TIAA CREF
Financial Services

# TIAA-CREF ONLINE AUDITOR ACCESS
# AUTHORIZATION/CHANGE FORM



## ONLINE AUDITOR SERVICES

This application allows you to authorize third-party auditors to become users of TIAA-CREF's Administrator Services, which provides access to the secure Plan Administrator website at **www.tiaa-cref.org/administrators** and the Administrator Telephone Center (ATC). These resources will provide the information and tools you need to efficiently administer your retirement plans.

You can use this application to add auditors to your institution's authorized users list, and request removal of an auditor's access to the website.

### WEBSITE ACCESS

Granting access to your institution's auditor(s) will provide them with access to your annual plan financial reports and most sample documentation provided through TIAA-CREF's secure Plan Administrator website at **www.tiaa-cref.org/administrators**. Auditors are granted access to your reports after we receive your signature on the authorization form. Your auditor will continue to receive access to your reports until you notify us otherwise.*

**To complete this application, the following definitions will be helpful. There are two Authorization levels:**

### PRIMARY AUTHORIZER

A Primary Authorizer is the administrator who has the authority to add, edit and delete third-party auditors at the institution. This authorization level may have access to one or more Administrator Services Functions.

### THIRD-PARTY AUDITOR

A Third-Party Auditor is the person that has been approved by the Primary Authorizer to be a registered user of the secure Plan Administrator website in order to access Plan Financial Reports (the "Authorized User"). A Third-Party Auditor does not have the authority to add, edit or delete other auditors at the institution.

**Once completed, please print, sign and fax, mail or e-mail to TIAA-CREF. Refer to page 5 for our fax number, mailing address and e-mail address.**

**Please note that missing signatures, incomplete or inaccurate information on this form will delay the adding/removal of access for Third-Party Auditor, which can impact/delay their ability to access your institution's data available on our secure Plan Administrator website.**

## SECTION 1: GENERAL INFORMATION

Please indicate whether you are applying as a Primary Authorizer or a Third-Party Auditor at your institution. If you are a Primary Authorizer and are replacing a current user, complete the application for the replacement user and provide the name of the user(s) to be deleted in Section 4.

Provide the general information requested in Section 1 for the administrator who is being authorized to use TIAA-CREF's Administrator Services. E-mail addresses will remain confidential and will not be shared with any external entities.

**Check One**

☐ I am a Third-Party Auditor applying for online access to Plan Financial Reports. (Auditor and Primary Authorizer must sign Section 5.)

☐ I am a Primary Authorizer of my institution and am deleting access to TIAA-CREF's Plan Administrator Services for a Third-Party Auditor. Please complete the application for the replacement user (if applicable) and indicate the user to be deleted in Section 4.

* Please note: This represents a change in policy. Previously, auditors were granted access only for a 10 month period, subject to extension thereafter.

CONTINUED ON NEXT PAGE

TIAA CREF
Financial Services

# TIAA-CREF ONLINE AUDITOR ACCESS
# AUTHORIZATION/CHANGE FORM



## SECTION 1: GENERAL INFORMATION (CONTINUED)

Prefix

Auditor First Name

Middle Initial

Auditor Last Name

Auditing Firm Name

Title

Department

Street Address

City

State

Zip Code

Phone Number — —

Extension

E-mail Address

Fax Number

## SECTION 2: PLAN ACCESS

Third-Party Auditors may be granted privileges to view the institution's 500 Plan Book, Certified Annual Reports, Supplemental Annual Reports, including legacy ERISA based on SLA ERISA package, and Form 5500. Indicate the plans you would like to access:

☐ Authorize Access to all plans associated with my institution.

☐ Authorize Access to only the following plans (must be six digits):

TIAA CREF
Financial Services

# TIAA-CREF ONLINE AUDITOR ACCESS
# AUTHORIZATION/CHANGE FORM



## SECTION 3: SECURITY QUESTION AND ANSWER (REQUIRED)

Please choose a security question and provide your answer. This will be used for authentication when you call TIAA-CREF.

- ☐ What is your mother's maiden name?
- ☐ What is the city/town where you were born?
- ☐ What is the name of the street you grew up on?
- ☐ What is your favorite sports team?
- ☐ What is the name of your pet?

Your Answer

Name of the TIAA-CREF Client

Plan Number of the TIAA-CREF Client

Name of the Auditing Firm

## SECTION 4: DELETE AN EXISTING USER

**This section is to be completed by a Primary Authorizer.**

Please indicate any Third-Party Auditor(s) who should be deleted from your organization's list of Authorized Users.
We will redirect all appropriate correspondence and information to any replacement Third-Party Auditor listed in Section 1.

