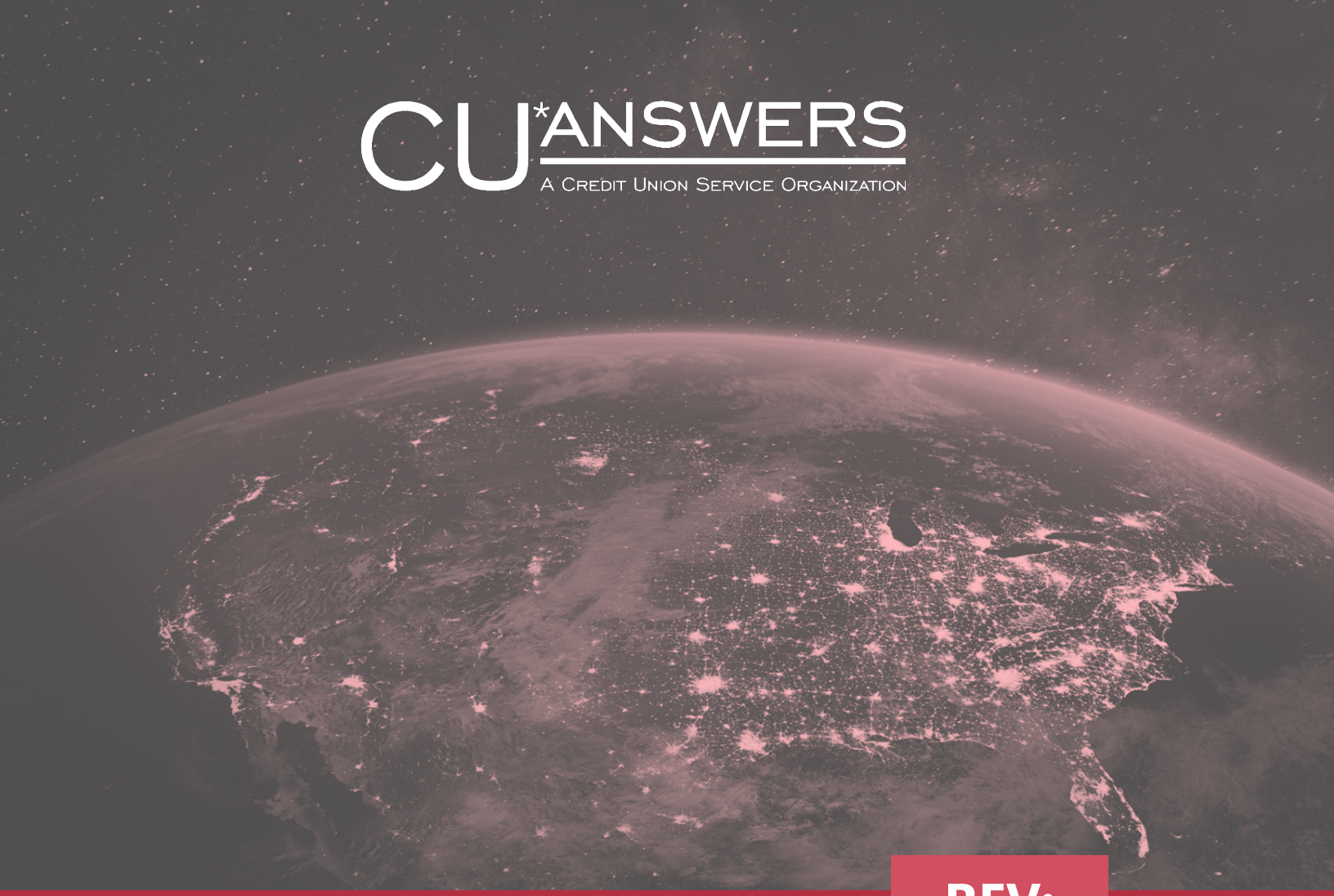
CU*ANSWERS

A Credit Union Service Organization



REV: 10/24

CU*ANSWERS

POLICY MANUAL

Contents

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 substantive 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 Human Resources 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

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. See **Appendix A** of this Policy for a sample of security best practices.

1.2 Sensitive Information Classifications

See **Appendix B** of this Policy for additional details.

