audit Team, which will be on no less than an annual basis and directed against the foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems.

This Program risk assessment will assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of member information.

The Program risk assessment will assess the sufficiency of policies, procedures, member information systems, and other arrangements in place to control risks.

2.6 MANAGE AND CONTROL RISK

CU*Answers will design the Information Security Program to control identified risks and implement commercially reasonable security controls, including: access controls on information systems with sensitive data; restrictions on physical access to information systems; reasonable efforts to provide encryption of sensitive information; procedures designed to ensure security during and after system modifications; as appropriate, dual controls procedures, segregation of duties, and employee background checks for employees; monitoring systems and procedures to detect actual and attempted attacks on or intrusions into information systems; response programs that specify actions to be taken when CU*Answers suspects or detects that unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies; review whether member information disposed of properly; and measures to protect against destruction, loss, or damage of member information due to potential environmental hazards, such as fire and water damage or technical failures.

Staff is trained to understand and implement this program. Controls will be tested both internally and by external parties. As part of this program, appropriate measures will be taken to properly dispose of member information.

2.7 AUDITS

Regular audits on the key controls and information systems is conducted by the Internal Audit Team. An annual report on the status of the Information Security Program will be part of the annual Audit Plan. The status will include the following information:

- The risk assessment
- The status of the controls
- Service provider arrangements

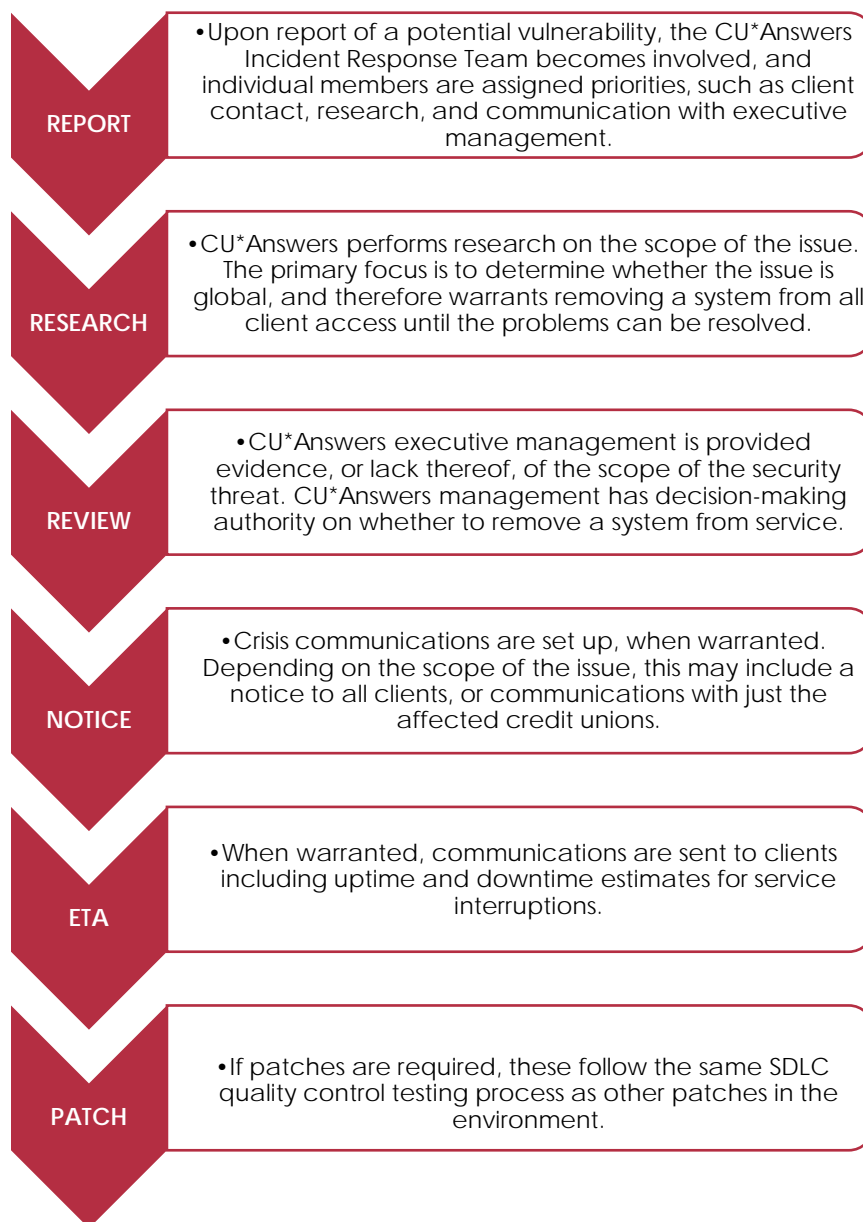
- Results of testing
- Breaches or violations reported to management

2.8 ACH

CU*Answers shall include as part of this Information Security Program compliance with the NACHA rules regarding “Protected Information,” insofar as these rules apply to CU*Answers. Although CU*Answers is not a financial institution, CU*Answers shall protect the confidentiality and integrity of Protected Information; and against unauthorized use of Protected Information that could result in substantial harm to a natural person, as it does with Sensitive Member Data.

2.9 INCIDENT RESPONSE PROTOCOL

The purpose of this policy is to provide guidelines for responding to a service or security issue broadly impacting one or more client credit unions. The basic process flowchart is as follows:



2.10 SERVICE OUTAGE

When a service CU*Answers provides directly or through a third party to one or more credit unions is substantially interrupted.

2.11 SECURITY BREACH

Defined as when CU*Answers is aware or suspects that a breach of sensitive data has taken place. A breach is whenever sensitive data has been exposed to an unauthorized party.

A breach of member data may result in a forensic investigation with the involvement of law enforcement and regulatory authorities.

2.12 SYSTEM OR APPLICATION VULNERABILITY

Defined as when a vulnerability has been reported in a system or application. A vulnerability is defined as a condition that creates the potential for sensitive data to be exposed to an unauthorized party.

2.13 NOTIFICATION

A CU*Answers employee who is aware of either a Service Outage, Security Breach, or System/Application Vulnerability should contact a security officer first. Then the employee should fill out either the CEO Incident or the Security Incident form.

2.14 FORM GUIDANCE

SERVICE OUTAGE	SECURITY INCIDENT	VULNERABILITY (HARDWARE OR SOFTWARE RELATED)
CEO Incident Form Discretionary	Security Incident Form Mandatory	Security Incident Form Mandatory

2.15 ROLES: INCIDENT RESPONSE TEAM

The IRT may be called together at any time an IRT member is aware of a potentially serious breach of security. If not already created, a Security Incident form must be filled out and sent to the Incident Response Team email group.

Incidents do not have to be confirmed in order to submit a Security Incident Report form; all employees are encouraged to use this form if they merely suspect and incident has occurred.

The IRT will coordinate resources to investigate and resolve the problem.

2.15.1 AUTHORITY TO ACT

The IRT has the authority to take appropriate and necessary steps to ensure the security, integrity, and availability of CU*Answers' networks. Decisions to remove systems or applications from production in order to contain a security breach should be cleared with the corporate officers or EVP of Technology or VP of Network Infrastructure before the action is taken. If none of these are available, any team member may remove the affected system or application from production. Immediately following such action, notification should be made to Client Services, Systems, and the Writing Team. Appropriate Alert messages should be posted, as necessary, to communicate the situation with clients.

Before a system that has been taken offline due to an incident can be put back into production, a statement in writing must be filed with the CEO indicating the incident has been contained, appropriate forensics have taken place or are not necessary, and the system has been appropriately sanitized.

2.15.2 USE OF THIRD PARTIES IN INCIDENT RESPONSE

Effectively responding to security breaches sometimes requires expertise of a nature not readily available on CU*Answers' staff. In such cases, CU*Answers' corporate officers may determine that outside expertise is necessary to effectively deal with the incident. In such cases, any of these positions may retain such help as necessary to deal with the immediate threat. All such activities must be documented and filed with the official incident report.

2.16 ROLES: CORPORATE OFFICERS

Provide guidance and leadership during a crisis, coordinating communication of the incident and remediation as needed. Corporate officers will make the determination to involve counsel, law enforcement, regulatory agencies, and the communication to clients and vendors.

2.17 ROLES: INTERNAL AUDIT

Responsible to communicate findings to corporate officers and staff as directed, to assess what changes need to be implemented going forward (and provide assurance the changes are implemented), to close out the incident and file a formal report to the Board of Directors.

2.18 CREDIT UNION SYSTEM VULNERABILITY

In some cases, CU*Answers might need to take the serious step of disabling access to a credit union system due to a security breach. This process will not be invoked until there has been a proper review of the incident.

*CU*Answers strongly recommends that the credit unions create internal procedures to handle this situation and educate staff on reporting responsibilities and escalation procedures.*

2.18.1 IDENTIFICATION

When a potential vulnerability is identified and reported to CU*Answers, the credit union and CU*Answers staff must document the exact circumstances that led to the discovery. Documentation should include the hardware and software tools and network components being used, and the business function that is vulnerable. No decisions will be made to suspend application availability at this stage. Only confirmed vulnerabilities can initiate a defensive system shutdown.