Please delete the following individual(s) from our institution's list of Authorized Users:

Name

Company

E-mail Address

Telephone Number — —

Name

Company

E-mail Address

Telephone Number — —

CONTINUED ON NEXT PAGE

TIAA CREF
Financial Services

# TIAA-CREF ONLINE AUDITOR ACCESS
# AUTHORIZATION/CHANGE FORM



## SECTION 4: DELETE AN EXISTING USER (CONTINUED)

Name

Company

E-mail Address

Telephone Number — —

## SECTION 5: SIGNATURES (REQUIRED)

If you are unsure of who your Primary Authorizer is for your institution please contact the Administrative Telephone Center at **888 842-7782**.

Please read the Security Guidelines on page 5. All signatories must agree to abide by these Guidelines. Please note that missing signatures, incomplete or inaccurate information on this form will delay the adding/removal of access for the Third-Party Auditor, which can impact/delay their ability to access your institution's data available on our secure Plan Administrator website.

I have read, and will comply with, the security guidelines set forth in this application.

**Auditor Name** (Print)(REQUIRED)

Phone Number — —

Extension

E-mail Address

**Signature**

Date (mm/dd/yyyy) / /

I approve adding/removing Administrator Services access for the auditor(s) listed on page 2 and 3 of this application and agree that I have read, and will comply with, the Terms and Conditions set forth in this application. **NOTE:** Please sign and date the form **only** after the third party signs this form. We will not accept this form unless the date you sign this form is on or after the date the third party signs this form.

**Primary Authorizer Name** (Print)(REQUIRED)

Phone Number — —

Extension

E-mail Address

**Signature**

Date (mm/dd/yyyy) / /

F11273-0711-04

## RETURN COMPLETED APPLICATION(S) USING ONE OF THESE METHODS

| Fax to | Mail to | E-mail |
|---|---|---|
| **800 842-5916** | **TIAA-CREF**<br>**P.O. Box 1259**<br>**Charlotte, NC 28201** | **paservices@tiaa-cref.org** |

Be sure to send all pages together. TIAA-CREF will notify you once this Application has been processed.

Any information missing on this application will delay processing. If you have any questions about how to fill out this form or if you need to know who the Primary Authorizer is, please call the Administrator Telephone Center at **888 842-7782**.

**NOTE**: You may download additional copies of this application from the TIAA-CREF Plan Administrator website at **www.tiaa-cref.org/administrators**.

## SECURITY GUIDELINES

The Auditor Services developed by TIAA-CREF allow authorized users of an institution to access certain information relating to such institution's participants' TIAA-CREF accounts and accumulations for the purpose of plan administration or counseling your employees.

**THE INFORMATION OBTAINED THROUGH THESE SERVICES IS EXTREMELY SENSITIVE AND HIGHLY CONFIDENTIAL, AND AUTHORIZED USERS OF THESE SERVICES AGREE TO MAINTAIN THE SECURITY OF THE SERVICES AND THE CONFIDENTIALITY OF THE INFORMATION DISCLOSED IN THE PLAN ADMINISTRATOR WEBSITE.**

**USE OF THESE SERVICES SIGNIFIES YOUR AGREEMENT TO COMPLY WITH THESE SECURITY GUIDELINES, AND TIAA-CREF RESERVES THE RIGHT TO REVOKE ACCESS TO THESE SERVICES FOR ANYONE WHO VIOLATES THESE GUIDELINES.**

From time to time, authorized representatives of TIAA-CREF may monitor the use of these services by authorized users; authorized users should not expect their use of the services to remain private and agree that TIAA-CREF may monitor and/or disclose their activity.

TIAA-CREF will revoke access for any authorized user who engages in improper conduct with regard to these services or the information obtained through the services. Examples of improper conduct include:

- Deliberately bypassing or probing security measures (other than testing in accordance with generally accepted auditing standards)
- Disclosing, except as otherwise permitted or provided herein, or failing to protect any information contained in the website or disclosed
- Failure to maintain the confidentiality of the security question and answer or the user ID and password
- Sharing the security question and answer, the user ID or password with any other individual
- Sharing or distributing proprietary or copyrighted software
- Using these services in connection with any unauthorized, illegal, fraudulent or unethical activities, or activities that may be embarrassing or detrimental to TIAA-CREF (other than in accordance with generally accepted auditing standards)
- Introducing or attempting to introduce viruses into TIAA-CREF's systems
- Transmitting encrypted materials in violation of applicable laws, including but not limited to privacy and export laws

TIAA-CREF will not be held liable for the misuse of these services. In the event you or any authorized user terminates employment with your institution, TIAA-CREF requests that you notify us promptly and we will revoke these services.