1.2.1 Non-Public Personally Identifiable Financial Information (PIFI)

PIFI 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 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 Publicly Available Information

CU*Answers has no obligation to protect information which:

- Was publicly available or in the public domain at the time of disclosure.
- Becomes publicly available or in the public domain through no fault of CU*Answers.
- Is in CU*Answers possession free of any obligation of confidence to the disclosing party at the time of disclosure.
- 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 a 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 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 Multi-Factor Authentication

CU*Answers employees are required to use Multi-Factor Authentication (MFA) when accessing network resources, connecting with remote sessions, or using teleconference software.

1.6.10 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.

Appendix A: Top Ten 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 Physical Documents. 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 request and approval 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 or Your System 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 employee's 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.

Appendix B: Federal Privacy Laws and Risk Summary

GLBA (Reg P)

(1) Personally identifiable financial information means any information:

(i) A consumer provides to you to obtain a financial product or service from you;

(ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or

(iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.

(2) Examples -

(i) **Information included**. Personally identifiable financial information includes:

(A) Information a consumer provides to you on an application to obtain a loan, a credit card, a credit union membership, or other financial product or service;

(B) Account balance information, payment history, overdraft history, and credit or debit card purchase information;

(C) The fact that an individual is or has been one of your customers or has obtained a financial product or service from you;

(D) Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;

(E) Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a loan or a credit account;

(F) Any information you collect through an internet "cookie" (an information collecting device from a Web server); and

(G) Information from a consumer report.

(ii) **Information not included**. Personally identifiable financial information does not include:

(A) A list of names and addresses of customers of an entity that is not a financial institution; and

(B) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

Examples (Red indicates the highest level of risk)

Consumer name plus home address.

Consumer name plus social security numbers.

Consumer name plus account numbers.

Consumer name plus credit and debit card numbers.

Consumer name plus phone numbers.

Consumer name plus income.

Consumer name plus credit score.

Consumer name plus household identifier (especially internet cookies).

Consumer name plus application to obtain a loan, a credit card, a credit union membership, or other financial product or service.

Consumer name plus account balance information, payment history, overdraft history, and credit or debit card purchase information.

Consumer name plus the fact that an individual is or has been one of your customers or has obtained a financial product or service from you.

Consumer name plus any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer.

Consumer name plus any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a loan or a credit account.

Consumer name plus information from a consumer report.

Personally identifiable financial information does not include information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

Biometric Information

Biometric information means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.

Consumer information plus a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.

Consumer name plus a photograph, if the image data to create an individual digital template or profile, which in turn you use for automated image matching and identification.

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

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:

- Ensure the security and confidentiality of member information.
- Protect against any anticipated threats or hazards to the security or integrity of such information.
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any member.
- 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 Sensitive Data Classification

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. Details on the type of data considered sensitive can be found in Appendix A and B of the Cybersecurity Policy.

2.3 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.

2.4 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.

2.5 Incident Response Plan

CU*Answers response to Incidents shall be defined in the Incident Response Plan described in **Appendix A** of this policy and the Disaster Recovery Business Resumption Plan.

2.6 Incident Notification

All CU*Answers employees and contractors who are aware of an Incident, as defined below, should contact a member of the Incident Response Team. Then the employee should notify the organization through the use of the CEO Incident or the Security Incident form.

2.6.1 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.

2.6.2 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.

2.6.3 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.

2.6.4 Form Use

The **CEO Incident Form** is discretionary at the election of the employee for **Service Outage Incidents**. The Security Incident Form is mandatory in the event the employee has knowledge of a Security breach Incident or a System or Application Vulnerability Incident.

2.7 Security Program Implementation and Oversight

The Board of Directors of CU*Answers has responsibility to oversee the Information Security Program and its implementation. As part of its responsibilities, the Board shall:

- Designated the Internal Audit team to oversee and implement its Security Program.
- Identify and assess the risks to covered data in each relevant area of CU*Answers operations and evaluate the effectiveness of the current safeguards for controlling these risks.
- Design and implement a safeguards program, and regularly monitor and test it.
- Implement policies and procedures to ensure that personnel are able to implement the Security Program.
- Select service providers that can maintain appropriate safeguards over covered data, ensure the service contract requires them to maintain safeguards, and oversee their handling of covered data.
- Evaluate and adjust the information security program in light of relevant circumstances, including changes in business or operations, or the results of security testing and monitoring.
- Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of covered data in the organization's control.
- Require the Internal Audit Team to report in writing, regularly and at least annually, to the Board of Directors on the status of the Security Program.

For purposes of the Security Plan, covered data is limited to information as described in **Appendix A and B** of the **Cybersecurity Policy**.

