CYBERSECURITY POLICY

THE CYBERSECURITY POLICY DEFINES THE DUTIES EMPLOYEES AND CONTRACTORS OF CU*ANSWERS MUST FULFILL IN SECURING SENSITIVE INFORMATION. THE CYBERSECURITY POLICY IS PART OF AND INCORPORATED INTO THE INFORMATION SECURITY PROGRAM AND POLICY, AS WELL AS THE ACCEPTABLE USE POLICY.

POLICY 01	VERSION: 3.0
	EFFECTIVE DATE: JANUARY 1, 2016
	BOARD RATIFICATION DATE: NOVEMBER 8, 2016
	POLICY OWNER: NETWORK SERVICES

WARNING

Failure to adhere to policies may result in discipline up to and including termination.

CONTENTS

POLICY PURPOSE AND OVERVIEW 3
CONSUMER PRIVACY 4
MINIMUM REQUIREMENTS FOR DATA SECURITY 5
PASSPHRASES AND PASSWORDS 6
SOCIAL ENGINEERING AVOIDANCE 7
TOP 10 THINGS TO KNOW ABOUT SECURITY AT CU*ANSWERS 8

POLICY PURPOSE AND OVERVIEW

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

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

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.

WARNING

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

SENSITIVE INFORMATION DEFINED

NON-PUBLIC PERSONALLY IDENTIFIABLE INFORMATION (PIFI)

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

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.

CONFIDENTIAL CLIENT AND VENDOR DATA

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

TRADE SECRETS AND CONFIDENTIAL EMPLOYER DATA

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

CONSUMER PRIVACY

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

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.

PRIVATE INFORMATION OF MEMBERS AND NON-MEMBER CUSTOMERS OF CLIENTS

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

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

NON-PUBLIC PERSONAL INFORMATION

Nonpublic Personal Information shall mean personally identifiable financial information, and list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information, and as otherwise more specifically defined in 12 CFR 716.

NO OBLIGATION TO PROTECT PUBLICALLY AVAILABLE INFORMATION

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

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.

MINIMUM REQUIREMENTS FOR DATA SECURITY

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

USE ENCRYPTION

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

ENSURE AUTHORIZATION

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

DO NOT DISCLOSE UNLESS ALLOWED

Users are allowed to disclose sensitive information only when authorized to do so, and refraining from disclosure if there is any doubt regarding the employees' authority to do so.

DO NOT STORE SENSITIVE INFORMATION INSECURELY

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

DATA LEAKAGE

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

NOTIFY WHEN SUSPECTED SECURITY INCIDENT OCCURS

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

DESTROY SENSITIVE INFORMATION

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

WARNING

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

For additional information, see CU*Answers Information Security Program and Policy.

PASSPHRASES AND PASSWORDS

Users are responsible for safeguarding their passphrases and passwords for access to Computer Resources. Individual passphrases and passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passphrases and passwords. No User may access Computer Resources with another User's password or account, except in a support role with accompanying documentation. Users 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 User's passphrase or password.

PASSWORD GUIDELINES

Strong passwords have the following characteristics:

Contain at least 12 alphanumeric characters. Contain both upper and lower case letters.
Contain at least one number (for example, 0-9).
Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/, or spaces).

Poor, or weak, passwords have the following characteristics:

Contain less than eight characters.
Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
Are some version of "Welcome123" "Password123" "Changeme123"

PASSPHRASES

A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!). **Passphrases are preferred whenever possible**.

SOCIAL ENGINEERING AVOIDANCE

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

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

If any employee or contractor encounters a social engineering attempt, the employee should contact the Security Incident Response team. For in-person social engineering attempts, the employee or contractor should contact a member of the Security Incident Response team or the employee's immediate manager.

TOP 10 THINGS TO KNOW ABOUT SECURITY AT CU*ANSWERS

ALWAYS USE A STRONG PASSPHRASE: Passphrases are stronger than passwords. I want to go to Jupiter! is better and easier to remember than Jup1t3r!. Network passwords should be at least 12 characters and must include two of the following three: special character, capital, or number. Spaces are considered special characters and are useful!

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

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

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

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

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

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

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

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

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