TD SYNNEX CORPORATION

POLICY GOVERNING COLLECTION, USAGE AND RETENTION OF BIOMETRIC INFORMATION

Original Effective Date	**July 2022**
Responsible Department	**Privacy – Legal**
Approved By	Name: **David Vetter**
	Role: **EVP, Chief Legal Officer**
Available Languages	**English**
Geographic Scope	**Global**
Version #	**2**
Date of Last Update	**June 2023**

I. PURPOSE AND SCOPE

When authorized to do so, TD SYNNEX Corporation (together with its direct and indirect parents, subsidiaries, and affiliates, the "Company") collects, uses and/or stores biometric identifiers or biometric information – namely, information collected from fingerprints, or via facial recognition/face geometry scan – (collectively, "biometric information") from employees or contractors (collectively, "staff") in connection with the administration of access to facilities and equipment; for timekeeping systems and associated time/attendance records; for the safety of staff; and for other legally permitted purposes relating to the operation of the Company's business or management of its staff. The Company has established this Policy outlining guidelines for the Company's collection, disclosure, retention and destruction of biometric information. Further information about how TD SYNNEX processes biometric information and about your rights as a data subject related to TD SYNNEX processing your personal data can be found on the HUB in Policy Central, under Internal Privacy Statements.

The Company, in its sole discretion, reserves the right to amend this Policy at any time.

II. COLLECTION & DISCLOSURE

It is the Company's policy to provide notice and obtain consent from staff before collecting their biometric information, including where such information is collected by a third-party service provider on the Company's behalf. Such notice will be designed to inform staff about the biometric information being collected, the purpose(s) for the collection and the length of time the information will be stored.

Please note that under no circumstances will the Company sell, lease, trade, or otherwise profit from staffs' biometric information. Absent each staff member's consent or unless required by law, such as a valid warrant, subpoena or government order, the Company will not disclose or disseminate biometric information to third parties other than to third party suppliers providing services on behalf of Company for the purposes described in Section I above. Any third party supplier the Company shares any biometric information will be specifically identified prior to or at the time consent is requested and will be subject to appropriate contractual restrictions.

During the time the Company retains biometric information, the Company exercises reasonable care, and contractually requires each third party supplier maintaining biometric information to exercise reasonable care, in protecting such information in a manner that is the same or more protective than the manner in which it protects other confidential and sensitive information.

III. RETENTION SCHEDULE

When permitted to collect biometric information, the Company will retain the information collected from staff until they are terminated or leave the Company, from contractors until they are no longer providing services to Company or until a staff member withdraws consent (whichever occurs first), unless further retention is required by law (such as longer national retention period, a valid warrant, subpoena or government order). TD SYNNEX has the right to keep the data longer to defend against or enforce legal claims. The Company therefore will retain your biometric information not longer than 90 days (for US residents up to 3 years) after employment or service ends or after consent is withdrawn.

IV. GUIDELINES FOR DESTRUCTION

Subject to any applicable legal requirements to retain such information as set forth in Section III above, it is the Company's policy to permanently delete and/or destroy biometric information it collects from staff and instruct relevant third party suppliers to permanently delete and/or destroy biometric information they maintain, from all systems, files and backups, including, but not limited to, cloud storage systems. The Company shall require all third party suppliers that collect or process employee biometric information to attest that they have securely and permanently deleted and/or destroyed biometric information in accordance with this Policy.

V. Helpful Contacts

If you have questions regarding this policy or how it impacts your role, you should contact your manager, a Privacy Champion (where available) or the Privacy Office at privacy@tdsynnex.com.

VI. Related Documents/Forms and Policies

To learn more, please visit Policy Central:

Code of Conduct

Processing of Personal Data Policy

Data Classification & Handling Policy

Cybersecurity & Acceptable Use Policy

Reporting Concerns

If you see or suspect a violation of this policy, it is your responsibility to speak up. We'll listen.

You can talk to your manager, your leadership team, HR, Legal, or our Ethics and Compliance team. Alternatively, you can submit a concern to our Board's Audit Committee or through the Ethics Line website or hotline.

If desired, you can even report anonymously. If you do report anonymously, be sure to check back through the Ethics Line website or hotline regularly to provide further details when required.

You are always protected from retaliation when you speak up in good faith.

There is zero tolerance for retaliation at TD SYNNEX. If you believe someone has retaliated against you, you should report the matter immediately. Any act of retaliation is grounds for discipline, up to and including termination.