2.18.2 CONFIRMATION

CU*Answers will make an effort to confirm the vulnerability. If the vulnerability cannot be duplicated, CU*Answers will respond back to the credit union with our findings that the error condition could not be duplicated. If the vulnerability can be duplicated, an assessment will be made as to whether access to the credit union will be removed.

2.18.3 EVALUATE THE BUSINESS DECISION

"What is the risk of one more member being exposed?"

The IRT should initiate a system-wide shutdown if any of the following conditions are met: multiple libraries become exposed such that members of one credit union may view, add, modify, or delete data of another credit union's member; Users can log on to any CU without proper authorization (i.e. without a valid user ID, PIN, or CUID); or Confirmed exploitation of a member's computer (such as viewing, adding, modifying, or deletion of data) by use of the application.

The members of the IRT will have the responsibility of evaluating the business risk of continued application availability. This decision will be based upon the apparent risks to member privacy, risk of financial loss, and other potential liabilities created by the vulnerability.

If the vulnerability exposes multiple libraries, CU*Answers will initiate a system-wide application shut down. This would affect all home banking. This action would be accompanied by a redirect page explaining that the system was temporarily unavailable. System shutdown can be initiated by corporate officers. System reactivation must be approved in writing by the Corporate Officers.

If the vulnerability is limited to one library, CU*Answers will advise the client on a recommended course of action which may include disabling member access until a patch can be deployed. The IRT should recommend the shutdown of a given library if any of the following conditions are met: exposure of member data such that others may view, add, modify, or delete data of another member; ability to log onto a particular credit union without valid credentials or authorization; ability to log onto other accounts without valid credentials.

Even if CU*Answers cannot contact the affected credit union, Corporate Officers may shutdown the library if the risk is sufficient. Library reactivation must also be approved in writing by the Corporate Officers and a previously authorized employee of the Credit Union.

2.18.4 CREDIT UNION RESPONSE

If the credit union wishes to respond in a manner other than that recommended by CU*Answers, the credit union will supply CU*Answers with a written statement from an authorized representative outlining their desired course of action.

2.18.5 REPAIR

If the vulnerability resulted in a system-wide shut down, the process of developing a patch will commence the same business day as the system was shut down. All efforts should be made to develop and deploy a working patch as quickly as possible.

If the vulnerability affects one library, a working patch should be developed and deployed within one business day.

Programming will be tasked with creating a patch for the vulnerability as quickly as possible and advising the security team of the amount of resources and time it will take to implement. Once the patch has been developed and successfully tested it will be implemented and secondary production testing will immediately commence.

2.18.6 NORMAL BUSINESS RESUMPTION

After the patch has been successfully deployed, CU*Answers will inform the credit union that the issue has been successfully resolved or that the system is now ready to turn back on.

To reinstate deactivated libraries, a signed document from CU*Answers' Corporate Officers and from an authorized representative of the credit union must be received. Upon reception, a designated member of the security team will reactivate the relevant libraries to resume normal business operations.



PROTOCOL FOR CYBERSECURITY VULNERABILITIES

For Distribution to All Clients

ADDRESSING VULNERABILITIES

Major vulnerabilities may require CU*Answers to address the vulnerability by taking a system offline. In addition, when patching a vulnerability or disabling a service or system, it is possible it will have effects beyond the scope of our original analysis. In such a case, we rely on the experiences of our clients to let us know when our security protocol results in a lost service.

It is the default policy of CU*Answers to patch affected systems as soon as practical. When CU*Answers is aware that a service has been disabled, we will advise all of the clients affected through email or other means. CU*Answers will also provide expectations when services can be restored.

WHAT TO DO IF I WANT A SERVICE TURNED BACK ON FOR MY CREDIT UNION?

If your credit union chooses to accept the risk and wishes to have a service restored, the credit union can follow these steps:

1. Complete the Release of Liability Form (attached on the following page).
2. Have a credit union officer approve and sign the form.
3. Notify CU*Answers about the request.
4. If not already notified, CU*Answers will contact an executive officer regarding the request. Approval by an executive is needed before the service will be restored.

There are circumstances where CU*Answers will not turn on a service even if a waiver is signed. This would be a case where turning a service back on for one client could make other clients vulnerable, and these clients have not consented to having the service turned on. CU*Answers will attempt to find safe work-around solutions for clients; but this will not always be possible. As a cooperative, CU*Answers cannot turn on a service if there is risk to non-consenting clients or if there is additional risk CU*Answers might be exposed to if the service was restored.

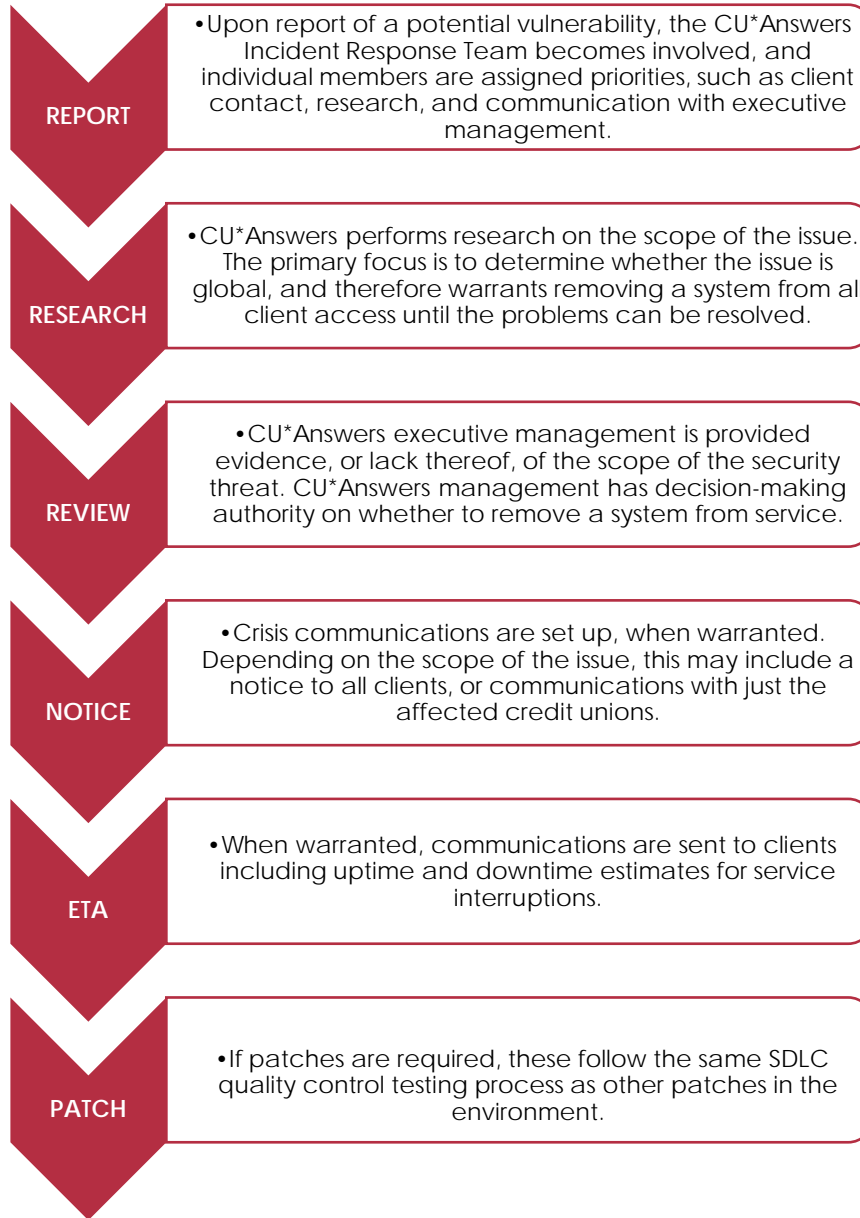
RELEASE OF LIABILITY [SAMPLE]

1. *[CREDIT UNION], and its officers, employees, directors, and agents, in consideration of such benefits and other good and valuable consideration, release absolutely, forever discharge, and covenant not to sue CU*ANSWERS, and its officers, employees, directors, agents, and business partners or software providers, from and concerning all liability, losses, claims, demands, actions, debts, and expenses of every name and nature for losses or other damages as a result of during, arising out of, or as a result of:*

[Describe the act or service involved in the cyber security vulnerability]
2. *[CREDIT UNION] reaffirms that software and other services provided by CU*ANSWERS cannot be guaranteed to be error free and agrees to implement reasonable processes to ensure the reliability and functionality of the software and services.*
3. *It is understood and agreed that this change is made in full and complete settlement and satisfaction the causes of action, claims and demands mentioned herein; that this Release contains the entire agreement between the parties; and that the terms of this Agreement are contractual and not merely a recital. Furthermore, this Release shall be binding upon the undersigned, and respective heirs, executors, administrators, personal representatives, successors and assigns. This Release shall be subject to and governed by the laws of the State of Michigan. This Release has been read and fully understood by the undersigned.*

CU*ANSWERS SECURITY PROTOCOL

CU*Answers has a well-defined protocol for responding to potential security emergencies. Our management follows a decision-tree to ensure that potential global vulnerabilities in our software are addressed. The process is as follows:



3 ACCEPTABLE USE POLICY

*The Acceptable Use Policy defines requirements for the use of Technological Resources owned and/or operated by CU*Answers.*

Policy Owner: Organizational Resource Development Team

3.1 POLICY PURPOSE AND OVERVIEW

CU*Answers relies on its computer network to conduct its business. To ensure that its computer resources are used properly by its employees, independent contractors, agents and other computer users, CU*Answers has created this Acceptable Use Policy. The rules and obligations described in this Policy apply to all users of CU*Answers' technology, wherever they may be located.

