Confidentiality Policy

TNFX is the trade name of TNFX Ltd., a company registered in the Seychelles and authorized as a Securities Dealer by the Financial Services Authority (FSA) of Seychelles with license number SD133 and its principal office located at CT House, Office 3A, Providence, Mahe, Seychelles.

These Terms constitute a legally binding contract between you and **TNFX** which you accept for yourself and on behalf of any principal or principals on whose behalf you are acting as agent by giving us instructions to deal or accepting services from us. These Terms supersede any other general terms of business or similar documents that may have been previously issued to you by us.

For your own protection, you should read and fully understand these Terms prior to submitting your account application to **TNFX**. If you do not understand anything in these Terms or the documents incorporated by reference, you should contact **TNFX** to ask for further information or seek independent professional advice before you open an account, place any order or enter into a transaction with **TNFX**.

Confidentiality Policy

1. Purpose and Scope

This Confidentiality Policy outlines the principles and procedures adopted by *TNFX LTD* (hereinafter referred to as the Company") to ensure the confidentiality, integrity, and protection of all non-public information relating to clients, counterparties, employees, and business operations.

This Policy applies to all directors, officers, employees, agents, introducing brokers, contractors, and any third parties acting on behalf of the Company.

2. Definition of Confidential Information

For the purpose of this Policy, **Confidential Information** includes, but is not limited to:

- Client personal data (identity documents, contact details, financial information)
- Trading data (account balances, positions, order history, strategies)
- Compliance records (KYC, AML, sanctions screening results)
- Internal systems, pricing models, liquidity arrangements, and risk management data
- Business plans, financial statements, and proprietary methodologies
- Communications between the Company and its clients or regulators

Confidential Information may be written, electronic, oral, or otherwise recorded.

3. Collection and Use of Information

The Company collects and processes Confidential Information strictly for legitimate business purposes, including but not limited to:

- Client onboarding and verification (KYC/CDD)
- Provision of trading and brokerage services
- Risk management, compliance monitoring, and fraud prevention
- Regulatory reporting and audits
- Customer support and account administration

Information is collected on a **need-to-know and purpose-limitation basis**.

4. Confidentiality Obligations

All persons subject to this Policy are required to:

- Maintain strict confidentiality of all non-public information
- Prevent unauthorized access, disclosure, or misuse of Confidential Information
- Use Confidential Information solely for authorized business purposes
- Refrain from sharing information with unauthorized persons, internally or externally

These obligations continue **during and after** the termination of employment or contractual engagement.

5. Disclosure of Confidential Information

Confidential Information shall **not** be disclosed to third parties except in the following circumstances:

- Where disclosure is required by applicable laws, regulations, or court orders
- To regulators, supervisory authorities, or law enforcement agencies
- To service providers or counterparties under strict confidentiality agreements
- With the explicit consent of the client

Any disclosure shall be limited to the **minimum necessary information** required to fulfill the purpose.

6. Data Security and Protection Measures

The Company implements appropriate **technical, administrative, and organizational safeguards**, including:

- Secure IT infrastructure and encrypted data storage
- Access controls and role-based permissions
- Monitoring and logging of system access
- Regular security reviews and compliance audits
- Employee training on data protection and confidentiality

Reasonable measures are taken to protect information from loss, misuse, unauthorized access, or disclosure.

7. Cross-Border Data Transfers

Where Confidential Information is transferred or processed outside the jurisdiction of incorporation, the Company ensures that:

- Adequate data protection standards are applied
- Transfers comply with applicable data protection laws
- Contractual safeguards are in place with third parties

8. Breach of Confidentiality

Any suspected or actual breach of confidentiality must be **reported immediately** to the Compliance Department.

The Company reserves the right to:

- Investigate breaches promptly
- Take disciplinary or legal action where appropriate
- Notify regulators or affected clients when required by law

9. Client Rights

Clients have the right to:

- Request access to their personal data
- Request correction of inaccurate information
- Request deletion of data where legally permissible
- Raise concerns regarding the handling of their information

Requests shall be handled in accordance with applicable regulatory requirements.

10. Retention of Information

Confidential Information is retained only for as long as necessary to:

- Fulfill contractual and business obligations
- Meet regulatory and legal record-keeping requirements

After the retention period, data is securely deleted or anonymized.

11. Amendments

The Company reserves the right to amend this Confidentiality Policy at any time to reflect changes in laws, regulations, or business practices. Updated versions will be made available through official communication channels.