2.8 Plan Changes

The Security Program is evaluated periodically to make appropriate adjustments based upon regulatory changes or changes to operations or business. When adjustments are made, appropriate notices are sent to staff. Questions regarding interpretation and implementation regulations are coordinated with the CU*Answers General Counsel.

2.9 Safeguards

CU*Answers teams work together to identify and assess risks to:

- Covered data including detection, prevention and response to attacks, intrusions and other system failures.

- Information systems, including network and software design, as well information processing, storage, transmission and disposal.

- Employee training and education, and in each case, put safeguards in place to address those risks and regularly test those safeguards to make sure they are effective.

2.10 Policies and Training

Where appropriate, procedures may be adopted as long as they are consistent with CU*Answers policy. Teams are responsible for facilitating and enforcing compliance with all information security policies and practices applicable to their team.

Training is made available to all employees. New employees must complete training to gain access to sensitive information.

2.11 Oversight of Service Providers and Contracts

CU*Answers shall take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. Vendors who will have access to covered data shall be reviewed in accordance with CU*Answers Vendor Management Policies.

2.12 Annual Reporting

Internal Audit shall submit written reports to the Board of Directors at least annually on the status of the Security Plan.

Appendix A: Incident Response Plan

Note: Full details are available in the Disaster Recovery Business Resumption Plan.

Roles and Responsibilities. Individual roles and responsibilities follow the same structure as the Business Continuity Plan (Roles and Responsibilities) with added emphasis on the security of IT assets (including systems, infrastructure, and information/data). Actions taken during each stage of the response must consider the impact on business operations overall. Scenarios involving the security risk to IT assets must be documented thoroughly in the event of potential legal ramifications.

The CU*Answers Incident Response Team is comprised of the following positions:

- Corporate Officers.
- Executive VPs.
- Technology Managers related to any incident.
- Internal Auditing.

The responsibilities of the IRT include:

- Quickly identify threats to the organization's information assets.
- Assess the level of risk and take immediate steps to mitigate impact and loss.
- Notify appropriate authorities and mobilize response and recovery teams.
- Respond and recover to bring operations back to normal.
- Document the response process and report findings along with lessons learned.

Incident Manager Responsibilities include:

- Oversee the global efforts of all resumption teams and ensure that recovery goals and timelines are met.
- Establish command/control center for management of incident from top level.
- Serve as liaison to the Board of Directors to get approval for the acquisition of major purchases and for strategic direction.
- Resolve issues of priority based on evolving circumstances.
- Oversee initial damage assessment and approve major equipment purchases.

- Ensure adequate cash flow for expenses during recovery as needed.

Public Relations responsibilities include:

- Serve as communications point of contact for the entire organization with external media relations (TV, print, web, etc.), public affairs, etc.

- Crisis communications message content creation and distribution to appropriate stakeholders.

- Serve as a conduit for all internal communications to and from executive and technical teams, alert staff, clients, major vendors, etc.

- Organize internal and external meetings/briefings on recovery status.

- Determine message(s) communicated to external media.

Security Officer responsibilities include:

- Go through facility and assess for damage/losses and take pictures.

- Act as liaison with insurance agency to document, file and settle claims.

- Coordinate with vendors and oversee restoration to any of the facilities.

Technology Recovery responsibilities include:

- Coordinate IT recovery effort with affected vendor(s).

- Coordinate the repair, replacement, installation, and configuration of all internal network user hardware (workstations, printers, etc.) as needed.

- Purchase, receive, store, distribute all software, equipment, and supplies, etc.

Legal Counsel/Internal Auditor responsibilities include:

- Determine recovery status of vital records.

- Ensure the safety and security of corporate and employee assets including employee and customer information during recovery.

- Review procedures used in recovery efforts to ensure security/compliance policies are followed.

- Ensure application/service security and availability, inform and update Executive Team on recovery status.

- Notify external auditors, if necessary.

Technology Recovery responsibilities include:

- Explore any work arounds to meet SLA.

- Ensure teams work with insurance provided forensics teams.

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 approved by the corporate officers or EVP of Technology or VP of Network Infrastructure before the action is taken. If none of these are available, any team member may remove the affected system or application from production. Immediately following such action, notification should be made to Client Services, Systems, and the Writing Team. Appropriate Alert messages should be posted, as necessary, to communicate the situation with clients.

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

Chain of Custody. A proper chain of custody for the evidence should be maintained. A chain of custody is a history that shows how the evidence was collected, analyzed, transported, and preserved. Evidence should be protected from unauthorized access and from modification or damage. Transfers or copies should be approved and witnessed. The IRT will take note of actions and results.