Technology that is the property of CU*Answers may only be used for legitimate business purposes. Users are permitted access to the technology to assist them in the performance of their jobs.

It is every employee's duty to use CU*Answers' technology responsibly, professionally, ethically, and lawfully. In the use of technology, Users must observe and comply with all other policies and guidelines of the company.

3.2 DEFINITIONS AND PROHIBITED USES

3.2.1 UNLAWFUL OR INAPPROPRIATE MATERIAL

Material that is fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by email or other form of electronic communications or displayed on or stored in CU*Answers' computers. Users encountering or receiving this kind of material should immediately report the incident to their supervisor(s).

Employees are prohibited from using CU*Answers Internet access or a CU*Answers provided device to view sites considered to be sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate to view.

3.2.2 OTHER PROHIBITED USES

Without prior written permission from a Corporate Officer, CU*Answers' Computer Resources may not be used for dissemination or storage of commercial or personal advertisements, solicitations, promotions, viruses or malware, political material, chain emails, or any other unauthorized use.

3.2.3 MISUSE OF SOFTWARE

Without either prior authorization or as part of a job function, Users may not do any of the following with software provided by CU*Answers: copy software for use on their home computers; provide copies of software to any independent contractors or clients of CU*Answers or any third person; install software on any of CU*Answers' workstations; modify, revise, transform, recast, or adapt any software; or reverse-engineer, disassemble, or de-compile any software. In their use of technology, Users must comply with all software licenses; copyrights; and all other state, federal and international laws governing intellectual property and online activities.

Users who become aware of any misuse of software or violation of copyright law should immediately report the incident to their supervisors.

3.2.4 UNSUPPORTED TECHNOLOGY

CU*Answers must strike a balance between innovation, effectiveness, and security when Users wish to install unsupported software or hardware which is not issued by CU*Answers. Unregulated installation of software and hardware may result in confidential data leakage, weak security, unavailability in a disruption, access control, and lack of "liquidity" of tools, where the vendor cannot be changed easily if the vendor fails to perform. However, in the interest of innovation and effectiveness, there is a process where tools can be approved for use by the organization.

3.2.5 APPROVAL FORM

Any request to use an unsupported application, regardless of origin (web, cloud, etc.) must be approved by the Network Services team (and possibly a Web Services representative in the case of web applications) before use is allowed. The requestor must complete form in detail and submit to team for review. The requestor's manager must approve the request before being submitted for approval.

3.3 NO EXPECTATION OF PRIVACY

Technology provided to Users by CU*Answers are to assist Users in performance of their jobs. Users should not have an expectation of privacy in anything they create, store, send, or receive on any technology, or with respect to calls and voice recordings made via the telephones and related voice technology owned and operated by CU*Answers. Technology owned by CU*Answers may be used only for business purposes.

3.4 ACCESSING THE FILES OF ANOTHER USER

Users may not alter or copy a file belonging to another user without first obtaining permission from the owner of the file. Ability to read, alter, or copy a file belonging to another User does not imply permission to read, alter, or copy that file. Users may not use the computer system to "snoop" or pry into the affairs of other users by unnecessarily reviewing their files and email.

3.5 ACCESSING OTHER COMPUTERS AND NETWORKS

A User's ability to connect to other technological Resources through the network does not imply a right to connect to those Resources or to make use of those Resources unless specifically authorized by the operators of those systems.

3.6 NO LOCAL ADMINISTRATOR RIGHTS

Users should not expect to have Local Administrator rights on their machines, unless an exception is granted by the Network Services team. Exceptions may be granted upon a showing of business need and completion of the proper form.

3.7 UNAUTHORIZED TECHNOLOGY OR SOFTWARE

Users are responsible and may be disciplined for any security breaches related to the use of unauthorized technology or software.

3.8 DUTY TO SECURE

Each User is responsible for ensuring that use of technology, as well as outside computers and networks, such as the Internet, does not compromise the security of CU*Answers. This duty includes taking reasonable precautions to prevent intruders from accessing the company's network without authorization, preventing introduction and spread of malware, and the use of other reasonable means to protect sensitive information.

Users must take reasonable steps to ensure sensitive information is maintained and transmitted securely. Users must not disclose sensitive information unless authorized by job description or by an officer of CU*Answers.

Consult the Cybersecurity Policy for additional information on the requirements for protecting sensitive information.

3.9 REMOTE DESKTOP SUPPORT

3.9.1 FROM THIRD PARTIES

Users may require a third party to provide remote desktop support, including WebEx and Citrix GoToAssist remote support tools. The following are the rules for obtaining remote desktop support from third parties.

3.9.2 PERMISSION REQUIRED

Users participating in remote access sessions with third parties must first obtain permission from their manager or supervisor.

3.9.3 PHYSICAL ATTENDANCE REQUIRED

A User participating must remain in attendance with the PC at all times in order to observe the actions of the third party.

3.9.4 SOFTWARE INSTALLATION REQUIREMENTS

Installation of software in a remote access session is governed by the software installation rules of this policy.

Users may need to support clients through remote desktop support. Users must adhere to all policies and procedures of CU*Answers while engaged in remote session support of a client.

3.10 ELECTRONIC COMMUNICATIONS

Examples of electronic communications include but are not limited to: email; messaging (both text and instant); and social media. A User should never consider electronic communications to be either private or secure unless encrypted with CU*Answers approved encryption software. Note that electronic communications may be stored indefinitely on any number of computers, including that of the recipient and any individuals the recipient has forwarded the electronic communications onto.

3.10.1 ENCRYPTION OF SENSITIVE INFORMATION

Users who send or receive sensitive information via electronic communications are required to use encryption when this information is sent out beyond the CU*Answers network borders (such as external email recipients).

3.10.2 NO EXPECTATION OF PRIVACY ON THE INTERNET

Users who post Information Internet should not be consider the data to be private or secure, even when a User is employing a private feature of an electronic communications site. Do not rely on the privacy controls of the provider to keep communications confidential.

3.11 LOGOS AND MARKS

Do not use without authorization the CU*Answer name, names of partners, clients or their logos that would infringe on the intellectual property rights of the owner. If a User has a personal blog where advice or opinion is offered on work-related matters, add a disclaimer to the homepage that states the comments are personal opinions and do not necessarily reflect the opinion of CU*Answers or any of its partners or affiliations.

WARNING

CU*Answers does not audit the personal electronic communications of Users with respect to non-work-related matters. However, should a personal electronic communication be brought to the attention of CU*Answers which adversely affects the reputation of CU*Answers or involves the unauthorized dissemination of sensitive information, this data may be used to discipline the User or terminate employment.

3.12 MOBILE/REMOTE COMPUTING AND ACCESS

CU*Answers recognizes that some Users may require mobile or remote access to technology. This access may include but is not limited to VPN access, a CU*Answers provided laptop or tablet, or access through a personal device. In addition to the other acceptable use rules encompassed in this policy, employees are required to follow these additional policy rules:

3.13 ENDPOINT SECURITY

As part of CU*Answers ongoing Data Leakage Control program, all devices shall be restricted to Read Only access for attached USB mass storage devices and optical media drives including but not limited to CD- ROM/CD-RW drives and DVD-ROM/DVD-RW drives. Data execute, write, and modify access is restricted. Where exceptions are made, member data must not be copied to, stored on, or moved by unencrypted USB mass storage or optical media. In order to have an exception, a form must be filled out and permission granted.

4 AUDIT POLICY AND EXAMINATION PROTOCOL

The Internal Audit Department provides objective assurance and consulting activity designed to add value and improve operations. The Internal Audit Department assists the Executive Management Team in accomplishing objectives by bringing a disciplined approach to value and improve the effectiveness of risk management, control, and governance processes.

Policy Owner: CFO

4.1 SERVICES

The Internal Audit department's consulting and advisory services provide management with assessments and advice advancing the goals and objectives of the organization. Internal Audit focuses on providing initial assessments, so risks may be identified and internal controls are designed at the beginning of a project.

