DTCC
Securing Today. Shaping Tomorrow.®

55 Water Street
New York, NY 10041-0099

Tel: 212-855-1000

# DTCC New York State Department of Financial Services ("NYSDFS") Terms

The DTCC NYSDFS Terms apply to the processing of Nonpublic Information, as defined in the NYSDFS regulation 23 NYCRR 500 (the "Regulation"), by the Depository Trust & Clearing Corporation, by itself or through any of its subsidiaries, affiliates or joint ventures, together or separately (collectively as "DTCC") and DTCC Members, Participants, Users or Clients.

These terms to apply between DTCC and it's Members, Participants, Users or Clients when the following conditions are met:

- DTCC Member, Participant, User or Client is directly subject to the Regulation as a Covered Entity, as defined by the Regulation;
- DTCC is processing Nonpublic Information, as defined by the Regulation, provided by the Member, Participant, User or Client; and
- A formal notice of applicability has been provided to DTCC.

## Notice of Applicability

In order to apply the DTCC NYSDFS Terms regarding the protection and processing of such Nonpublic Information by DTCC, a formal notice of applicability must be submitted by the DTCC Member, Participant, User or Client.

This notice must include (1) the details listed below, (2) an acknowledgement of the agreement to the DTCC NYSDFS Terms posted on DTCC.com, and (3) be submitted to PrivacyOffice@dtcc.com.

The DTCC NYSDFS Terms will become effective with respect to such entity once DTCC has obtained all of the information requested and provided an email confirmation that all information required has been received.

| | |
|---|---|
| **Firm Name:** | |
| **NYSDFS Institution #:** | |
| **Brief description of the services provided by DTCC:** | |
| **Overview of the Nonpublic Information processed by DTCC:** | |
| **Contact name and email address where confirmed Cybersecurity Events will be reported to:** | |

# DTCC New York State Department of Financial Services ("NYSDFS") Cybersecurity Terms for Financial Services Companies 23 NYCRR 500 (the "Regulation")

These Terms between DTCC Members, Participants, Users or Clients, each a Party, together, "the Parties" and the Depository Trust & Clearing Corporation and/or any of its subsidiaries, affiliates, or joint ventures ("DTCC") who is providing one or more services to the Parties apply to the protection and Processing of Nonpublic Information of a Party by DTCC.

## 1. DEFINITIONS AND INTERPRETATION

These Terms relate to the Processing of Nonpublic Information that is subject to the Regulation. The terms "**Covered Entity**", "**Cybersecurity Event**", "**Information System**", "**Multi-Factor Authentication**", "**Nonpublic Information**", "**Person**", "**Risk Assessment**", **"Risk-Based Authentication",** "**Chief Information Security Officer**" or "**CISO**", and "**Third-Party Service Provider**" all have the meanings given to those terms in the Regulation.

"**Processing**" or **"Process"** means any operation or set of operations which is performed on Nonpublic Information that includes, but is not limited to collection, recording, retrieval, use, combination, disclosure by transmission, dissemination or otherwise making available, any covered information.

## 2. ACCESS CONTROLS AND MULTI-FACTOR AUTHENTICATION

2.1. DTCC shall maintain written policies and procedures for access controls that limit access to the DTCC's relevant Information Systems that Process or have access to the Party's Nonpublic Information.

2.2. Based on its Risk Assessment, DTCC shall use effective controls which may include Multi-Factor Authentication or Risk-Based Authentication to protect against unauthorized access to the Party's Nonpublic Information.

2.3. Multi-Factor Authentication shall be used by any individual accessing the Party's Nonpublic Information on DTCC's Information Systems from an external network.

## 3. ENCRYPTION OF NONPUBLIC INFORMATION

3.1. DTCC shall maintain written policies and procedures for encryption to protect the Party's Nonpublic Information in transit and at rest.

3.2. As part of its cybersecurity program, based on its Risk Assessment, DTCC shall implement controls, including encryption, to protect the Party's Nonpublic Information held or transmitted by DTCC both in transit over external networks and at rest.

3.3. To the extent DTCC determines that encryption of Nonpublic Information in transit over external networks or at rest is infeasible, DTCC may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Party's CISO.

## 4. INCIDENT RESPONSE

4.1. Upon discovery and confirmation of a Cybersecurity Event involving the Party's Nonpublic Information by the DTCC, DTCC shall, and without undue delay, notify the Covered Entity, to the extent known, (a) the nature of the Nonpublic Information breached including, where possible, the data fields and approximate number of records concerned, (b) the location, if known and applicable, of any individual who can be identified from the Nonpublic Information, and (c) the measures taken by DTCC to address the Cybersecurity Event. Reports made under this section shall be submitted to the contact and email address provided by the Parties in their Notice of Applicability.