

CU*ANSWERS

Policy Manual

Revised April 2022

CU*ANSWERS

Our Next Adventure



Table of Contents

01. CYBERSECURITY	4
02. INFORMATION SECURITY	12
03. ACCEPTABLE USE	24
04. AUDIT	32
05. PHYSICAL SECURITY	40
06. CLIENT SUPPORT	46
07. LARGE SCALE ABSENCE	50
08. RECORDS AND INFORMATION MANAGEMENT	54
09. VEHICLE	60
10. VENDOR MANAGEMENT AND PROCUREMENT.....	66

CU*ANSWERS

Policy Manual Overview

Policies Approved
by the
CU*Answers Board of Directors

This Policy Manual establishes a set of 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. Our Organizational Resource Development and Internal Audit Teams are available to discuss policy requirements in detail with employees. Employees are encouraged to submit proposed revisions to policies at any time.

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.

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, and the Acceptable Use Policy.*

Policy Owner: Network Services

01

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, the non-public personally identifiable financial information of both credit union consumers or members, and 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 (including 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 the 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.

1.2 SENSITIVE INFORMATION CLASSIFICATIONS

1.2.1 NON-PUBLIC PERSONALLY IDENTIFIABLE FINANCIAL 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 specific financial consumer or household.

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. Confidential client or vendor data is any data regarding client or vendor business 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 the data's 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 must 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 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 in a commercially reasonable timeframe any security breach 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:

1. Was publicly available or in the public domain at the time of disclosure,
2. Becomes publicly available or in the public domain through no fault of CU*Answers,
3. Is in CU*Answers possession free of any obligation of confidence to the disclosing party at the time of disclosure, or

4. 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

Staff must use encrypted methods authorized by CU*Answers before sending confidential information to parties outside of the organization.

1.6.2 ENSURE AUTHORIZATION

Staff are required to have reasonable assurance that any recipient of confidential information is authorized to receive the sensitive information prior to sending.

1.6.3 DO NOT DISCLOSE UNLESS AUTHORIZED

Staff are permitted to disclose sensitive information only when authorized to do so. Staff should never disclose information if they have any doubt that they have authority to do so.

1.6.4 STORE SENSITIVE INFORMATION SECURELY

Staff 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 any local machine or mobile device.

1.6.5 DATA LEAKAGE

Staff 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 CU*Answers to do so.

1.6.6 NOTIFY WHEN SUSPECTED SECURITY INCIDENT OCCURS

Staff are required to notify CU*Answers 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

Staff are responsible for safeguarding their passphrases and passwords for access to CU*Answers Computer Resources. Individual passphrases and passwords must not be printed, stored insecurely, or given to others. Users are responsible for all transactions made using their passphrases and passwords. No employees nor 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.

1.7 SOCIAL ENGINEERING AVOIDANCE

CU*Answers employees and contractors should always be aware criminals will use 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.

Staff 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.

Staff should always avoid clicking on links or opening attachments from unknown or suspicious sources. 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.

TOP 10 THINGS TO KNOW ABOUT SECURITY AT CU*ANSWERS

ALWAYS USE A STRONG PASSPHRASE

Passphrases are stronger than passwords. A best practice is for network passwords to be at least 12 characters. Passphrases and passwords must include two of the following three requirements: special character, capital letter, 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 socially 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 technology 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 sensitive information going outside our network must be encrypted through approved technology. Our technology teams can show you how to utilize encryption.

SHRED SENSITIVE INFORMATION

Documents containing sensitive information 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 AND SECURE AREA 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.

DO NOT 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 and the employees' manager. This would include the Help Desk (who will escalate the call) or the Internal Audit department at x335. Complete a Security Incident Form as soon as possible to alert the organization.

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 handling sensitive information, unfair or deceptive practices, breach of contract, or privacy violations.

WHAT IS A "PASSPHRASE"

A passphrase is like 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.

