QUESTIONS: Call the Administrator Telephone Center (ATC) at **888-984-0010.**

ADMINISTRATOR SERVICES

This application allows you to authorize administrators at your agency to become users of TIAA's Administrator Services, which provides access to the secure Plan Administrator website 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 or delete users from your agency's authorized users list, and upgrade or remove a user's access to online functionality.

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 other Plan Administrators at the agency. This authorization level may have access to one or more Administrator Services Functions.

PLAN ADMINISTRATOR

A Plan Administrator is an administrator who has been authorized to use TIAA's Online Administrator services. A Plan Administrator cannot add, edit or delete the access rights of another administrator. This authorization level may have access to one or more Administrator Services Functions.

NEITHER THE PRIMARY AUTHORIZER NOR ANY PLAN ADMINISTRATOR IS AUTHORIZED TO GRANT ACCESS TO ANY INDIVIDUAL OUTSIDE OF YOUR AGENCY THROUGH THE USE OF THIS FORM. ANY ACCESS TO AGENTS, REPRESENTATIVES OR SUBCONTRACTORS OF YOUR AGENCY MUST BE ADDRESSED SEPARATELY FROM THIS FORM.

Once completed, please print, sign and fax, mail or email to TIAA. Refer to page 6 for our fax number, mailing address and email address.

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

EDELIVERY TERMS AND CONDITIONS

By requesting we deliver any documents to you electronically, you agree to the following terms and conditions, and acknowledge you can electronically access, view, print and save these documents.

Your request to receive documents electronically requires you to have Internet access and a valid email account. We will email you a notification when a document is available for viewing and you can thereafter log in to your secure TIAA account to access it. In the case of public documents like Prospectuses, Supplements, Annual Reports and Semi-Annual Reports, we will include a direct link to the document for your convenience.

Accessing public documents will not require you to log in to the secure site. Once you access the document, we provide the option for you to save it to your personal computer or print it. We may provide certain documents in portable document format, often referred to as a PDF. This format requires you to use free Adobe Reader software, which you can download at **adobe.com**.

Your preference selections remain effective until changed by you, or as the result of service necessity (e.g., incorrect or nonworking email address), or upon notice from TIAA. Should you have any questions, wish to change your eDelivery preferences, or request a paper version of any document, please contact your Relationship Manager. If your plan is serviced by the Administrator Telephone Center, you can speak with a representative at **888-984-0010** weekdays, 8 a.m. to 6 p.m. (ET).

When accessing the Internet, you may incur online subscription charges through your Internet service provider. TIAA, however, charges no fee for electronic delivery.

Please print using black or dark blue ink.

Be sure to send all pages together. TIAA 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, please call the Administrator Telephone Center at **888-984-0010**.

SECTION 1: GENERAL INFORMATION

Please indicate whether you are applying as a Primary Authorizer or a Plan Administrator at your agency. 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 5.

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

Check One

☐ I am applying as a Primary Authorizer of my agency. Sign Section 6 and obtain the signature of the current Primary Authorizer. If you are the only Primary Authorizer at your agency, check here:

☐ I am applying as a Plan Administrator of my agency. Sign Section 6 and obtain the signature of the Primary Authorizer.

☐ I am a Primary Authorizer of my agency and am deleting access to TIAA's Plan Administrator Services for a Primary Authorizer and/or a Plan Administrator. Please complete the application for the replacement user (if applicable) and indicate the user to be deleted in Section 5.

First Name | Middle Initial | Last Name | Suffix

Agency Name

Title | Department

Street Address

City | State | Zip Code

Contact Telephone Number | Extension

Email Address | Fax Number

2. PLAN INFORMATION AND ACCESS

Plan Number: 4 0 6 0 8 1

Name of Employer: NEW YORK STATE DEFINED CONTRIBUTION PROGRAM

Agency/Public Institution

Note: List all agencies for which you would like access including name, address, website and Location or Payroll Code.

2. PLAN INFORMATION AND ACCESS (CONTINUED)

Please list agencies for which you would like access:

Agency Name	Address	Agency Website	Location Code/ Payroll Code

3. ADMINISTRATOR SERVICES FUNCTIONS

☐ **Plan Administration** Ability to Enroll employees/Approve & Decline Retirement Plan Elections (RPE) Access to employee account information, (dates & vesting status) including account balance, contributions & asset allocation.

