



Information Security Policy

TDB Securities implements an information security management system to ensure the confidentiality, integrity, and availability of clients' financial and personal information, and operates in compliance with applicable laws and regulations of Mongolia as well as internationally recognized standards and best practices, including ISO/IEC 27001:2022, the NIST Cybersecurity Framework, and PCI DSS.

Assurances to Clients

- We classify and protect data (Public / Internal / Highly Confidential). "Highly Confidential" data is encrypted at rest, and TLS protection is applied during transmission.
- Access is controlled: privileges are granted strictly on a need-to-know basis and governed through RBAC. System administrator activities are monitored, and administrators do not have direct access to business data.
- We use official communication channels, and two-factor authentication (2FA) is required to access all official systems.
- Payment data protection: we do not store card PIN or CVV/CVC in our systems; card/account numbers are displayed in a masked format; and the payment data processing network is segregated.
- Incident management and notification: if client information is exposed to risk, we will provide a clear explanation as soon as practicable and issue guidance to mitigate potential risks. Where sensitive information is at risk, clients will be notified within 72 hours.
- We respect clients' data rights, including the right to be informed, to access their information, and to request corrections (corrections/updates are processed within three (3) business days following verification).
- Protection of confidential information: copying, uploading, or processing confidential information (including clients' personal data) on public AI platforms is prohibited.