INFORMATION SECURITY POLICY AND PROGRAM

*As part of our client contracts, CU*Answers agrees to adhere to the laws protecting consumer information, including implementing an Information Security program.*

Policy Owner: Network Services

02

2.1 POLICY PURPOSE AND OVERVIEW

The Guidelines for Safeguarding Member Information (Guidelines) sets 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:

1. Ensure the security and confidentiality of member information;
2. Protect against any anticipated threats or hazards to the security or integrity of such information;
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any member; and
4. 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

2.1.1 CORPORATE OFFICERS

The corporate officers of CU*Answers are the C-Level employees (e.g., the Chief Executive Officer/CEO).

2.1.2 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.

2.1.3 INCIDENT RESPONSE TEAM

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

2.1.4 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 Policy.

2.3 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.

2.4 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.

2.5 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.

2.6 AUDITS

Regular audits on the key controls and information systems are 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:

1. The risk assessment;
2. The status of the controls;
3. Service provider arrangements;
4. Results of testing; and
5. Breaches or violations reported to management

2.7 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.

2.8 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 on the following page.

INCIDENT RESPONSE PROTOCOL

REPORT. Upon report of a potential vulnerability, the CU*Answers Incident Response Team becomes involved, and individual members are assigned priorities, such as client contact, research, and communication with executive management.



RESEARCH. CU*Answers performs research on the scope of the issue. The primary focus is to determine whether the issue is global, and therefore warrants removing a system from all client access until the problems can be resolved.



REVIEW. CU*Answers executive management is provided evidence, or lack thereof, of the scope of the security threat. CU*Answers management has decision-making authority on whether to remove a system from service.



NOTICE. Crisis communications are set up, when warranted. Depending on the scope of the issue, this may include a notice to all clients, or communications with just the affected credit unions.



ETA. When warranted, communications are sent to clients including uptime and downtime estimates for service interruptions.



PATCH. If patches are required, these follow the same SDLC quality control testing process as other patches in the environment.

2.8.1 SERVICE OUTAGE

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

2.8.2 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.

2.8.3 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.

2.8.4 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.

2.8.5 FORM GUIDANCE

SERVICE OUTAGE	SECURITY INCIDENT	VULNERABILITY
CEO Incident Form Discretionary	Security Incident Form Mandatory	Security Incident Form Mandatory

2.9 ROLES: INCIDENT RESPONSE TEAM (IRT)

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 to submit a Security Incident Report form; all employees are encouraged to use this form if they merely suspect an incident has occurred.

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

2.9.1 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, Network Services, and the Writing Team. Appropriate Alert messages should be posted, as necessary, to communicate the situation to 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.

2.9.2 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.

2.9.3 ROLES: CORPORATE OFFICERS

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

2.9.4 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.

2.10 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.

2.10.1 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.

2.10.2 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.

2.10.3 EVALUATE THE BUSINESS DECISION

“What is the risk of one or more members 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 members; 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; or 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.

2.10.4 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.

2.10.5 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.

2.10.6 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.

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.

RELEASE OF LIABILITY [SAMPLE]

[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]

[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.

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 (see following page):

INCIDENT RESPONSE PROTOCOL

REPORT. Upon report of a potential vulnerability, the CU*Answers Incident Response Team becomes involved, and individual members are assigned priorities, such as client contact, research, and communication with executive management.



RESEARCH. CU*Answers performs research on the scope of the issue. The primary focus is to determine whether the issue is global, and therefore warrants removing a system from all client access until the problems can be resolved.



REVIEW. CU*Answers executive management is provided evidence, or lack thereof, of the scope of the security threat. CU*Answers management has decision-making authority on whether to remove a system from service.



NOTICE. Crisis communications are set up, when warranted. Depending on the scope of the issue, this may include a notice to all clients, or communications with just the affected credit unions.



ETA. When warranted, communications are sent to clients including uptime and downtime estimates for service interruptions.



PATCH. If patches are required, these follow the same SDLC quality control testing process as other patches in the environment.

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**

03

3.1 POLICY PURPOSE AND OVERVIEW

CU*Answers relies on its computer network to conduct its business. To ensure 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 the Users 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 User's duty to use CU*Answers' technology responsibly, professionally, ethically, and lawfully. Users must observe and comply with all other policies and guidelines of the company when using technology.

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 supervisor.

