

GLOBAL DATA SECURITY AND PRIVACY POLICY

Policy Owner Group:	Vantism Financial Solutions Risk Management & Compliance Committee
Governance Group:	Executive Security & Privacy Operations Council
Approved By:	Chief Information Security Officer (CISO)
Approval Date:	October 12, 2026
Effective Date:	October 12, 2026
Next Review Date:	October 12, 2027
Classification:	PUBLIC (For Client Transparency and Public-Facing Site Publication)

1. OBJECTIVE AND SCOPE

This Global Data Security and Privacy Policy ("Policy") describes Vantism Financial Solutions ("the Company" or "Vantismfin.com") baseline approach to information security and privacy. It applies to the collection, storage, transmission, processing, retention, and disposal of information handled by the Company, subject to applicable law, contractual commitments, and documented service-specific limitations. It applies to all internal personnel, external contractors, and third-party subprocessors handling information on behalf of the Company across all operational jurisdictions, including the United States, the United Kingdom, the European Economic Area (EEA), Canada, the Asia-Pacific (APAC) region, Japan, and the Middle East.

This Policy is a public transparency statement and does not replace applicable law, a client contract, Data Processing Agreement, privacy notice, or internal security standard. Where there is a conflict, applicable law and binding contractual obligations prevail.

2. ORGANIZATIONAL STATUS AND CAPACITY

Depending on the specific contractual engagements and the nature of the processing activity, the Company's regulatory status is defined as follows:

- **Data Controller:** The Company acts as an independent Data Controller for data points collected for internal business administration, regulatory compliance, corporate recordkeeping, billing, marketing, and security log maintenance.
- **Data Processor / Subprocessor:** For core accounting, bookkeeping, and tax services executed on behalf of corporate clients, the Company acts as a Data Processor or Subprocessor. All processing routines in these capacities are governed strictly by the executed client engagement contracts and Data Processing Agreements (DPAs).

The Company requires personnel, contractors, vendors, and subprocessors that handle information on its behalf to be subject to appropriate confidentiality, privacy, security, and incident-notification obligations. Third parties are

assessed and managed according to the nature of the services, data involved, and associated risk.

3. TECHNICAL PRIVACY REGIMES & JURISDICTIONAL COVERAGE

The Company manages data processing capabilities designed to align with international regulatory frameworks, implemented on a jurisdiction-by-jurisdiction basis where legally applicable:

- **United States:** Designed with reference to IRS Publication 4557 administrative guidance frameworks, and the Federal Trade Commission (FTC) Safeguards Rule where legally applicable to covered financial data.
- **United Kingdom:** Alignment with the UK Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).
- **European Economic Area (EEA):** Processing involving personal data subject to the EU General Data Protection Regulation (EU GDPR) is managed in accordance with applicable EU GDPR requirements, including requirements relating to international transfers.
- **Canada:** Adherence to the Personal Information Protection and Electronic Documents Act (PIPEDA) alongside provincial privacy statutes where applicable.
- **Japan:** Structured with reference to Japan — Act on the Protection of Personal Information (APPI).
- **Asia-Pacific (APAC):** Core baseline practices are modeled around applicable privacy requirements, including the Singapore Personal Data Protection Act (PDPA), with local legal requirements assessed by jurisdiction.
- **Middle East:** Operational controls are deployed to support national data protection frameworks, including the United Arab Emirates (UAE) and Kingdom of Saudi Arabia (KSA) Personal Data Protection Laws (PDPL).

4. DEFINITIONS AND DATA CLASSIFICATIONS

- **Personal Data:** Any information relating to an identified or identifiable natural person. Business contact information may constitute personal data where it relates to an identified or identifiable individual, subject to applicable law.
- **Confidential Business Information / Client Data:** Corporate financial logs, accounting general ledgers, corporate tax returns, bookkeeping spreadsheets, and operational transactional records linked explicitly to an enterprise or corporate entity.

4.1 PRIVACY PRINCIPLES

The Company processes personal data only for legitimate business, contractual, legal, security, or other lawful purposes permitted by applicable law. We apply data minimization, purpose limitation, access controls, and retention limits appropriate to the nature of the information and processing activity. Privacy and security requirements are considered when designing or materially changing systems, services, and processing activities.