4.2 SCOPE

The Internal Audit department reviews the organization's framework of risk management, internal control, and governance processes to determine if best practices are being followed concerning whether:

- Initiatives are operating within the highest standards and are directed toward the policies and procedures of the organization;
- Significant legislative or regulatory issues impacting the organization are recognized and addressed appropriately;
- Significant financial, managerial, and operating information is accurate, reliable, and timely;
- Resources are acquired economically, used efficiently, and adequately protected;
- Existing policies and procedures are appropriate and updated;
- Operations, processes and initiatives are consistent with established missions, objectives and goals and whether they are being carried out as planned;
- Risks within and outside the organization are appropriately identified and managed. Quality service and continuous improvement are in the organization's control process;
- Contractors meet the contract objectives, while in conformance with applicable laws, regulations, policies, procedures and best practices;
- Operations, processes or initiatives are reviewed at the request of executive management;
- Improvements to member service, management of risks, internal controls, governance, profitability, and the organization's effectiveness, efficiency and image may be identified during audits. This information will be communicated to appropriate levels of management;
- Risks within and outside the organization are appropriately identified and managed. Quality service and continuous improvement are in the organization's control process;
- Contractors meet the contract objectives, while in conformance with applicable laws, regulations, policies, procedures and best practices;

- Operations, processes or initiatives are reviewed at the request of executive management; and
- Improvements to client service, management of risks, internal controls, governance, profitability, and the organization's effectiveness, efficiency and image may be identified during audits. This information will be communicated to appropriate levels of management.

4.3 CONFIDENTIALITY

Documents and information given to the Internal Audit department shall be handled in the same prudent and confidential manner as employees normally accountable for them. Internal Audit staff will be instructed in the handling and safeguarding of confidential information.

4.4 AUDIT DEPARTMENT RESPONSIBILITIES

In order to meet the purpose, objectives and scope of this policy the Internal Audit department will endeavor to:

- Establish procedures for conducting activities according to the organization's policies and direction provided by executive management, and by professional standards;
- Select, train, develop and retain a competent internal audit staff that collectively has the abilities, knowledge, skills, experience, expertise and professional certifications necessary to accomplish the purpose, objectives and scope of this policy;
- Conduct an annual risk assessment and produce an audit plan that will accomplish the mission, objectives and scope of this policy. This plan will include some unassigned hours in order to provide flexibility for changing conditions. This plan shall in part be based upon risks and control concerns identified by management. This plan will be periodically updated as necessary;
- Implement the annual audit plan, as approved, including, as appropriate, any plan amendments, special tasks or projects requested by executive management;
- Coordinate with audit clients to finalize recommendations for improvement and identify implementation timelines. Internal audit staff shall consider costs and benefits while formulating and discussing their recommendations;
- Evaluate and assess significant new or changing services, processes, operations, and control processes coincident with their development, implementation, and/or expansion;
- Conduct periodic follow-up reviews to evaluate the adequacy of management's remediation;
- Issue periodic reports to executive management summarizing results of audit activities and the status of follow-up activities;
- Provide periodic summaries of consulting and advisory activities to management;
- Assist in the investigation of significant suspected fraudulent activities within the organization and notify management, as appropriate, of the results;
- Consider the scope of work of the external auditors and regulators, as appropriate, for the purpose of providing optimal audit coverage to the organization at a reasonable overall cost;
- Consult with the organization's management, as requested, on potential policy and procedure changes;

- Participate, in an advisory capacity, in the planning, design, development, and implementation and modification phases of major information related systems to determine whether: adequate controls are incorporated in the systems; adequate risk management techniques have been utilized; thorough systems testing is performed at appropriate stages; systems documentation is complete and accurate; and the intended purpose and objectives of the system implementation or modifications have been met;
- Participate in professional audit organizations by attending meetings, joining the governing boards, presenting speeches and papers, and networking with other professionals. Participate in other professional organizations related to the mission of the organization; and
- Act as the primary point of contact for handling all matter related to audits, examinations, investigations or inquiries of the external auditors.

4.5 STANDARDS OF AUDIT PRACTICE

The Internal Audit department shall follow the professional standards of relevant professional organizations.

4.6 REPORTING RESPONSIBILITIES

The Internal Audit department reports directly to the CFO. The Internal Audit department has responsibility to sign off on all internal audit reports presented to executive management. Executive management shall forward on these reports unedited to the Board of Directors for either acceptance or direction on how to modify policies and procedures. There shall be no fewer than six internal audit reports provided to executive management and sent to the Board of Directors each fiscal year.

The Internal Audit department shall be made consistently available to the Board of Directors for inquiry into any audit report findings.

4.7 ACCESS

The Internal Audit department members are granted authority for full, free and unrestricted access to all of the organization's functions, records, files and information systems, personnel, contractors, physical properties, and any other item relevant to the function, process or division under audit. All contracts with vendors shall contain standard audit language enabling the organization's internal auditors and other auditors and specialists access to relevant records and information when appropriate. All of the employees of the organization are required to assist the staff of Internal Audit department in fulfilling their audit functions and fiduciary duties.



EXAMINATION PROTOCOL

This document is intended to establish general guidelines for any agency, individual or audit firm performing an audit or regulatory exam at CU*Answers. This protocol is intended to streamline the audit process, ensure that all appropriate individuals are involved from the outset of the audit/review, reduce the overall time associated with the process, and assure that any audit findings are based on correct information.

If any procedures outlined result in significant burden on behalf of any department being reviewed or on the external audit firm or agency, the Internal Audit department will work with the department or auditor to modify this protocol as necessary.

SCHEDULING

Requests for audits should be made in advance to the Internal Audit department of CU*Answers. Advance arrangements ensure that the appropriate individuals are available to assist the examiners, relevant records are located and available, any interviews are scheduled to provide minimum disruption of departmental activities, and required facilities and services are available.

ENTRANCE CONFERENCE

The Internal Auditor or designated representative will schedule an entrance conference with the external auditing team. The entrance conference may be held by a teleconference if all affected parties agree. All parties must be aware that the meeting and subsequent discussion is intended as an entrance conference. During the entrance conference, CU*Answers requests that the external auditors provide the following information: scope of audit; timing of the audit, including estimated start and completion dates, deliverables and reports; requesting agency or individual as applicable, external audit team personnel, including designation of an audit lead; contact information and work schedules of onsite visits; and processes to allow the CU*Answers audit team the opportunity to review and comment on the deliverables and reports, including any draft findings and the final audit report.

As appropriate, weekly status calls and/or meetings may be requested and scheduled. Written track will be kept of all follow-up items, and these items will be reviewed at the next meeting.

CHANGES TO SCHEDULE

The Internal Auditor shall be informed as soon as possible of any known changes in audit timelines, deadlines or changes in scope, external audit team personnel, contact information or other pertinent or important information.

INFORMATION REQUESTS

All anticipated material and interview requests should be made at least 30 days prior to the audit start date. Information in these requests will be prepared and provided to the external auditors by the audit start date. Interviews will be scheduled by the Internal Auditor. All requests for information must be in writing, including the requested return date of the information. If the request for information is considered informal, the external auditor may contact the Internal Auditor, but the request must be followed up in writing. The Internal Auditor will inform the external auditors if the audit requests cannot be reasonably accommodated in the requested time and provide an estimated deliverable date.

ON-SITE REQUESTS AND INTERVIEWS

Information requests made on-site may take more than one day, depending upon the information requested. CU*Answers will make every reasonable effort to provide information in an efficient manner to external auditors.

CU*Answers requests a minimum of 48 hours to respond to and provide large data and information files to on- site external auditors.

An Internal Audit team member and appropriate personnel will accompany external auditors on all visits with CU*Answers staff. This includes walk through visits of any CU*Answers facility. Internal Audit team members may take notes and request follow-up meetings for clarification.

FINDINGS

Potential findings shall be communicated to the Internal Audit lead as soon as possible. CU*Answers shall have a minimum of thirty days to prepare and offer rebuttal to any potential findings. If any external auditor experiences a delay, lack of responsiveness, or an item of concern from CU*Answers personnel, the external auditor shall inform the Internal Audit team of the issue immediately. The Internal Audit team shall make every reasonable effort to assist in the resolution of the problem.

EXIT CONFERENCE

Upon notification from the auditors that the onsite audit has been completed, Internal Audit will schedule an exit conference. The exit conference may be held via telephone, teleconference or in person, as long as mutually agreed upon by all affected parties. The external auditors will not introduce any new findings or information at the exit conference. As long as proper protocol is followed, all issues, findings, information, and concerns will have been provided and discussed prior to the exit interview.

The external auditors shall provide written documentation of potential findings to Internal Audit. A mutually agreed upon response time shall be discussed during the exit interview or subsequent communication between auditors and CU*Answers.



5 BUILDING SECURITY POLICY

The Building Security Policy covers the responsibilities of employees with regard to building security (external and internal), key information, security cameras, and Operations fire and power systems.

Policy Owner: Facilities Management

5.1 SIGN IN REQUIRED FOR ACCESS

All visitors except young children are required to sign in and have badges for entrance into the secure areas of any facility owned or leased by CU*Answers. Young children must be escorted at all times by a CU*Answers employee. Visitors are never to be left unattended at a front desk reception area in any facility.