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. 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 software and hardware 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 before use is allowed. The requestor must complete the form in detail and follow submission instructions. 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 is 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.

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 Executive 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 up to and including termination.

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, do 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 the 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. 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 signed authorization from their manager or supervisor through usage of the proper form

3.9.3 PHYSICAL ATTENDANCE REQUIRED

Participating Users must observe the actions of the third party, and Users must not leave the PC unattended at any time.

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 on the Internet should not 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.

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.

3.12.1 APPROVAL REQUIRED

Mobile or remote access to any CU*Answers Computer Resource requires approval by the departmental supervisor and the Executive Team. CU*Answers reserves the right to deny remote access at any time if the device does not meet minimum secure access requirements. An employee who has not completed the 90-day probationary period is not allowed remote access to CU*Answers Computer Resources unless an exception is made by a corporate officer.

3.12.2 MINIMUM SECURITY STANDARDS

Any device used to connect remotely to CU*Answers Computer Resources must be secured by a password (or PIN if approved by Internal Networks). Remote access requires the device to maintain a secure, encrypted connection between CU*Answers

Computer Resources and the local machine. Only approved mobile device management software may be installed on the user's PC for the purpose of updating the device with operating system updates and/or syncing of corporate data. Network Services may change standards at any time.

3.12.3 NO LOCAL SAVE OF SENSITIVE INFORMATION

Employees are expressly forbidden to save sensitive information to any local machine that has mobile or remote access to CU*Answers Computer Resources.

3.12.4 CONSENT TO REMOTE WIPE

All Users must consent to have their mobile access device, whether personal or CU*Answers issued, remotely wiped in the case of termination of employment, loss of the device, or suspicion of a security breach. CU*Answers is not responsible for any loss of personal information which may be stored on the device.

3.12.5 LOST OR STOLEN DEVICE

If the local machine used to connect remotely to CU*Answers is lost or stolen, employees are required to immediately notify a security officer or a supervisor.

3.12.6 VPN

The use of VPN to connect to CU*Answers Computer Resources is strictly prohibited except for approved devices. Users are never allowed to connect using VPN on machines that are accessible to the general public. CU*Answers has the right to terminate any VPN connection at any time if the security of the connection is in question. VPN connections to CU*Answers Computer Resources are strictly limited for business purposes only. No VPN connection may be maintained for longer than five minutes unattended without security measures such as screen-locking employed. Users may never allow any unauthorized individual to access CU*Answers Computer Resources through a VPN connection.

3.12.7 ALWAYS ON VPN

Special business cases allow an employee to have "always-on" 24/7/365 VPN access from the employee's home office. The employee's PC will not have dual factor VPN client authentication, but rather will have connectivity as if the employee's machine is connected to the CU*Answers internal office network. Because of the cybersecurity risk and the fact that alternative methods of remote access through the VPN Client exists, these requests will be denied in the absence of an exceptional Business Case.

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.

AUDIT POLICY

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

04

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 risk assessments and assurance of controls to management.

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:

1. Significant legislative or regulatory issues impacting the organization are recognized and addressed appropriately;
2. Significant financial, managerial, and operating information is accurate, reliable, and timely;
3. Existing policies and procedures are appropriate and updated;
4. Operations, processes and initiatives are consistent with established missions, objectives and goals and are being executed as planned;
5. Risks within and outside the organization are appropriately identified and managed;
6. Contractors meet the contract objectives, while in conformance with applicable laws, regulations, policies, procedures and best practices;
7. Operations, processes or initiatives are reviewed at the request of executive management; and
8. If improvements to member service, management of risks, internal controls, governance, profitability, and the organization's effectiveness, efficiency and image are identified during audits, such 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:

1. Establish procedures for conducting activities according to the organization's policies and direction provided by executive management, and by professional standards;
2. 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;
3. Conduct an annual risk assessment and produce an audit plan that will accomplish the mission, objectives and scope of this policy;
4. Implement the annual audit plan, as approved, including, as appropriate, any plan amendments, special tasks or projects requested by executive management;
5. Coordinate with audit clients to finalize recommendations for improvement and identify implementation timelines;
6. Evaluate and assess significant new or changing services, processes, operations, and control processes coincident with their development, implementation, and/or expansion;
7. Conduct periodic follow-up reviews to evaluate the adequacy of management's remediation;
8. Issue periodic reports to executive management summarizing results of audit activities and the status of follow-up activities;
9. Provide periodic summaries of consulting and advisory activities to management;
10. Assist in the investigation of significant suspected fraudulent activities within the organization and notify management, as appropriate, of the results;
11. 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;
12. Consult with the organization's management, as requested, on potential policy and procedure changes;

13. Participate in professional audit organizations by attending meetings, joining the governing boards, presenting speeches and papers, and networking with other professionals; and
14. Act as the primary point of contact for handling all matters 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/specialists access to relevant records and information when appropriate. All employees of the organization are required to assist the staff of the Internal Audit department in fulfilling their audit functions and fiduciary duties.

EXAMINATION PROTOCOL

This document establishes 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 business hours to respond to and provide large data and information files to on-site external auditors.

An Internal Audit team member and any 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.

PHYSICAL SECURITY POLICY

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

Policy Owner: Facilities Management

05

5.1 SIGN IN REQUIRED FOR BUILDING 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 always be escorted 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), the front desk/reception areas of each 44th street facility, and the Innovation Center in Las Vegas.

5.3 BADGE COLORS AND ACCESS

Badges must always be visible. 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.

RED BADGE Visitors Visitors must sign in and be escorted in all facilities at all times in secure areas	YELLOW BADGE Approved Guests Must sign in, but do not require an escort through the facilities	BLUE BADGE Long Term Contractors Do not need to sign in or be escorted	GREEN BADGE Employees Do not need to sign in or be escorted
---	--	--	---

5.4 VISTORS 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.

5.5 KEY FOBS

5.5.1 CONTROLS

Combinations and external key fob controls are the responsibility of the Facilities 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 key fob must be reported immediately to Facilities, ORD, or the Internal Audit Team.

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, during 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 key fob. 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 key fob.

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.

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 the 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 Facilities Team is responsible for the alarm verification. The 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 follow all current End of Day protocols, including ensuring no other employees remain in secure areas and ensuring coffee pots are turned off.

5.8 RETURN OF VENDOR/CONTRACTOR 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 key fobs at the end of the visit or at the end of each day. Under no circumstances may any visitor take key fobs off the premises.

5.9 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.

5.10 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.

5.10.1 LOSS OF KEYS

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

5.10.2 DISTRIBUTION

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

5.10.3 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 Facilities. 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 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.

5.11.1 KENTWOOD 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.

5.11.2 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, iSeries 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.

5.11.3 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, iSeries 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.

5.11.4 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.

5.12 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.

5.13 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 always be closed to ensure the rooms are airtight. 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.

5.14 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 calculated to ensure the appropriate concentration level.

CLIENT SUPPORT POLICY

*Because CU*Answers has responsibility 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 CU*BASE Support staff. Any time an employee leaves CU*Answers' employment, the security for Employee ID 89 will be changed immediately. The password for 89 is also changed for self-processors and certified distributors every 30 days.

Each credit union client 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 one or more 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 union’s 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.

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**

07

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 of a large-scale absence event is the responsibility of Corporate Officers.

7.2 CLIENT SERVICES

Delays in servicing our clients should be expected. CU*Answers will communicate delays to clients appropriately by sending out a scripted message using our Alert procedures.

7.3 COVERAGE OF ALL SHIFTS

Management will ensure all necessary shifts are covered across all areas of the company. Employees and managers who have the capability to work from home may be encouraged to do so, if the situation allows.

7.4 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 to complete important tasks. Management shall make decisions on readjusting the priority list and delay of non-critical project travel.

7.5.1 PROGRAMMING

Projects will be prioritized by management; inevitably some projects will be delayed or put on hold for a short period of time. CU*Answers 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., delay CU*BASE releases and demos if necessary.)

7.5.3 CU*BASE ISSUE DOCUMENTATION

Updated documentation will be used to ensure a greater number of employees can be responsible for any CU*BASE issues.