☐ **General Access** Limited to general inquir(i)es and requests (nonconfidential data) & ordering print materials.

☐ **Contributions** This includes activities related to contributions made to the plan.

NOTE: If your agency's payroll is administered by a state or local payroll administrator, a TIAA profile will be created.

If your agency's contribution file is remitted to TIAA directly by a Third-Party Provider, for example, ADP, Ceridian or Paychex, please submit a form for those representatives checking only the functions that apply.

Person requesting access for Plan Administration will answer questions or authorize the following:

☐ Contribution remittance files and wires

☐ Distribution requests from participants

☐ Loan requests from participants

☐ Plan compliance corrections

☐ Receive prospectus correspondence

4. SECURITY QUESTION AND ANSWER REQUIRED

Please choose a security question and answer. TIAA will use this question to authenticate caller.

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

Answer

5. COMPLETE ONLY TO DELETE AN EXISTING USER

Name	Title
Name	Title

6. PLAN SPONSOR SIGNATURE (REQUIRED)

I certify under penalties of perjury that I am duly authorized to: (1) access and act upon plan-related information provided through TIAA's Administrative Services for purposes of administering the VDC plan and (2) complete and sign this form.

Person Requesting Access (person listed in Section 1)-This signature is always required (for person requesting).

Please sign your full legal name with suffix, if applicable, using black or dark blue ink. Digital signatures are not accepted.

Name (Please print) | Contact Telephone Number | Extension

Signature | Today's Date (mm/dd/yyyy) / / 20

Primary Authorizer

☐ **New Primary Authorizer** ☐ **Additional Primary Authorizer**

Please sign your full legal name with suffix, if applicable, using black or dark blue ink. Digital signatures are not accepted.

Name (Please print) | Contact Telephone Number | Extension

Signature | Today's Date (mm/dd/yyyy) / / 20

Email Address

I have read, and will comply with, the security guidelines set forth in this application. I approve the Plan Administrator to have access to the Administrator Services indicated herein.

Please sign your full legal name with suffix, if applicable, using black or dark blue ink. Digital signatures are not accepted.

Current Primary Authorizer Name REQUIRED (Please print) | Contact Telephone Number | Extension

Signature | Today's Date (mm/dd/yyyy) / / 20

Email Address

RETURN COMPLETED FORM(S) TO:

FAX:
800-842-5916

STANDARD MAIL:
TIAA
P.O. Box 1268
Charlotte, NC 28201-1268

EMAIL:
paservices@TIAA.org

TERMS AND CONDITIONS

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 ALL INFORMATION DISCLOSED IN THE PLAN ADMINISTRATOR WEBSITE.

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

From time to time, authorized representatives of TIAA 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 may monitor and/or disclose their activity. TIAA 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
- Disclosing or failing to protect information disclosed in the Plan Administrator website
- Failure to maintain the confidentiality of the security question and answer or the user ID and password
- Sharing the security question, answer, 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
- Introducing or attempting to introduce viruses into TIAA's systems
- Transmitting encrypted materials in violation of export laws
- Transmitting personal information in violation of privacy laws

TIAA will not be held liable for the misuse of these services. In the event you or any Authorized User terminates employment with, or consulting services for, your institution, TIAA requests that you notify us immediately and we will revoke these services.

Disclaimer of Warranties. Neither TIAA, the Primary Authorizer nor any 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 Agreement, including without limitation, any damages resulting from any delay, omission or error in the electronic 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. Each of the Primary Authorizer and the TPA with respect to the Authorized User and any of its representatives whether authorized hereunder or not (as the case may be, 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 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 authorized or unauthorized). 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").

Should such Confidential Information be orally or visually disclosed, the disclosing party shall summarize the information in writing as confidential within thirty (30) days of disclosure. Each party agrees that it will not use in any way for its own account, except as provided herein, nor disclose to any third party, any such Confidential Information revealed to it or exposed by the other party. Each party will take every reasonable precaution to protect the confidentiality of such Confidential Information and, with respect to Personal Information, shall comply with all applicable privacy laws as an agent of the disclosing party, for this limited purpose. 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 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. 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 the exceptions to confidentiality set forth in the immediately preceding sentence. 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. The information transmitted 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. Should any Party access information that is outside such scope, such party shall immediately notify the other Parties of the discovery.