5.2 SECURE AREAS

All facilities owned or leased by CU*Answers are considered secure requiring a badge for access. Visitors must be escorted, except for the front desk and training areas in the 28th street ground level (including the hallway and restrooms in that immediate space), and the front desk/reception areas of each 44th street facility.

5.3 BADGE COLORS AND ACCESS

Badges must be visible at all times. It will be the employee's responsibility to advise the Administration Team immediately of any lost badge. Employees who lose their badges will be issued one free replacement; subsequent replacements will be \$10.00 each. Color of badges determines the level of access.

5.4 VISITORS WITHOUT BADGES

If CU*Answers employees encounter a visitor in a secure area without a badge, it is the responsibility of employees to politely inquire into the purpose of the visitor's visit. If amenable, the visitor should be escorted back to the front desk and be provided both a badge and an escort to their location. A Security Incident form should be filled out and sent to the Security Incident Response Team.

Red Badge	Yellow Badge	Blue Badge	Green Badge
Visitor	Approved Guests	Long Term Contractors	Employees
<i>Visitors must sign in and be escorted in all facilities at all times in secure areas</i>	<i>Must sign in, but do not require an escort through the facilities</i>	<i>Do not need to sign in or be escorted.</i>	<i>Do not need to sign in or be escorted.</i>



5.5 KEYFOBS

5.5.1 CONTROLS

Combinations and external keyfob control is the responsibility of the Administration Team. Records will be maintained to document changes and access granted. Office access is restricted and must be granted through either electronic verification of the employee's key-fob or personally by an employee.

5.5.2 LOSS OF KEYFOB

A loss of a keyfob must be reported immediately.

5.5.3 ACCESS BY LANDLORD(S) AND SECURITY CONTRACTOR

Special access privileges are granted to both the building landlord(s) and contracted security companies. These are outside of the key-fob policies so that these individuals can access the building in case of emergencies involving the physical building systems (such as a security alarm or dealing with an HVAC problem during off hours). Both the landlord and the security companies have keys to the building that will allow them to access all floors of both buildings, including restricted areas. However, in off-hours a CU*Answers employee must be present to disable the alarm.

5.5.4 NON-CU*ANSWERS VISITORS AND CONTRACTORS

The Administration Team will make the final determination if a non-CU*Answers visitor or contractor shall receive a keyfob. Client Services and Education may require this visitor or contractor to provide car keys or other valuables as a surety for the return of the keyfob.

5.6 BUILDING AND ALARM ACCESS

This section describes who may be granted the proper access codes to be able to arm/disarm the alarm and open or close the building. Specific job responsibilities or job titles that fall into each category outlined below are noted on a separate matrix maintained by the Administration and Facilities Teams.

New employees will not be granted access privileges to arm/disarm the building, regardless of job duties or other needs, until after their 90-day introductory period is successfully completed.

5.6.1 EMPLOYEES WHO CAN ARM/DISARM THE BUILDING SECURITY SYSTEM

In general, this group would include employees whose job responsibilities require them to be able to access the building outside of normal working hours, or to open building for the start of the business day. Job duties that routinely require off-hours access generally include supervisors and staff who perform after-hours maintenance.

5.6.2 EMPLOYEES WHO CANNOT ARM/DISARM THE BUILDING SECURITY SYSTEM

Employees who are not granted privileges to arm and disarm the building based on the reasons outlined above, can be in the building only during normal business hours or after an authorized person has disarmed and opened the building. All contractor employees will not be granted any access to the building and must ring the doorbell to gain access even during normal working hours.

Employees will be restricted as to which alarm panel they can use to disarm and arm the alarm system, according to where their primary workstation is located and/or where the job duties are being performed.

5.6.3 ALARM VERIFICATION

The Administration and Facilities Teams are responsible for the alarm verification. The VP of Administration or Facilities Manager will complete a CEO incident report on all set off alarms and report them the first business day after the incident to the CEO.

5.6.4 FALSE ALARMS

Employees who set off the alarm falsely will receive one warning before being potentially fined to cover any expenses charged to CU*Answers for these violations (such as the Police Department costs).

5.7 END OF DAY PROTOCOLS

The last employee to leave a secure area must have alarm privileges. It is the responsibility of this employee to activate the alarm at the end of the night. This is true for all floors. This employee is responsible to ensure no other employees remain in the secure area. This employee must also check to see that no coffee pots remain on and all lights are turned off.

WARNING

Any employee failing to activate the security system when they are the last to leave the building will be subject to corrective action ranging from suspension up to and including termination.

5.8 SPECIAL PROTOCOLS FOR THE KENTWOOD AND MUSKEGON FACILITIES

The perimeter electronic alarm system will be armed in the “stay” mode each evening by 12:00 midnight to warn personnel working in the building of any breach of the external perimeter during the third shift hours at this location.

5.9 RETURN OF KEYFOBS

It is the responsibility of both the Client Service and Education Team and the visitor’s sponsor to ensure all visitors sign out and return keyfobs at the end of the visit or at the end of each day. Under no circumstances may any visitor keyfobs to be taken off the premises.

5.10 EMPLOYEE SEPARATION

Employees who are terminated due to corrective action must be escorted immediately from the building, either by ORD or, depending on the employee’s position, the CEO/CFO or a member of the Board. In addition, all locks and combinations must be changed the same day.

5.11 KEYS AND COMBINATIONS

All personnel are required to lock and secure data and company information that is sensitive and should not be left available for the perusal of third parties.

5.11.1 LOSS OF KEYS

A loss of a key must be reported immediately to Administration, Facilities, a corporate officer, or a security officer.

5.11.2 DISTRIBUTION

Administration will maintain a copy of building keys in a secure location as well as detailed records to document key distribution.

5.11.3 MASTER KEYS AND SUB-MASTER KEYS

Officers and Facilities Managers have either Master or Sub-Master keys. A request for a Master or Sub-Master key must go through Administration. If an employee who has been granted either an external entrance key or master key leaves CU*Answers’ employ without returning their key, all locks and combinations will be changed immediately.

5.11.4 COMBINATION CHANGES

Electronic combinations will be changed as needed. If for any reason Administration or any other department head feels that security has been violated, the combinations will be changed immediately.

Employees should understand that revealing a combination to any other party will result in corrective action ranging from suspension to termination of the violating parties.

5.12 SPECIAL RESTRICTIONS

Several areas inside the CU*Answers offices have restricted access even to CU*Answers employees. These areas are restricted through the use of electronic strike systems with key-fob scan or manual combination locks.

5.12.1 MUSKEGON BUILDING ACCESS OFF HOURS

Four spare cards have been allocated for off-hours access to the Muskegon facility at the Kentwood facility, and one card at the 28th street facility. These are available to senior management, operations, or Information Technology employees on a need basis. Note that employees must have alarm access as well in order to access the Muskegon facility.

5.12.2 KENTWOOD AND MUSKEGON OPERATIONS CENTER / DATA ROOM

Only certain authorized employees will be allowed access to the computer room, including the Operations Center located outside of the main computer room. Employees granted access will include the following departments: Corporate Officers, VP of Administration and Facilities Manager, iSeries Administrators, Network Services, Internal Audit, Operations, and select Programmers. Occasional additional access may be granted on a case-by-case basis for special project needs and must be approved by a Corporate Officer.

5.12.3 28TH STREET DATA CENTER

Only certain authorized employees will be allowed access to the computer room located on the Garden Level, including the small Operations Center located outside of the main computer room. Employees granted access will include the following departments: Corporate Officers, VP of Administration and Facilities Manager, Series-i Administrators, Network Services, Internal Audit, Operations, Conversion Programmers, and select Programmers. Occasional additional access may be granted on a case-by-case basis for special project needs and must be approved by a Corporate Officer.

5.12.4 ACCOUNTING AREA

Only certain authorized employees will be allowed access to the accounting area, which includes accounting personnel workstations, located on the 2nd floor. Employees granted access will include the following departments: Corporate Officers, VP of Administration and Facilities Manager, Series-i Administrators, Network Services, Internal Audit, Human Resources, Accounting personnel, and Third-party auditors and examiners. Occasional additional access may be granted on a case-by-case basis for special project needs and must be approved by a Corporate Officer.

5.12.5 ACCOUNTING VAULT

Only certain authorized employees will be allowed access to the accounting vault located on the 2nd floor. Access is via a key only. Employees granted access will include: The CFO, Accounting personnel, VP of Administration and Facilities Manager, Human Resources personnel, Internal Audit, and any staff with a Master Key or Sub-master Key.

5.13 SECURITY CAMERAS

CU*Answers utilizes cameras to aid in visitor verification, key area monitoring, and vendor deliveries. Cameras are located at all major entrances and thoroughfares.

Security images are stored on a hard drive on the security computer located in the computer room. Network Services reviews functionality of the computer.

5.14 FIRE PROTECTION

All Data Centers are protected by dedicated independent FM-200 systems. To allow the FM-200 systems to function properly all computer room doors must be closed at all times to ensure the rooms are air tight. Natural gas generators and centralized Liebert UPS systems supply power continuance for the Data Centers at all three locations.