- Logging events clearly in chronological order with a time stamp for each event.

- Use a consistent format.

- Include facts, not speculation or unsure interpretations.

- Correct mistakes when found and record the cause of mistakes.

Third-Party Support During an Incident Response. Effectively responding to security incidents may require skills and expertise not readily available from the CU*Answers staff. In such cases, the Executive Council may determine that engaging outsourced support is necessary. Examples include data breach experts and legal counsel. All such activities must be documented and filed with the official incident report.

Forensic Evidence. Affected machines should be removed from the network and physically isolated for forensic examination.

- Determine if any countermeasures, such as encryption, were enabled when the compromise occurred.

- Analyze backup, preserved, or reconstructed data sources.

- If applicable, ascertain the number of members affected and type of information compromised.

Chain of custody as outlined above will be followed. The organization will preserve the machines offline and untouched if instructed by law enforcement. All actions will be logged/recorded.

Communications. Communicating in a crisis is a critical component of an effective incident response, both internally among teams and externally to key partners, vendors, customers, as well as law enforcement and regulatory agencies when necessary. Characteristics include the proper content, frequency, and methods used for informing each group of stakeholders.

The Crisis Communications section of the Business Continuity Plan provides additional details including notification and posting of alerts.

Forms have been created for specific types of incidents, including:

- CEO Incident Report. To report service outages for internal or external (vendor) products and services provided to our client base.

- Security Incident Report. To report incidents of a security nature, whether attempted/successful attacks, system/software vulnerability, violation of security policy, etc.

Scenarios. Networks and systems today have become highly integrated with multiple external vendors and service providers and are accessed in more ways, due in part to the expansion in the type and volume of digital services, available 24/7 to a global market. Planning and preparing for every scenario is an exhausting effort.

With early detection and accurate initial assessment, the appropriate response level can be applied (high, medium, low) depending on the scope and duration of the impact, availability of a workaround process, and sensitivity of data or system at risk. Key decisions that must be made include whether to take systems or networks offline during the response effort.

For the purpose of this plan, process, and procedures for types of incidents are grouped into categories based on the nature of the attack and response effort required.

General Incident Response scenarios:

- Malware or Ransomware Outbreak (virus suspected or confirmed, or other malicious code).

- Denial of Service attack (DoS).

- Lost or Stolen Devices.

- Business Email Compromise.

- Insider Threat.

Not all incidents require equal priority. Denial of service attacks, while inconvenient, do not represent the same level of seriousness as does a disclosure of confidential information to unauthorized parties. The Incident Response Team will assign priority based on the actual circumstances and will adjust activities accordingly. If the incident in question specifically deals with the breach of sensitive data, that will take preference.

The threat landscape is constantly changing. Maintaining a strong security posture involves regularly assessing risk, implementing mitigating controls, conducting regular training exercises and penetration tests, maintaining secure networks and devices through hardening and system patching, as well as responding to vulnerabilities in a timely manner.

Vulnerability Management. Vulnerability management is one of many orchestrated steps taken to minimize the risk of an attacker (external or internal) exploiting a vulnerability. Vulnerabilities can be detected in a number of ways, including:

- Announced by professional security organizations.
- Announced by software/hardware vendors.
- Result of regular vulnerability scans (internal and external).
- Result of an actual cyberattack (attempted or successful).

Typically, when announced, vendors will provide either countermeasures for mitigating the risk and/or a software update to apply to correct the vulnerability.

When vulnerabilities are announced or detected, it's important to determine if it's already been exploited (attempted or successful), and the criticality and impact to users on the network to apply the resolution. Is it critical enough to take offline during business hours or is the risk low enough that an after-hours resolution can be scheduled?

Incident Handling Guidelines. Incidents that threaten the security, confidentiality, and availability of IT assets can come from a number of sources from internal threats to cyber-attacks over Internet connections or through trusted vendor networks. Below are general incident handling guidelines with some specific actions for different scenario types.

Early detection and containment are key to an effective incident response. It's important that staff and teams are mindful of potential threats that could be the early signs of an attack. Cybersecurity awareness training is provided to all staff to aid in detection and reporting when social engineering attempts are spotted. Other forms of detection can come from controls in place such as Intrusion Detection Systems (IDS), Endpoint Detection and Response (EDR), Security Information and Event Management (SIEM), or an external source such as vendor or even law enforcement.

