TrustVerify Security Policies

Magnificentech Solutions Ltd trading as TrustVerify

Review edition · 8 Nov 2026 · Proposed public edition awaiting founder approval.

Scope

These policies cover the TrustVerify website, dashboard, API, staff, work devices and supporting cloud services. Customers remain responsible for their own systems and instructions. Magnificentech Solutions Ltd trading as TrustVerify operates TrustVerify as a remote business.

Information Security Policy

We aim to protect confidentiality, integrity and availability. Our policy requires least privilege, multi-factor authentication, customer-data separation, encryption, minimal data collection and safe testing. Work devices must be kept updated, locked and protected. Important security updates are handled promptly. The founder reviews this policy annually.

Access Control Policy

Use named accounts, least privilege and multi-factor authentication. Administrator access requires multi-factor authentication. Approve access before use, remove it promptly when no longer needed and review it quarterly. Customer roles and data separation limit access to the right customer. Passwords are stored as strong one-way hashes.

Data Protection Policy

For customer verification data we act on documented customer instructions as processor; for our own account, billing and marketing data we are controller. Our policy is to minimise personal data, limit retention, protect sensitive identity data, support individual rights and assess high-risk processing. Supplier terms and international-transfer safeguards require review. Michael Omotayo is Founder and DPO. See our privacy notice for service-specific details.

Incident Response Policy

Report suspected incidents promptly. We record and assess events, contain harm, preserve evidence, recover service and review lessons. For personal-data breaches we notify affected customers without undue delay, notify the ICO within 72 hours where required, and notify individuals where high risk requires it.

Business Continuity and Backup Policy

Our policy requires recoverable backups and a rollback path for production changes. Proposed recovery objectives are subject to validation through restore exercises and do not constitute a service guarantee. We maintain version-controlled release materials and review continuity arrangements regularly.

Supplier Management Policy

Assess suppliers before sharing personal data, including security, processing locations and data-processing terms. Record acceptance dates and review important suppliers annually or after material changes. Review transfer safeguards and maintain a current sub-processor list.