The main building systems are water pipe sprinkler type fire systems.

5.15 DATA CENTER FM-200 SYSTEMS

The FM-200 System removes heat energy from fire, not oxygen from the environment. FM-200 absorbs heat from the flame zone and interrupts the chemical chain reaction of the combustion process. Stored as a liquid in pressurized cylinders, FM-200 flows through a piping network to a discharge nozzle where it is deployed as a gas. The amount of FM-200 delivered to each nozzle is carefully calculated to ensure the appropriate concentration level.

FM 200 SYSTEM

When there is an emergency in the computer room and the FM-200 system is triggered and alarm will sound, and strobe lights will activate. The FM-200 compounds will not harm you, however prudence is the order of the day here and if the fire is serious, employees should evacuate the area immediately. If the FM-200 system is triggered, the power will be cut automatically to the Computer room. There is a yellow kill switch located on the wall to manually override a dispense event if necessary. There is also a red manual override switch to kill power to the room if necessary (i.e. in case of electrocution).

Inside each Data Center is a hand-held fire extinguisher that should be used for small, localized events.

Once the system has discharged, FM-200 and any harmful combustion byproducts can be removed from the space by simple ventilation. You can resume normal operations almost immediately once the fire has been extinguished and the fire department has provided you with an "all clear."



6 CLIENT SUPPORT POLICY

Because CU*Answers is responsible to protect the data of our credit union clients and members in the support process, this policy has been created to specifically enumerate what employees may or may not do during the client support process.

Policy Owner: Client Services and Education Team

6.1 SECURITY PROFILES

Employee ID 89 is the designated alias entry for CU*Answers Software Support staff. The security attached to Employee ID 89 will be changed at least every 60 days or when deemed necessary. Any time an employee leaves CU*Answers' employment, the security for Employee ID 89 will be changed immediately.

Each credit union will determine a policy regarding the security access allowed to Employee ID 89. The original policy will be filed in the client contract file. A scanned copy will also be stored in an internal network folder. CSR staff will honor this policy when performing telephone support.

6.2 CREDIT UNION SECURITY PROFILES

Each credit union will designate a security officer(s) responsible for updating their employee profiles. This person's name will be on file at CU*Answers (located in both the Client Service Area and in the Credit Union contract file). The CSR staff will not perform updates to a credit union's security in any way and will be instructed to work through the credit union's security officer.

6.3 DATA CENTER SECURITY PROFILES

For online credit unions, individual IDs will be assigned to all CU*Answers (data center) staff. Passwords can be reset only by using a Data Center Staff ID that has been granted administrator privileges. If a password must be reset, CU*BASE will force the password to be changed on the first use.

6.4 MAINTENANCE

It is CU*Answers' policy that CSR staff will not perform member transactions, member file maintenance, or general ledger entries on behalf of the credit union without express written authority from the credit union. The need to perform these functions should only arise when there is a deficiency in normal program processes. If it is determined that manual entry is appropriate, the credit union will always be notified, and appropriate written authorization will be maintained as necessary from appropriate credit union personnel with authority to approve such changes.

6.5 TRANSACTIONS TO MEMBER ACCOUNTS

The volume of member accounts affected will be evaluated and a determination between use of either a manual entry or program update will be made. Once approval is given, a properly authorized CU*Answers employee will perform the necessary transactions. Detailed listings of the transactions and any exceptions will be delivered to the credit union for their records.

6.6 MEMBER FILE MAINTENANCE

The volume of member accounts affected will be evaluated and a determination between manual entry or program update will be made. Once approval is given, a properly authorized CU*Answers employee will perform the necessary transactions. Detailed listings of the changes made will be delivered to the credit union for their records.

6.7 GENERAL LEDGER ENTRIES

The volume of entries will be evaluated and a determination whether a manual entry or a program update will be made. Once approval is given, a properly authorized CU*Answers employee will perform the necessary transactions. A JEID of

“WE” will be used on all journal entries made by client support staff. Detailed listings of the entries and any exceptions will be delivered to the credit union for their records.

6.8 SYSTEM CONFIGURATION MAINTENANCE

During the course of credit union development with CU*BASE, or as a result of software enhancements, the need to perform change to a credit unions configuration may arise. All changes will be documented with “before and after” detail, including supporting reasoning behind all changes. The credit union will always be notified, and appropriate written authorization will be maintained as necessary from appropriate credit union personnel with authority to approve such changes.



7 LARGE SCALE ABSENCE POLICY

This policy describes the procedures and controls implemented by CU*Answers to provide for continuation of business operations necessary to support our clients and partners should a large-scale absence impact our staff. For more information, see the current CU*Answers disaster recovery plan.

Policy Owner: Organizational Resource Development Team

7.1 LARGE SCALE ABSENCE PROGRAM

A large-scale absence, for purposes of this document, is defined by CU*Answers as missing 50% or more of the employee population for a period of up to 2 consecutive weeks. The determination that CU*Answers is experiencing a large-scale absence event will happen at the Corporate Officer level.

7.2 METHOD

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

7.3 CLIENT SERVICES

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

7.4 COVERAGE OF ALL SHIFTS

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

7.5 PRIORITIZING DAILY AND PENDING DUTIES

Time sensitive items must be considered. For example, if the timeframe is end of month, team members must be diverted across departments in order to complete important tasks. Management would make decisions on readjusting the priority list and delay of non-critical project travel.

7.5.1 PROGRAMMING

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

7.5.2 MANAGING PROJECT TIMELINES

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

7.5.3 RESPONSIBILITY FOR RESULTING CU*BASE ISSUES

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

7.6 DELIVERY

7.6.1 DELIVERING THE SERVICE TO THE CLIENTS WITH QUALITY

For services that require travel, employees will be expected to be aware of their ability to complete their responsibilities without negative effects on the client. If necessary (i.e. in a conversion situation) CU*Answers'

management may need to make a decision regarding whether or not more employees will need to be sent to supplement for the unavailable employees. For services delivered from our offices, cross-training and up to date documentation will be necessary to be able to continue to provide quality service. In some cases, CU*Answers and Xtend have relationship(s) with Staffing Agencies if additional staff is needed.

7.6.2 HANDLING TIME ESSENTIAL DUTIES

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

7.6.3 AT THE CLIENT SITE

In a scenario where an entire team is unable to perform duties:

- Until additional staff can arrive on site, web and phone conferences would have to be utilized for training, support, sign-off etc. Several concurrent sessions could be scheduled to facilitate training by department;
- Depending on the location of the credit union, the COO may tap other CU*Answers credit union employees as support staff;
- If the Credit Union is going through an event, the alternatives for sign-offs, etc. are as follows: CPAs and Board members may be used as alternatives to a CEO for sign-off authorization; and
- Additional support may have to be rescheduled for a particular department, i.e. 'live week' may be postponed if several credit union employees are unavailable for the necessary training.

7.7 OPERATIONS

7.7.1 SHIFT COVERAGE AND GENERAL DEPARTMENT RESPONSIBILITIES

Adjust schedules of remaining team members to cover all shifts and run with reduced staff per shift. Managers will provide additional coverage as needed. Beginning of Day, End of Day, and File Transmissions must be delegated to other trained team members in the absence of Operators from the shift on which the processes are carried out. Operations cross-trains team members on an ongoing basis to ensure delivery of time-sensitive items. An e-mail/call chain is in place in order to contact the Operations Team to let them know of any changes in shift and duties they must fulfill as the situation changes.

7.7.2 CROSS-DEPARTMENTAL COVERAGE OPTIONS

The Operations department can also look outside of its own department in an event. Employees from other teams can be drawn upon to cover gaps in processing shifts in the event of a serious shortage in Operations staff.

7.8 COMMUNICATION

If Corporate Officers declare a large-scale absence event has occurred at CU*Answers, clients shall be notified via the Emergency Notification System.

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

7.9 TRAVEL DURING AN EVENT

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

7.10 ADDITIONAL PANDEMIC POLICIES

If the absence is due to a pandemic disease, the following additional controls are required: infected staff should defer coming to work for the length of the incubation period of the virus; staff should utilize the hand sanitizing stations provided around the office and wash hands often; clean keyboards and other equipment, especially if workstations are shared between staff members; a certain degree of social distancing could be practiced; reducing frequency, proximity, and duration of contact can also help reduce the spread.

Staff interactions during an event will be decided upon by CU*Answers Corporate Officers and communicated to the employees through ORD. Depending on the circumstances surrounding the event, decisions will be made regarding: severely discouraging or disallowing large assemblies of employees (on or off work premises); closing all meeting rooms; limiting all staff interactions as much as possible; encourage or force employees to work at home or at other CU*Answers offices; and/or offering masks and setting up for cleaning stations around the office.

8 RECORDS AND INFORMATION MANAGEMENT POLICY

This policy provides CU*Answers with guidelines for properly establishing a Records and Information Management (RIM) Program, and assisting those departments that require long-term records retention. The goal is to provide CU*Answers with a policy that provides compliance with our legal, regulatory, and contractual obligations.