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 will decide whether more employees will be sent to supplement for any unavailable employees. For services delivered from CU*Answers' offices, cross-training and up to date documentation will be developed as needed to provide quality service.

7.6.2 HANDLING TIME ESSENTIAL DUTIES

Essential duties will be assigned 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:

1. Until additional staff can arrive on site, web and phone conferences will be utilized for training, support, and sign-off.
2. Depending on the location of the credit union, the Executive Council may assign other CU*Answers employees as support staff.
3. 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

Management shall 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 shall cross-train team members on an ongoing basis to ensure delivery of time-sensitive items.

7.7.2 CROSS-DEPARTMENTAL COVERAGE OPTIONS

Employees from other teams will 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 Corporate Officers 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, CU*Answers shall develop protocols for cleaning workstations, social distancing, and remote work options.

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:

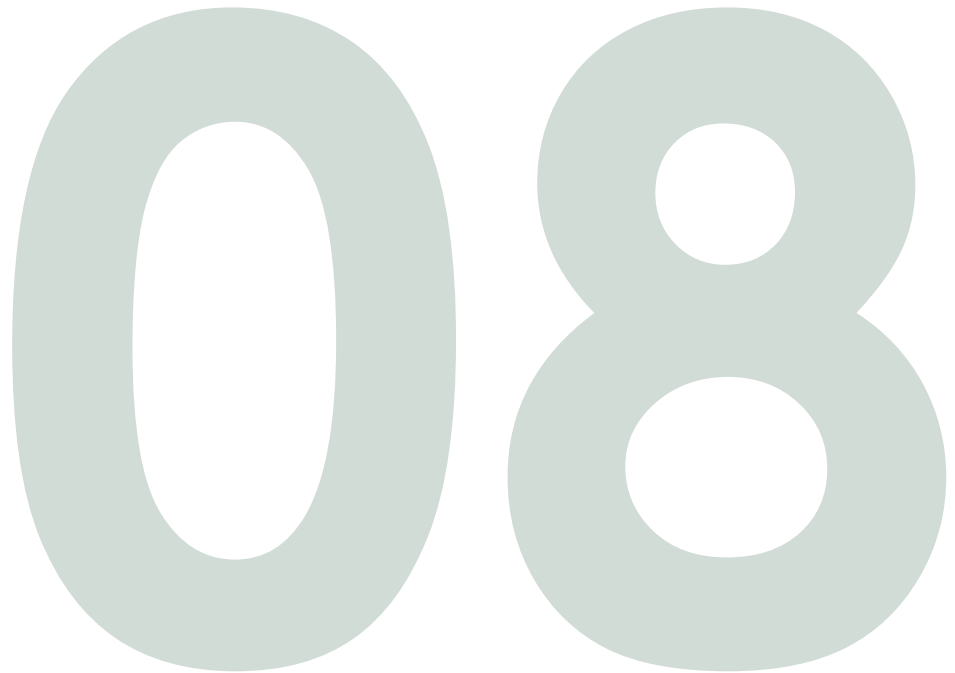
1. Severely discouraging or disallowing large assemblies of employees (on or off work premises).
2. Closing all meeting rooms; limiting all staff interactions as much as possible; encouraging or requiring employees to work at home or at other CU*Answers offices.
3. Offering masks and setting up for cleaning stations around the office.

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.

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.

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

Records that serve administrative, legal, or fiscal purpose for which they were created should be retained.

8.2.3 ESTABLISH SAFEGUARDS

Establish safeguards against the illegal removal, loss, or destruction of records. Records should be disposed of in accordance with an approved records retention schedule.

8.2.4 DEPARTMENT RESPONSIBILITY

Management of records is the responsibility of the owner or creator of the record. CU*Answers will ensure each department shall assist in the implementation of the RIM program. Departments shall be provided guidance on how records should be organized and stored to ensure timely and efficient retrieval. Departments shall assist in managing their department's records and assisting in the implementation of any litigation hold(s) enacted by CU*Answers.

8.3 RECORDS RETENTION SCHEDULE

The records retention schedule is the key tool for departments to use to manage their records effectively. Records retention schedules shall identify records to be preserved, the length of retention, and the location of the records.