## DISCLAIMER OF WARRANTIES

Neither TIAA, the Primary Authorizer nor the Authorized User (each, a "Party") makes any warranties, expressed or implied, concerning any subject matter of this Agreement, including, but not limited to, any implied warranties of merchantability and fitness for a particular purpose.

## LIMITATION OF LIABILITY

Except with respect to a Party's confidentiality, privacy, and security obligations under this Agreement, in no event will any Party be liable to any other Party for any special, indirect, incidental, punitive or consequential damages (including loss of use, data, business, or profits) arising out of or in connection with this transmission or receipt of data pursuant to this Agreement, whether such liability arises from any claim based upon contract, warranty, tort (including negligence), product liability or otherwise, and whether or not a Party has been advised of the possibility of such loss or damage.

## INDEMNITY

The institution represented by the Primary Authorizer, (the "Indemnifying Party") agrees to indemnify and hold TIAA (the "Indemnified Party") harmless for any claims or demands, including costs, expenses and reasonable attorney's fees due to: (a) unauthorized access to or misuse of the data facilities of the Indemnified Party through the Third Party Auditor's or the Indemnifying Party's data facilities or equipment; or (b) the misuse of information obtained through the Indemnified Party's data facilities by the Indemnifying party or any of its employees, agents, contractors, or other persons (whether or not authorized pursuant to this form, including but not limited to the Authorized Users and the Third Party Auditor).

The Indemnifying Party agrees to defend the Indemnified Party against any such claims or demand.

## CONFIDENTIALITY

The Parties acknowledge that by reason of their relationship to each other hereunder, each will have access to certain information and materials concerning the other's technology. products and clients that is confidential and of substantial value to that party, or which constitutes personal information protected under privacy laws ("Personal Information"), which value would be impaired if such information were disclosed to third parties or, in the case of Personal Information, the security of which is subject to privacy laws ("Confidential Information"). Except as otherwise provided herein, each party agrees that it will not use in any way for its own account, nor disclose to any third party, any such Confidential Information revealed to it or exposed by the other party. Each party will take reasonable precautions to protect the confidentiality of such Confidential Information and, with respect to Personal Information, shall comply with all applicable privacy laws. Upon request by the receiving party, the disclosing party shall advise whether or not it considers any particular information or materials to be Confidential Information. The receiving party acknowledges that unauthorized use or disclosure thereof could cause the disclosing party irreparable harm that could not be compensated by monetary damages. Accordingly each party agrees that the other will be entitled to seek injunctive and preliminary relief to remedy any actual or threatened unauthorized use or disclosure of such other party's Confidential Information. Except with respect to Personal Information, the receiving party's obligation of confidentiality shall not apply to information that: (a) is already known to the receiving party, is independently developed by the receiving party or is publicly available at the time of disclosure; (b) is disclosed to the receiving party by a third party who is not in breach of an obligation of confidentiality to the party to this agreement which is claiming a proprietary right in such information; or (c) becomes publicly available after disclosure through no fault of the receiving party. In addition, the receiving party's obligation of confidentiality shall also not apply to disclosures of Confidential Information (which may include Personal Information) required pursuant to law, rule or regulation, or as needed to fulfill professional auditing obligations and standards; such disclosures of Confidential Information to fulfill professional auditing obligations and standards are intended to include disclosures (1) in connection with quality and peer reviews and (2) to the Public Company Accounting Oversight Board and similar bodies with jurisdiction over the Third-Party Auditor (ie, the Authorized User).

CONTINUED ON NEXT PAGE

## CONFIDENTIALITY (Continued)

These limited rights of disclosure do not override Authorized User's obligations under AICPA Rule 301 and similar rules and regulations adopted by the boards of accountancy of the various states regarding confidential treatment of client information to which Authorized User will continue to abide. As between the receiving party and the disclosing party, the confidentiality obligations herein shall apply to Personal Information regardless of whether any of the information satisfies exceptions (a), (b) or (c) to confidentiality set forth in this paragraph. This confidentiality obligation shall survive the termination or expiration of this Agreement.

Each of the Parties will safeguard the information accessed or transmitted between them under this Agreement as Confidential Information, highly sensitive data and not disclose it to any third party except as otherwise permitted or provided herein. The information transmitted and disclosed between the Parties pursuant to this Agreement will be limited to only such data as is necessary to carry out the Authorized Party's obligations to the Plan Administrator and the institution represented by the Primary Authorizer. Should any Party access information that is outside such scope, such party shall promptly notify the other Parties of the discovery.