Unless mandated by law, regulation, contractual obligations, or as the result of a litigation hold, there is no legal duty to preserve information generated in the course of business.

Policy Owner: CFO

8.1 SCOPE AND DEFINITIONS

Records and information management (RIM) is the systematic control of all records, regardless of media, from the point of their creation or receipt, through their processing, distribution, organization, storage, and retrieval, all the way to their final disposition. Information flows through the organization in the form of paper and electronic records including but not limited to word processing documents, spreadsheets, e-mail, graphical images, and voice or data transmissions. Information can be stored on a variety of storage media, such as microfilm, microfiche, diskette, optical disk, CD-ROM, videotape, and paper.

8.2 PRINCIPLES

This policy details the requirements and responsibilities to initiate a well-defined RIM program. The RIM program applies to those departments that require a long-term records-retention, -storage, and -disposition program. Absent specific, written provision to the contrary, it is presumed that the RIM program applies to all departments within the CU*Answers.

8.2.1 INTERNAL RECORDS ONLY

This policy applies to CU*Answers' records and information. Records and information managed for clients is governed by the clients' own RIM policies and the agreements between the clients and CU*Answers.

8.2.2 PRESERVE ONLY RECORDS OF VALUE

Ensure only essential records of continuing value are preserved. Records should be retained in the active office areas as long as they serve the immediate administrative, legal, or fiscal purpose for which they were created.

8.2.3 ESTABLISH SAFEGUARDS

Establish safeguards against the illegal removal, loss, or destruction of records. Records either should be disposed of in accordance with an approved records-retention schedule or transferred to the records-retention center until the prescribed retention period has expired.

8.2.4 RESPONSIBILITY OF OWNER/CREATOR

Management of records is the responsibility of the owner or creator, of the record. CU*Answers will ensure that one or more Records Managers will be designated for each department to assist in the implementation of the RIM program. The department director or the director's designated representative should remain in periodic contact with the Records Manager to discuss initiating the records-management program or reviewing an existing records-management program to handle records properly from their creation through their destruction. Departments can be provided guidance on how records should be organized and stored to ensure timely and efficient retrieval.

8.3 RETENTION SCHEDULE

The records-retention schedule is the key tool for departments to use to manage their records effectively. Information is a valuable asset; however, if records that contain information cannot be retrieved efficiently or are retained beyond their legal, regulatory, or administrative retention period, they lose their value and may impose a liability to CU*Answers.

8.4 RECORDS LIAISONS

Departmental Records Liaisons are responsible for: training staff on record retention procedures; assisting in developing and enforcing the records-retention schedule for their department; managing the department's records; attending records liaisons' meetings; assisting in the implementation of any litigation hold(s) enacted by the CU*Answers.

8.5 COORDINATE CHANGES

The CFO shall cause departmental activities to be coordinated with the Records Liaison to include approval of new or replacement records storage and file equipment as requested.

8.6 MINIMUM REQUIREMENTS

8.6.1 RECORDS-RETENTION SCHEDULES

Each department is responsible for determining retention periods for records created. A record may be kept beyond the legal or regulatory retention period if it satisfies an administrative need based on business necessity, which is stated on the records-retention schedule.

A Records Retention schedule will have the following minimum characteristics: an inventory all current records maintained, including all media types; a master list of data and record types and draft preliminary retention schedule; retention periods will be based on legal, contractual, administrative, and historical value; final approval for retention schedule is from the Accounting Manager; the retention schedule will be audited annually.

8.6.2 RECORDS-DESTRUCTION SCHEDULES

Each department is responsible for destroying any paper or electronic record once the specific retention period for any paper or electronic record has been reached. Notwithstanding minimum retention periods, all records shall be maintained until all required audits are completed and shall be kept beyond the listed retention period if a litigation hold is enacted (see Litigation Hold Policy).

Destruction of records is permitted in accordance with the law only after expiration of the retention periods stated on the approved departmental retention schedules.

8.6.3 COMPLIANCE AND AUDITING

The company shall annually inventory records to confirm information in the records- retention tracking system; the Records Manager will have the records-retention schedule reviewed and validated annually for accuracy; the Records Manager will advertise and initiate an annual files purge by all departments. The purpose is to have individuals review personal active file systems, as well as electronic document folders, and to purge documents that are no longer required.

8.6.4 ANNUAL RECORDS DESTRUCTION PROGRAM

The Records Manager will annually inventory all records that have been kept past their retention schedule. The Records Manager will confirm with each department that the records can be destroyed before initiating record destruction. The Records Manager will record all instances of electronic or physical destruction of documents as part of the audit report.



LITIGATION HOLD

If a litigation hold is enacted, the Internal Audit Team will be responsible to manage the litigation hold. If a litigation hold is appropriate, the hold notice should be issued as soon as practical. The notice should identify the data that are subject to the litigation hold and advise all employees not to delete, overwrite, or otherwise alter or destroy any records (paper or electronic) that may contain information that is reasonably related to the identified subject matter. The notice should also make clear that this obligation applies to records that currently exist or are created in the future. The litigation hold notice should include directions to all CU*Answer employees to advise if that employee has any paper or electronic records related to the litigation hold in his or her possession so that the information can be collected in a timely manner. The notice should also describe all the types of media where records may be stored—e.g., laptops and all other portable devices, such as cell phones, PDAs, home computers, and voice mail. The notice should advise that all data, even data on back-up tapes, should not be overwritten or rotated until further notice.

IDENTIFICATION OF "KEY" EMPLOYEES

CU*Answers shall identify employees likely to have paper or electronic records that are subject to the litigation hold ("key employees") by reviewing relevant documents and sending a follow-up e-mail to all employees. Key employees must confirm their understanding of the litigation hold and to request that they gather the paper and electronic records in one location for collection.

COLLECTION OF APPLICABLE RECORDS

Internal Audit should work with appropriate support staff to develop a plan for the systematic and orderly collection of all paper and electronic records subject to the litigation hold. A personal meeting with each key employee to confirm that all paper and electronic records have been identified and collected should be conducted and documented. Records subject to the litigation hold should be stored in a central location where they can be cataloged. All key employees should sign a document verifying that to the best of their knowledge they have identified and turned over all paper and electronic records subject to the litigation hold.

PRODUCTION OF APPLICABLE RECORDS

Internal Audit will be responsible for coordinating any production of documents outside CU*Answers. Internal Audit should update the key employees and CU*Answers' responsible lawyer(s) as needed regarding the status of the litigation hold. Internal Audit should periodically remind all key employees (and any other personnel newly assigned to the applicable matters) of their continuing obligations to preserve records under the litigation hold. Internal Audit will be responsible for determining when a litigation hold is no longer necessary. Copies of all communications regarding the litigation hold should be sent to Internal Audit so that a complete file regarding the CU*Answers' efforts to comply with the litigation hold is maintained. Any questions regarding this policy or its implementation should be directed to CU*Answers' responsible lawyers.

9 VEHICLE POLICY

The purpose of this policy is to ensure the safety of individuals and to outline the expectations and guidelines for utilizing a company vehicle, rental vehicle, and/or a personal vehicle for company business. It is the drivers' responsibility to operate the vehicle in a safe manner to prevent injuries and property damage. CU*Answers endorses all applicable state motor vehicle regulations relating to driver responsibility.

Policy Owner: Administration Team

9.1 COMPANY VEHICLES

"Company Vehicles," for purposes of this policy, pertain to all vehicles in the pool available to all eligible employees travelling on Company Business and to any vehicles leased by CU*Answers for use by a specified individual.

9.2 RENTAL VEHICLES

"Rental Vehicles," for the purpose of this policy, pertain to all vehicles rented by CU*Answers to eligible employees travelling on Company Business.

9.3 COMPANY BUSINESS

"Company Business" for the purpose of this policy, pertains to any activity the employee engages in under the direction of, or on behalf of, CU*Answers. This does not pertain to regular commuting to and from work.

9.4 DRIVING-RELATED POSITION

A "Driving-Related Position" for the purpose of this policy, pertains to a position that has been determined by CU*Answers to require driving of either the employee's personal vehicle or a Company Vehicle for Company Business.

9.5 SCOPE

The policy applies to all use of Company Vehicles, rental vehicles and the use of personal vehicles for Company Business.

9.6 ELIGIBLE DRIVERS

Every employee who either operates a Company Vehicle, a rental vehicle, or operates a personal vehicle on Company Business must have a valid and current Driver's license. Current auto insurance is required for any use of a personal vehicle for Company Business. Drivers are required to provide proof of insurance and a state- issued driver's license on no less than an annual basis.

Motor Vehicle Records are obtained: 1) prior to employment on all candidates for Driving-Related Positions; and 2) periodically during employment as deemed appropriate by CU*Answers on all employees performing Driving-Related Positions. Consent to such inquiries is a condition of employment in a Driving-Related Position. An unacceptable driving record will result in disqualification for a Driving-Related Position.