8.4 COMPLIANCE AND AUDITING

8.4.1 ANNUAL REVIEW

CU*Answers shall annually inventory and review the records retention schedule for accuracy and purge documents no longer required.

8.4.2 ANNUAL RECORDS DESTRUCTION PROGRAM

CU*Answers shall record all instances of electronic or physical destruction of records as part of the audit report.

LITIGATION HOLD

If a litigation hold is enacted, the Internal Audit Team has oversight responsibility. 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*Answers 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, 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 communication to all employees. Key employees must confirm their understanding of the litigation hold and to request that they gather the physical 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 physical and electronic records subject to the litigation hold. A personal meeting with each key employee to confirm that all physical and electronic records have been identified and collected should be conducted and documented. All key employees should sign a document verifying that to the best of their knowledge they have identified and turned over all physical 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.

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: Facilities Team

09

9.1 DEFINITIONS

9.1.1 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.

9.1.2 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.

9.1.3 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.

9.1.4 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.

9.2 SCOPE

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

9.3 ELIGIBLE DRIVERS

Every employee who 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.

9.4 DRIVING RECORD CRITERIA

9.4.1 GOOD DRIVING RECORDS

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 are not limited to, three or more moving violations in a year.

9.4.2 VIOLATIONS

Violations include:

1. Any ticket, citation, or other law enforcement determination relating to these;
2. 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)
3. Any combination of accidents and/or moving violations; or
4. Any driving violation or infraction that results in the employee being ineligible for insurance coverage under the policy or policies applicable to Company Vehicles.

9.5 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.

9.6 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:

1. 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.
2. 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.
3. All drivers and passengers operating or riding in a Company Vehicle or rental vehicle must wear seatbelts, even if air bags are available.
4. 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.
5. All laws must be obeyed.

9.7 MAINTENANCE AND ADMINISTRATION

Keys to the pool of available Company Vehicles are kept in the office of the Facilities Manager. 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 are 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.

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.

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

10.1 VENDOR MANAGEMENT PROGRAM

The Vendor Management program mitigates and manages risk. Risks may include:

1. Reputational risk through the misuse of sensitive or confidential data;
2. Transaction risks such as fraudulent activity;
3. Strategic Risk relative to the dependency of service provided; and
4. Compliance risk primarily including the privacy and safeguard regulations of GLBA – Financial, Concentration, and Operational.

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 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:

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

10.3.2 TIER II

Public companies that provide a service technical in nature that may house sensitive 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 sensitive 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 are 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 access sensitive 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 track some or all of the following:

1. Annual or audited financial statements (or quarterly financials if it is an owned CUSO).
2. Publicly available controls audit.
3. Insurance/bond.
4. Internal network infrastructure audit or penetration test.
5. Disaster recovery/business resumption policies and annual testing.

The following items may optionally be reviewed during the due diligence process:

1. Review of financial statements, preferably audited statements.
2. Review of insurance coverage.
3. Contacting references and user groups.
4. Determination if service provider performs background/reference checks on its new employees.
5. Determination if third parties/contract employees would support the service provider in fulfilling its requirements.
6. Conclude if the service provider uses third parties/contract employees. If so, what type of due diligence they perform on those third parties.
7. Perform an onsite visit, if applicable.
8. Review SSAE report, if applicable.
9. Determine service provider's knowledge of GLBA, Regulation E, Privacy Act, Consumer Protection and Bank Secrecy Act.
10. Determine how long the vendor has been in business.
11. Conclude on the vendor's experience and ability to provide service in question.
12. Review disaster recovery/business resumption plan of vendor.
13. Determine security precautions implemented, such as firewalls, encryption, authentication, etc.
14. 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, these 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 no less than 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. Staff or management must fill out the appropriate form for any capital expenditure requests above \$10,000.00 (Project Due Diligence Form). The form will then be peer reviewed as well as being reviewed by Internal Audit, if applicable, who will complete a risk assessment and attach that to the form. The form must be filled out completely and submitted for Corporate Officer approval (CEO or CFO).

If approved, the VP of Administration 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 upon request. The VP of Administration tracks the open and closed statuses of the capitalized projects.