EMERGENCY MANAGEMENT AND BUSINESS CONTINUITY
Measures Applied in Unexpected Situations

Dear Customer,
As Finnova, acting as a crypto asset service provider, we conduct our activities within the framework of the Capital Markets Board (SPK) regulations and adopt the fundamental principle of protecting investor security at the highest level.
Finnova Technology has developed a comprehensive unexpected situation plan to protect our customers' assets and be prepared against potential risks. Within this framework, various measures have been taken to minimize customer risks and ensure service continuity.

Our customers' assets are held in secure custody institutions, minimizing the risk of direct damage in emergencies or unexpected situations. However, due to extraordinary circumstances, service interruptions, communication breakdowns, or failure to execute instructions may occur. Our Business Continuity Plan aims to ensure that our operations continue with minimal disruption in such cases.

Risk Mitigation Measures and Communication Protocols

1. System Security and Backup
   Our platform activates the emergency recovery plan under the following critical conditions:

- External Attacks: When cyber-attacks targeting our system infrastructure or wallets are detected,
- Hot Wallet Security: If assets in our hot wallets are deemed at risk,
- External Service Provider Interruptions: If liquidity providers, blockchain networks, or critical third-party services experience incompatibility or outages,
- Suspicious Transfers: When unusual deviations are observed in crypto asset transfers,
- Balance Inconsistencies: If systemic inconsistencies or errors are detected in user balances,

In these cases, our automatic early warning systems activate, and the recovery plan is implemented immediately with the approval of the board of directors.

What Happens to Customer Assets?
Within the scope of the recovery plan, the security of customer assets is the highest priority, and the following measures are promptly taken:

- Wallet Security: Assets in hot wallets are moved to cold wallets and isolated from the system.
- Transaction Restrictions: Wallet addresses at risk are put into transaction-blocked mode.
- Balance Verification: User balances are verified by blockchain analysis systems.
- Unauthorized Transfer Prevention: No asset transfers occur without completing manual approval processes.
- Alternative Security Measures: If necessary, backup wallet infrastructure is activated.

All these operations are carried out transparently, documented with log records and external audit processes.

How Are Account and Transaction Processes Affected?
When the emergency plan is activated, temporary transaction restrictions may be applied to protect customer assets:

- Withdrawal transactions may be halted and only allowed after manual review.
- Account accesses are put into monitoring mode to track abnormal login and transaction

activities.

- Wallet balances can be viewed in read-only mode.
- Users are informed about the process via email, SMS, and in-platform notifications.

These restrictions are fully temporary and normal operations resume once security is ensured.

2. Financial Transactions and Customer Security

- EFT or transfer instructions of our customers are processed by authorized staff after identity verification and authorization checks.
- Requests for EFT, transfers, or account-to-account transfers to third parties are strictly not accepted.
- In emergency and unexpected situations, customers will be enabled to transfer their assets smoothly to their desired financial institution.

3. Alternative Communication Channels

- In extraordinary situations, our customers can contact us via our website or alternative communication lines.
- Relevant contact information will be regularly shared on our website and in monthly statement documents.

4. Emergency Scenarios and Notification Process

- Our company manages all processes diligently during unexpected situations, from operational services to employee safety, to continue protecting customer rights.
- If the Board of Directors decides to suspend operations, all customers will be duly informed through all our communication channels and their transactions will be completed smoothly if possible.

Customer Service and Alternative Contact Information

- Phone: +90 444 59 10
- Email: destek@finnova.com.tr
- Web: www.finnova.com.tr

Our company's main headquarters is located at Barbaros Mah. Begonya Sok. A+live Plaza Tower No:7/15, Ataşehir / Istanbul.