When an incident is detected or reported, it's important to:

- Determine if it is an actual incident or false positive.
- Determine the stage of the attack if possible (active, inactive, or attempt) and risk level.
- Engage the Incident Response Team (IRT) and inform the Executive Council (EC).
- Submit a Security Incident Report.
- Engage external parties as determined by the EC (legal counsel, cyber insurance provider, data breach experts, law enforcement, etc.).
- Determine appropriate forms of notification to all affected parties (board, staff, partners, vendors, clients, regulatory agencies, etc.) See **Crisis Communications** section.
- Document all steps taken throughout the incident response.
- Perform a preliminary analysis of the facts and assessment of the situation to determine the nature and scope of the incident (number of systems compromised, data at risk, etc.).
- Identify the types of information/data at risk (sensitive, PII, etc.).
- Identify the impact to other users on the network (internal/external) during remediation stages.
- Identify user/system accounts involved (change all passwords and/or deactivate accounts).
- Identify services/protocols used in the attack (consider blocking or restricting).
- Include means of ingress, egress, and all lateral movements by the intruder.
- Determine if data was exposed and/or exfiltrated. Monitor systems and network for signs of continued intruder access.
- Take necessary steps to quarantine/isolate the affected systems while preserving the evidence (i.e., log files).
- Follow procedures to eradicate and recover affected systems to a pre-incident configuration.
- Determine if any controls and safeguards need to be added or enhanced.
- Determine if any policies, procedures, or plans need to be updated.

Appendix B: 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 a Credit Union Wants a Service Turned Back On. If your credit union chooses to accept the risk and wishes to have a service restored, the credit union can follow these steps:

- Complete the Release of Liability Form.
- Have a credit union officer approve and sign the form.
- 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.

Acceptable Use Policy

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

Policy Owner: Human Resources

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

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 Users 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 authorization 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 Observation Required

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

3.9.2 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.

3.11 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.

3.12 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 Requirements

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 Users 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 Access

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

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:

- Significant legislative or regulatory issues impacting the organization are recognized and addressed appropriately.
- Significant financial, managerial, and operating information is accurate, reliable, and timely.
- Existing policies and procedures are appropriate and updated.
- Operations, processes and initiatives are consistent with established missions, objectives and goals and are being executed as planned.
- Risks within and outside the organization are appropriately identified and managed.
- Contractors meet the contract objectives, while in conformance with applicable laws, regulations, policies, procedures and best practices.
- Operations, processes or initiatives are reviewed at the request of executive management.
- 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:

- Establish procedures for conducting activities according to the organization's policies and direction provided by executive management, and by professional standards.

- Select, train, develop and retain a competent internal audit staff that collectively has the abilities, knowledge, skills, experience, expertise and professional certifications necessary to accomplish the purpose, objectives and scope of this policy.

- Conduct an annual risk assessment and produce an audit plan that will accomplish the mission, objectives and scope of this policy.

- Implement the annual audit plan, as approved, including, as appropriate, any plan amendments, special tasks or projects requested by executive management.

- Coordinate with audit clients to finalize recommendations for improvement and identify implementation timelines.

- Evaluate and assess significant new or changing services, processes, operations, and control processes coincident with their development, implementation, and/or expansion.

- Conduct periodic follow-up reviews to evaluate the adequacy of management's remediation.

- Issue periodic reports to executive management summarizing results of audit activities and the status of follow-up activities.

- Provide periodic summaries of consulting and advisory activities to management.

- Assist in the investigation of significant suspected fraudulent activities within the organization and notify management, as appropriate, of the results.

- Consider the scope of work of the external auditors and regulators, as appropriate, for the purpose of providing optimal audit coverage to the organization at a reasonable overall cost.

- Consult with the organization's management, as requested, on potential policy and procedure changes.

- Participate in professional audit organizations by attending meetings, joining the governing boards, presenting speeches and papers, and networking with other professionals.

- 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

Internal Audit shall administratively report to the Executive Management team. The Internal Audit team shall report to the Board of Directors audit report findings. Any reports written by the Internal Audit team shall be provided to Executive Management and shall be forwarded unedited to the Board of Directors for acceptance or direction on modifying policies and procedures. There shall be no fewer than six Internal Audit reports each fiscal year.

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.

Appendix A: 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: Human Resources

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 Visitors Without Badges

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

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 Key Fob

A loss of a key fob must be reported immediately to Facilities, Human Resources, or the Internal Audit Team.

5.5.3 Access by Landlord(s) and Security Contractor(s)

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 Key Fobs

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 Human Resources 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 Operation/Data Centers

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 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.

