Anti-Fraud Policy

1. Introduction

This Anti-Fraud Policy (the "Policy") is established by Vault Fintech Solutions s.r.o. ("Vault", "the Company", "we", or "us") to prevent, detect, and respond to fraudulent activity, and to ensure compliance with relevant legal obligations. This Policy will be periodically reviewed and updated to reflect changes in applicable laws, regulatory expectations, and industry best practices.

2. Definitions

Fraud: Any intentional act of deception or misrepresentation committed to secure an unfair or unlawful gain.

Fraudulent Activity: Any activity involving false representation, misuse of company systems, or unauthorized transactions.

Suspicious Activity: Unusual behavior or transaction patterns that may indicate fraudulent conduct.

3. Fraud Prevention Measures

Vault employs a comprehensive fraud prevention framework, including:
- User verification through robust KYC/AML checks;
- Real-time transaction monitoring to detect anomalies;
- Secure account access controls;
- Periodic internal audits;
- Confidential whistleblower reporting channels.

4. Detection and Investigation

Suspicious activity is actively monitored. If detected, transactions may be held for review, further user verification requested, and affected accounts may be frozen. Documented cases may be reported to authorities in accordance with legal obligations.

5. Response to Fraud

In the case of confirmed fraud, Vault will:
- Act immediately to prevent further financial impact;
- Notify affected parties as necessary;
- Report the case to law enforcement and regulatory authorities;
- Apply remedial actions to prevent recurrence.

6. Sanctions and Legal Actions

Those found engaging in fraud may face:
- Account suspension or termination;
- Legal action under Czech and EU law;
- Liability for financial damages.

7. Policy Statement

Vault maintains a zero-tolerance stance against all forms of fraud and is committed to thorough investigation and legal action against individuals involved in fraudulent behavior. Adequate resources will be allocated to ensure effective implementation and communication of this Policy.

8. Purpose and Scope

This Policy outlines the responsibilities of all parties in preventing fraud, actions to be taken when fraud is suspected, verification mechanisms, reporting processes, and recovery plans.

9. Legislative Compliance

This Policy complies with all applicable laws in the Czech Republic and other relevant jurisdictions. Vault ensures compliance through internal policies and procedures.

10. User Verification

Users must provide accurate and valid personal information. Providing false information or documents will be considered fraudulent. Vault may verify this data directly or through authorized third parties, applying appropriate security measures as detailed in our Privacy Policy.

11. Account Security

Users are responsible for securing their login credentials and for all activity under their account. In the event of suspicion of compromise, users must immediately notify Vault. Delays in reporting may result in liability for any losses incurred.

12. Key Responsibilities

Vault is responsible for:
- Regularly assessing fraud risks;
- Maintaining effective fraud prevention systems;
- Ensuring staff are aware of their responsibilities;
- Establishing clear reporting and escalation protocols.

13. Fraud Detection and Investigation

Vault's Operational Anti-Fraud Department, led by the Head of Anti-Fraud Services, is responsible for detecting, investigating, and responding to fraud. This department oversees fraud-related user and transaction evaluations.

14. Miscellaneous

This Policy is subject to periodic updates. By using Vault services, users agree to comply with the principles outlined in this Policy.