5. CORE TECHNICAL CONTROLS AND OBJECTIVES

The Company maintains security controls intended to protect information against unauthorized access, alteration, disclosure, loss, and destruction. Controls are implemented according to risk, system architecture, contractual requirements, applicable law, and documented exceptions.

5.1 Data Encryption

The Company targets the use of Advanced Encryption Standard with 256-bit keys (AES-256) for data-at-rest within production environments. Data-in-transit across public networks mandates Transport Layer Security (TLS) version 1.3 or higher, where supported. Legacy cryptographic handshakes are systematically deprecated. Any required technical deviations must be formally approved by the CISO, documenting compensating controls such as network isolation or IP-whitelisting.

5.2 Identity and Access Management (MFA)

Multi-Factor Authentication (MFA) is required for user access to production, administrative, remote-access, and client-data environments. For system-to-system automated integrations where interactive MFA is technically unfeasible, authorized alternative controls are explicitly mandated, including managed identities, certificate-based authentication, scoped API keys, and periodic credential rotation under Role-Based Access Control (RBAC).

5.3 Infrastructure Security

The Company uses logical segmentation and access restrictions to help separate client-data environments. Vulnerabilities are identified through periodic assessments of relevant networks, hosts, and applications and are prioritized for remediation based on severity, exploitability, exposure, and business impact. Exceptions require documented risk acceptance, compensating controls where appropriate, ownership, and a review date.

5.4 Backup Resilience

The Company maintains backup and recovery arrangements appropriate to the relevant service and risk profile. Where applicable, these include daily and weekly immutable backups designed to support a target Recovery Point Objective (RPO) of 24 hours and Recovery Time Objective (RTO) of 48 hours. Recovery and disaster-recovery arrangements are tested periodically, including at least annually for applicable production environments.

6. DATA RETENTION, SANITIZATION, AND DISPOSAL

Data retention, legal holds, and disposal requirements are maintained in a jurisdiction-specific records-retention schedule and local corporate recordkeeping laws. When retention periods expire, personal and client data is erased utilizing validated, media-appropriate sanitization methods, including cryptographic erasure where applicable, in accordance with documented retention and disposal procedures. Data lifecycle execution remains subject to active legal holds, statutory tax audits, or active law enforcement mandates requiring temporary preservation.

7. INTERNATIONAL DATA TRANSFERS AND INDIVIDUAL RIGHTS

7.1 Transfer Safeguards

Where personal data is transferred internationally from a jurisdiction with transfer restrictions, the Company uses an applicable lawful transfer mechanism, such as an adequacy decision, Standard Contractual Clauses (SCCs), the UK International Data Transfer Agreement (IDTA), the UK Addendum, or another legally recognized mechanism. Transfer Impact Assessments and supplementary safeguards are used where required by applicable law.

7.2 Individual Privacy Rights

Data subjects may submit inquiries regarding their rights—including access, correction, deletion, objection, or restriction of processing. Requests are assessed subject to identity verification, statutory exemptions, and lawful extensions. The Company will respond within the legally applicable period, including generally one month under the UK GDPR and within applicable statutory time limits (generally 30 days for access requests) under PIPEDA, subject to any lawful extensions. Individuals may submit privacy-rights requests or complaints through the contact details in Section 9. The Company may request information necessary to verify identity and will explain any legally permitted refusal, limitation, or extension.

8. DATA INCIDENT RESPONSE AND BREACH MANAGEMENT

The Company maintains an incident-response process for suspected and confirmed security events. When a personal-data breach meets an applicable legal or contractual notification threshold, the Company will notify the relevant supervisory authority, affected individuals, clients, or other required parties within the timeframes required by applicable law or contract. Where the UK GDPR applies, notification to the UK Information Commissioner's Office will be made without undue delay and, where feasible, within 72 hours after becoming aware of a notifiable breach. When acting as a Data Processor or Subprocessor, the Company will notify the relevant Data Controller without undue delay in accordance with the applicable Data Processing Agreement.

9. GOVERNANCE, ASSURANCE, AND CONTACTS

The Company maintains records and audit evidence appropriate to demonstrate the operation of applicable security and privacy controls. This Policy is reviewed at least annually and may be updated to reflect legal, regulatory, operational, or security changes. For privacy-rights requests, privacy complaints, policy questions, or security concerns, contact the Company's designated privacy function at: **ContactUs@vantismfin.com**. Requests are handled in accordance with applicable law and the Company's internal procedures.