5.11.3 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 with 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: Human Resources

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 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.

7.5.1 Managing Project Timelines

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

7.5.2 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:

- Until additional staff can arrive on site, web and phone conferences will be utilized for training, support, and sign-off.

- Depending on the location of the credit union, the Executive Council may assign other CU*Answers employees as support staff.

- 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 Human Resources. 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 Human Resources. Depending on the circumstances surrounding the event, decisions will be made regarding:

- Severely discouraging or disallowing large assemblies of employees (on or off work premises).

- Closing all meeting rooms; limiting all staff interactions as much as possible; encouraging or requiring employees to work at home or at other CU*Answers offices.

- 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: Executive Management

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.

Appendix A: 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 driver's 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

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:

- Prior to employment on all candidates for Driving-Related Positions.
- 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 Human Resources 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 Records 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:

- Any ticket, citation, or other law enforcement determination relating to these.
- Three or more chargeable accidents within a year where chargeable means the driver is determined to be the primary cause of the accident through speeding, inattention, etc. (factors such as weather or mechanical problems will be taken into consideration).
- Any combination of accidents and/or moving violations.
- Any driving violation or infraction that results in the employee being ineligible for insurance coverage under the policy or policies applicable to Company Vehicles.

9.5 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:

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

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

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

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

- All laws must be obeyed.

9.7 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: AuditLink

10.1 Vendor Management Program

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

- Reputational risk through the misuse of sensitive or confidential data.
- Transaction risks such as fraudulent activity.
- Strategic Risk relative to the dependency of service provided.
- 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:

- Have access to, transmit, or store a large amount of sensitive data.
- Would have a significant impact on the income and expense statement in the event of its dissolution or contract termination.
- Would be difficult to replace in a reasonable time while seriously disrupting service.

- Have high level access to IT infrastructure behind the firewalls where corporate secrets and sensitive information reside.

- 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 or more important in this case to manage the impact of their failure vs. the management of the vendor relationship. Examples of these type of companies would include DTE Energy or Consumers Energy.

10.3.5 Tier V
Companies that fall into this tier may 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:

- Annual or audited financial statements (or quarterly financials if it is an owned CUSO).

- Publicly available controls audit.

- Insurance/bond.

- Internal network infrastructure audit or penetration test.

- Disaster recovery/business resumption policies and annual testing.

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

- Review of financial statements, preferably audited statements.
- Review of insurance coverage.
- Contacting references and user groups.
- Determination if service provider performs background/reference checks on its new employees.
- Determination if third parties/contract employees would support the service provider in fulfilling its requirements.
- Conclude if the service provider uses third parties/contract employees. If so, what type of due diligence they perform on those third parties.
- Perform an onsite visit, if applicable.
- Review SSAE report, if applicable.
- Determine service provider's knowledge of GLBA, Regulation E, Privacy Act, Consumer Protection and Bank Secrecy Act.
- Determine how long the vendor has been in business.
- Conclude on the vendor's experience and ability to provide service in question.
- Review disaster recovery/business resumption plan of vendor.
- Determine security precautions implemented, such as firewalls, encryption, authentication, etc.
- Compare market share in the given service area to competitors.

10.5 Evaluation Reporting

The assessment and analysis of all vendors will be completed, and then on an annual basis, 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. Security reviews will be conducted if applicable to the capital expenditure. 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.

Contract Review Policy

*This Contract Review Policy applies to any type of contractual agreement that obligates the CU*Answers to provide or receive payments, services, goods, gifts or use of CU*Answers property, facilities or other resources, to or from a vendor or third party. Each contract is subject to this Policy regardless of whether it has been drafted by the CU*Answers or a third party.*

Policy Owner: Executive Management

11.1 Contract Review

CU*Answers will only be bound by written contracts that have been reviewed and approved in accordance with this Policy, and that have been executed by CU*Answers Executive Management who have specific contract signature authority.

11.2 Policy Scope

Contract means any agreement between two or more parties that creates a legally binding obligation or right. A Contract may or may not involve the payment of money. This Policy applies to any document that obligates the CU*Answers, irrespective of the terminology used to describe that document. Any amendment or revision to an existing contractual agreement must also be reviewed and approved.

11.3 Internal Audit Role

The Internal Audit Team has responsibility for reviewing contracts. Internal Audit will concentrate on Areas of review that will be provided to Executive Management as applicable.

11.3.1 Term and Termination

Review of the length of term of the agreement, and what the exit strategy is for both parties to the contract.

