INFORMATION SECURITY
POLICY AND PROGRAM

UNDER THE CONTRACTS WITH OUR CLIENTS, CU*ANSWERS AGREES TO ADHERE TO THE LAWS PROTECTING CONSUMER INFORMATION, INCLUDING AN INFORMATION SECURITY PROGRAM.

POLICY 02	VERSION: 2.0
	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

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

This *Information Security Policy and Program* is designed to:

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

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

KEY TEAMS

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

SECURITY OFFICERS

The security officers of CU*Answers are any corporate officers, the VP of Network Technologies, the AVP of Managed Technologies, the Mangers of Network Engineering and Implementation, the Internal Auditor, and the Facilities Manager.

INCIDENT RESPONSE TEAM

The IR team consists of the following positions: CEO, CIO, COO, CFO, Executive VP of Sales, VP of Network Technologies, the Managers of Network Engineering and Implementation, Series-I Administration Manager, Writing Team Manager, and the Internal Auditor.

DATA CLASSIFICATION

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

EXAMPLES OF SENSITIVE MEMBER DATA

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

PROGRAM

IMPLEMENTATION

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

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

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.

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.

AUDITS

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

- The risk assessment
- The status of the controls
- Service provider arrangements
- Results of testing
- Breaches or violations reported to management