Any employee in a Driving-Related Position who has a driver's license revoked or suspended will immediately notify the ORD Team within 24 hours of the revocation or suspension and immediately discontinue use of Company Vehicles or driving on Company Business. Failure to follow this procedure may result in disciplinary action up to and including termination.

WARNING

All accidents that occur in Company Vehicles, regardless of severity, must be reported to the police and to the ORD Team immediately. This same procedure must be followed when operating a rental vehicle or personal vehicle while on Company Business. Failing to follow this procedure may result in disciplinary action up to and including termination.

Drivers must report to the ORD Team all ticket violations received during the operation of a Company Vehicle, rental vehicle or while driving a personal vehicle on Company Business, within 1 week of the occurrence of the ticket. Failing to follow this procedure may result in disciplinary action up to and including termination.

9.7 DRIVING RECORD CRITERIA

Employees in Driving-Related Positions are expected to maintain good driving records and follow the reporting criteria above when incidents that affect their record occur. If a pattern of unsafe or irresponsible driving is detected, a decision may be made to suspend or revoke the driving privileges of the employee at the discretion of the company officers.

Criteria of an unacceptable record may include, but not limited to: three or more moving violations in a year. Violations include any ticket, citation, or other law enforcement determination relating to these; three or more chargeable accidents within a year where chargeable means the driver is determined to be the primary cause of the accident through speeding, inattention, etc. Factors such as weather or mechanical problems will be taken into consideration; any combination of accidents and/or moving violations; any driving violation or infraction that results in the employee being ineligible for insurance coverage under the policy or policies applicable to Company Vehicles.

9.8 ACCEPTABLE USE OF VEHICLES

Company Vehicles are to be driven by authorized employees only and limited to use for Company Business except as otherwise authorized in writing by CU*Answers.

With respect to any driving for Company Business, travel should generally be limited to that necessary for the Company Business, and not include significant deviations from route or schedule for personal matters. This provision does not preclude incidental, occasional personal stops provided they do not interfere with the employee's performance of his or her duties.

9.9 DRIVER SAFETY RULES

Any violation of the safety rules below while operating a Company Vehicle, rental vehicle or a personal vehicle for Company Business will be grounds for disciplinary action up to and including termination:

The use of a mobile device for written communication, including but not limited to texting and emailing, is strictly prohibited. The law in Michigan defines that a person shall not read, manually type, or send a text message on a wireless 2-way communication device that is located in the person's hand or in the person's lap, including a wireless telephone used in a cellular telephone service or personal communication service, while operating a motor vehicle that is moving on a highway or street.

Cell phone use for verbal communication while driving should be kept to a minimum. Drivers need to be aware when use of the cell phone is creating a distraction from safe driving and adjust their usage accordingly, including pulling off the road to continue and/or finish the conversation if needed. Whenever possible, drivers should complete calls while the vehicle is parked and/or use the phone in a "hands free" mode via a headset or speaker.

All drivers and passengers operating or riding in a Company Vehicle or rental vehicle must wear seatbelts, even if air bags are available.

Drivers are responsible for the security of Company Vehicles and rental vehicles assigned to them, ensuring keys are removed and doors are locked when the vehicle is unattended. Employees may often be travelling with company or client property in the vehicles; proper precautions must be taken to ensure the safety and care of this property.

All laws must be obeyed.

9.10 MAINTENANCE AND ADMINISTRATION

Keys to the pool of available Company Vehicles are kept in the office of the VP of Administration. These keys must be returned after each use of the vehicle. Vehicles in the pool available to employees must be reserved for use and are available on a first come first serve basis. Employees must use the Company calendar to reserve the use of a Company Vehicle through the resource booking feature. When the Company Vehicles are not in use they are to be left in CU*Answers' Main office parking lot. The mileage log booklets must be completed by the employee after/during each use and is to be kept in the glove box of each Company Vehicle.

The Company Vehicle should always be returned clean and with a full tank of gas when possible; please notify the Facilities Management if the tank is half full or less when you return to the office.

9.11 SMOKING IN COMPANY VEHICLES IS STRICTLY PROHIBITED.

Each Company Vehicle shall be regularly maintained by the facilities technician. Any necessary maintenance or repairs detected by the employee while operating the vehicle shall be reported to Facilities immediately.

10 VENDOR MANAGEMENT AND PROCUREMENT POLICY

Security and privacy of information is vital to the business of CU*Answers. Our service providers who access sensitive information must also abide by the guidelines as established by law. The vendor management policy requires CU*Answers to provide appropriate due diligence with key service providers prior to entering into or renewing an agreement.

In addition, CU*Answers has a responsibility to its client-owners to manage large scale projects efficiently. CU*Answers will not approve large scale capital projects without going through a formal vetting and project management process.

Policy Owner: CFO

10.1 VENDOR MANAGEMENT PROGRAM

The Vendor Management program is to help mitigate and manage that risk. Risks may include:

- Reputational risk through the misuse of sensitive or confidential data;
- Transaction risks such as fraudulent activity;
- Strategic Risk relative to the dependency of service provided; and
- Compliance risk primarily in the area of GLBA

A regular review of these vendors and their continued ability to provide services in a safe and sound manner is an essential process in mitigating these risks.

10.2 OVERSIGHT

Vendor oversight through this program is the responsibility of the sponsoring team and the Corporate Officers. Not all vendors are subject to this level of risk review as determined and documented during the risk assessment process.

10.3 VENDOR RISK RATINGS

10.3.1 10.3.1 TIER I

Tier I vendors pose the highest degree of risk and require the largest degree of ongoing due diligence. Vendors that fall under this tier generally meet one or more of the following criteria:

- Have access to, transmit, or store a large amount of non-public member data;
- Would have a significant impact on income and expense statement in the event of its dissolution or contract termination;
- Would be difficult to replace in a reasonable period of time while seriously disrupting service;
- Have high level access to IT infrastructure behind the firewalls where corporate secrets and member information reside; and/or
- Have access to the facilities in an unescorted manner and in doing so may also have access to member data.

10.3.2 TIER II

Public Companies that provide a service technical in nature that may house member data. A Tier II company may also have a significant impact on income and expense statements.

10.3.3 TIER III

Tier III vendors generally will have some degree of access to non-public member data, they are not as difficult to replace quickly, and have no access to the credit union's network or physical locations. Typical vendors that fall into this category would be private mortgage and credit life and disability providers.

10.3.4 TIER IV

These vendors would consist of public companies that could be viewed as vital to the community infrastructure. If a company of this type were to fail it would have regional catastrophic effects. Companies that fall into this category generally are the public utilities. These companies are considered critical, however the failure of these types of companies is highly unlikely as they are vital for the community or region to survive. Contingency and disaster recovery plans or more important in this case to manage the impact of their failure vs. the management of the vendor relationship. Examples of these type of companies would include DTE Energy or Consumers Energy.

10.3.5 TIER V

Companies that fall into this tier may come into contact with member data or have physical access to the facility. Generally, these companies would have very little direct access to information, can be replaced very quickly, and would have little if any impact on the ongoing business operations of the credit union if they fail.

10.4 EVALUATION PROCESS

Based upon categorization CU*Answers will require some or all of the following events tracked:

- News feeds.
- Annual or audited financial statements (or quarterly financials if it is an owned CUSO).
- Publicly available control audit.
- Insurance/bond.
- Internal network infrastructure audit or penetration test.
- Disaster recovery/business resumption policies and annual testing.

The following items are those that may be reviewed during the due diligence process:

- Review of financial statements, preferably audited statements.
- Review of insurance coverage.
- Contacting references and user groups.
- Determination if service provider performs background/reference checks on its new employees.
- Determination if third parties/contract employees would support the service provider in fulfilling its requirements.
- Conclude if the service provider uses third parties/contract employees. If so, what type of due diligence they perform on those third parties.
- Perform an onsite visit, if applicable.
- Review SSAE report if applicable.

- Determine service provider's knowledge of GLBA, Regulation E, Privacy Act, Consumer Protection and Bank Secrecy Act.
- Determine how long the vendor has been in business.
- Conclude on the vendor's experience and ability to provide service in question.
- Review disaster recovery/business resumption plan of vendor.
- Determine security precautions implemented, such as firewalls, encryption, authentication, etc.
- Compare market share in the given service area to competitors.

10.5 EVALUATION REPORTING

The assessment and analysis of all vendors will be completed, and then on an annual basis vendors will be evaluated to determine if the criticality status has changed. Reports of vendor reviews, along with any specific recommendations, will be presented to the Board of Directors at least once a year.

10.6 CAPITAL EXPENDITURE PROCUREMENT

For any capital expenditure, defined as an expense greater than \$10,000.00 a process will be invoked to provide due diligence on the process. Staff or management must fill out the appropriate form for any capital expenditure requests above \$10,000.00. The form must be filled out completely and submitted to management approval (unless management is the CEO or CFO). The form will then be reviewed by Internal Audit, who will complete a risk assessment and attach that to the form. The form will go to the CFO for review and approval, and then to the CEO for the same.

If approved, the Administration team will track the project's process. The requesting team will be required to provide updates on the status of the project. Status reports will be provided regularly to the board of directors.