11.3.2 Nature of the Offer

Review the services or products on offer, preconditions to provision of those offers, and pricing for these offers.

11.3.3 Service Levels and Warranties

Promises of warranties, if any, and promises of service delivery, response times, and support levels.

11.3.4 Data Security

Access to and location of sensitive data, promises of security, validation of security controls, notification of data security and business continuity incidents, and insurance requirements.

11.3.5 Compliance

Requirement of compliance with all applicable laws, regulations, and regulatory guidance.

11.3.6 Choice of Governing Law

Except as approved by Executive Management, governing law shall be Michigan when the contract is originated through CU*Answers.

11.3.7 Subcontractors and Assignment

Rights of a party to use a subcontractor for its obligations or assign its rights and obligations to another party.

Appendix A: CU*Answers Non-Disclosure Policy and Agreements

CU*Answers is proud to be organized as both a credit union service organization and a cooperative business owned by our clients. We believe the governance structure of our cooperative is significantly more open, democratic, transparent and inclusive than many of our competitors. CU*Answers is owned and democratically controlled by the clients who actually use our products, rather than by third parties whose only stake is their financial investment.

As a technology firm, CU*Answers is often asked to sign Non-Disclosure Agreements ("NDAs") with our partners and vendors. Our leadership recognizes NDAs are extremely common in our industry, and our policy has been to review the terms carefully. CU*Answers then negotiates the terms whenever the terms conflict with our organizational model. Unfortunately, given the sheer volume of NDAs, CU*Answers is now subject to hundreds of pages of terms from our partners and vendors. In addition, many partners and vendors wish CU*Answers to sign NDA agreements at the outset of the relationship. This demand significantly slows down the pace of business as we spend time negotiating acceptable terms given our status as a cooperative. Furthermore, as a cooperative CU*Answers has a responsibility to share certain information among our clients and peers. Therefore, when CU*Answers is asked to sign an NDA we will provide one of four pre-drafted NDA agreements. Our policy recognizes certain information, such as federally protected member and employee information, must always be kept confidential and inviolable. CU*Answers will also never knowingly usurp protected property and trademark rights. However, CU*Answers will always intend to both compete in our market space and continue the work of developing products and enhancements demanded by our consumers, until dictated otherwise by a new business relationship. CU*Answers believes these agreements are fair, mutually beneficial, and less burdensome than most NDAs. We hope you will keep an open mind as you review our templates as we develop a strong business relationship together.

ACH Policy

The purpose of this document is to set forth written policy regarding the management of activities and procedures of automated clearing house (ACH) service operation. This policy addresses the following ACH areas of activity: (1) Receive ACH Transactions from the Federal Reserve; (2) Process files in a timely manner and post transactions to member accounts (3) Send return ACH transactions to the Federal Reserve; and (4) Annually review ACH rule changes and make recommendations for changes to the core system.

*It will be the policy of CU*Answers to comply with all ACH rules, OFAC and FinCEN sanctions, laws of the United States, state laws, and federal regulations and other related requirements. This policy specifically defines this institution's intentions regarding those requirements under ACH Rules, The Green Book, and Uniform Commercial Code Article 4A, which permit alternative handling, based upon individual CU*Answers policies and procedures.*

Policy Owner: Operations

12.1 ACH Risk Assessment

CU*Answers will conduct an assessment of the risks of its ACH activities and implement a risk management program on the basis of the assessment that complies with the requirements of its regulators.

12.2 Annual ACH Audit

CU*Answers will conduct an annual ACH audit of activities listed in the policy overview in accordance with the minimum ACH audit requirements of the current ACH Rules. The scope, outline, and scheduling for the ACH Audit shall comply with CU*Answers formal ACH Audit Policy.

Verification of compliance will be performed through annual audits and may include (1) interviewing key personnel regarding knowledge of required procedures, (2) reviews of timing and content of client contract and disclosure requirements, and where applicable, (3) testing of specific activities to identify possible compliance exceptions.

12.3 Audit Review

Completed audit results will be reported to the Internal Auditor, Executive Management, and reviewed and approved by the Board of Directors. Exceptions will be noted along with recommended action for correction or corrective action already taken or in process.

12.4 ACH Security Requirements

CU*Answers will create a security framework that includes policies, procedures, and processes to secure ACH data and protect the integrity of certain ACH data throughout its lifecycle. The security framework will establish minimum data security obligations to protect ACH data within its processes.

12.5 National Association Registrations

CU*Answers will complete the ACH Contact Registration and other applicable registrations with the National Association as appropriate.

