CLIENT SUPPORT POLICY

Because CU*Answers is responsible to protect the data of our credit union clients and members in the support process, this policy has been created to specifically outline what employees may or may not do during the client support process. This policy applies to teams with specific client service responsibilities as well as to all employees in their day-to-day interactions with clients.

NOTE: This policy is a companion to the "Data Security Policy," which addresses external access (sign-on) to key hardware systems (including IBM i systems and PCs) and internal security software for controlling sign-on privileges and authority.

CU*ANSWERS
A Credit Union Service Organization

POLICY VERSION CONTROL

Version: 3.0
Last Update: December 31, 2013
Board Ratified: April 2016

SECURITY PROFILES

CU Security Profiles: Online Clients

For online credit unions, individual IDs – referred to as "data center employee IDs" – will be assigned to all CU*Answers staff. Each data center employee ID is attached to a credit union employee ID referred to as an "alias." The credit union then controls what privileges are assigned to that alias, thus controlling access for all data center employee IDs that are attached to that alias. Passwords can be reset only by using a data center employee 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.

CU*BASE employee IDs 89-99, including 9*x* where *x* equals a character A-Z, are reserved for data center use as alias employee IDs.

CU Security Profiles: Self-Processing Clients

For our self-processing partners, a specific user profile (such as CUACSR) and employee ID 89 are designated for use by all CU*Answers support staff. The password attached to this user profile and employee ID will be changed at least every 60 days or when deemed necessary. When someone leaves CU*Answers' employment, the password for employee ID 89 and the designated user profile will be changed immediately.

Credit Union Security Officers

Each credit union will designate a security officer(s) responsible for updating employee ID settings in CU*BASE. This person's name will be recorded in the CU*Answers Customer Master Database. Unless instructed otherwise by the credit union, the passwords, access privileges, and other settings on the reserved alias employee IDs are the responsibility of CU*Answers and can be changed by CU*Answers service personnel as needed to provide support to the credit union. Other than reserved alias IDs, CU*Answers client support staff will not perform updates to settings for credit union employee IDs under any circumstances.

Download Authority

CU*Answers utilizes a software tool that restricts which online users can upload or download data to or from CU*BASE. Credit unions can request specific employees be granted access to these commands for the purpose of completing certain tasks. Client Services must review these requests for accuracy and ensure that the signature provided is officially designated as a credit union security officer. This requirement is an intentional "speed bump" in the process intended to protect both the credit union and CU*Answers against potential fraud from employees attempting to gain unauthorized access to member data.

Each credit union will determine a policy regarding the security access allowed to data center employees.

This policy should include guidelines for the access privileges that will granted to user profiles (if appropriate) and designated Employee IDs or alias IDs. *(A sample policy is available from the CU*Answers website.)*

The signed policy will be retained by CU*Answers and staff will honor this policy when performing telephone support.

Policies will be reviewed by the CFO and CEO as part of the contract renewal process.

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 authori-zation will be maintained as necessary from appropriate credit union personnel with authority to approve such changes.

MAINTENANCE

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.

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.

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" or "CU" 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.

System Configuration Maintenance

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

Reports (Online Credit Unions)

To reduce the risk of exposing member data, CU*Answers personnel generally will not generate CU*BASE reports and send them to credit union print queues for its online clients. If during a support contact a credit union employee needs assistance generating a report, the CSR or other support staff will instruct the user how to perform the steps so that the report will be automatically channeled to the credit union's own printer.

One exception to this would be reports generated as part of batch repair programs that are necessary to correct a system anomaly. Typically in these situations, a batch of reports is created by the system then moved to individual credit union HOLDxx output queues (not directly to printers) by a CSR or other authorized personnel. Another exception is when a new client

converts to CU*BASE, the conversions team will generate a number of reports directed to credit union output queues as part of the data conversion process.

Password Resets

CU*Answers support personnel will never reset the password for a credit union staff Employee ID.

Although CU*Answers support personnel are able to reset User ID (CU*BASE login) passwords and vary on devices, credit unions are instructed that this procedure should be done by a credit union Security Officer. If a credit union security officer is not available, the credit union may request assistance from Client Services. A fee will be charged for this service (fee amount is listed in the official Pricing Guide, published annually and available from the CU*Answers website) and credit unions that request this service frequently will be brought to the attention of the internal auditor for special review.

WWW.CUANSWERS.COM