12.6 Contingency Planning and Testing

CU*Answers will maintain a current contingency plan for both received and return files transmitted between the Federal Reserve and CU*Answers operations center. Such plan will be tested at least annually.

12.7 Receipt of ACH Transactions

12.7.1 Record Retention

CU*Answers will retain ACH records, including electronic records, for a minimum of six years and provide upon request from a participating DFI or ACH Operator. All ACH records must be retained in a secure and access limited manner.

12.7.2 Processing Days

CU*Answers will observe the regular Federal Reserve Bank schedule of holidays for processing ACH entries:

ACH credit entries will be made available for withdrawal no later than the Settlement Date (even if "non-processing" day) of the entry. Funds from Same Day ACH credits processed in the first same day processing window must be made available to the Receiver for withdrawal no later than 1:30pm RDFI local time. Funds from the second same day processing window must be made available to the Receiver for withdrawal no later than 5:00pm RDFI local time. Funds from the third same day processing window must be available to the receiver by the end of the completion of the RDFI's processing for that Settlement Date. Funds from all non-Same Day ACH credits (regardless of SEC code) made available to the RDFI by 5:00pm, RDFI local time, on the banking day before Settlement Date must be made available to the Receiver for withdrawal by 9:00am, RDFI local time, on Settlement Date.

ACH debit transactions received having a settlement date of a non-processing day will be posted on the Settlement Date.

12.7.3 Acceptance of ACH Entries

CU*Answers will process all debit and credit ACH transactions as required under NACHA Rules.

12.7.4 Statement Requirements

CU*Answers will comply with the requirements for Minimum Description Standards that all descriptive information concerning each debit or credit posting to an account will be made available as part of the account statement.

12.8 Return of ACH Transactions

CU*Answers will comply with the appropriate requirements for ACH debit and credit return entries for third party processors, including ACH entries returned revoked, unauthorized, or due to erroneous check conversion transaction.

12.9 Secured Electronic Network

CU*Answers will exchange ACH banking information via a direct VPN with a FedLine Advantage router. The information will be encrypted using technology that is, at minimum, the equivalent to commercially reasonable security standards.

12.10 Origin of ACH Transactions

12.10.1 Corporate Origination

Origination agreements will be executed with each corporate Originator that binds them to the ACH rules, OFAC and FinCEN sanctions, laws of the United States, state laws, and federal regulations and other related requirements.

12.10.2 Security Policy

CU*Answers will develop commercially reasonable security procedures for the transmission of ACH transactions and will provide these procedures to each Originator or Third-Party Service Provider/Sender. For all ACH transactions that involve the exchange or transmission via a secure, the information will be encrypted using technology that is, at minimum, the equivalent to commercially reasonable standards.

12.10.3 OFAC Requirements

CU*Answers will scan addenda data associated with IAT ACH transactions prior to posting the ACH to a member account. In the event a potential hit against the OFAC lists are detected the ACH item will be excepted out, reviewed by the credit union, and then manually posted by credit union staff.

12.11 Agreements

CU*Answers will ensure contracts with clients for which ACH transactions are processed contain all requirements associated with NACHA rules.

12.12 Pricing

CU*Answers will incorporate a schedule of fees for processing ACH transactions and will update it annually.

12.13 Determination of Choice of Law

Regarding the "Choice of Law" disclosure, CU*Answers will disclose Michigan as the default choice of law for processing of ACH transactions where such disclosure is required in contracts and other agreements.

12.14 On-Going ACH Education and Training

To maintain compliance with new as well as existing requirements under the various regulatory sources for ACH activities, CU*Answers will implement the following procedures: (1) Assign specific responsibilities for ACH receipt and posting and return functions to designated personnel; (2) Obtain the current ACH Operating Rules and review rule revisions for the current year; (3) Provide for regular training of ACH personnel responsible for processing activities; (4) ACH contact personnel shall maintain a complete reference library of primary regulation sources (i.e., ACH Rules, Federal Regulation E, and FRB Article 5 and 8).

12.15 FRB Access and Roles

CU*Answers Operators are responsible receiving and posting transactions to member accounts. They are also responsible for sending returns on behalf of clients. At this time, it is not feasible to separate those duties as in many cases only one or two operators are on duty at a time. The VP of Business Continuity and Data Center Operations and the AVP of Operations are End User Authorization Contacts (EUAC) and do not have the authority to process files. The Operations Assistant Manager is also an EUAC and does have the capability to process files.