Tapify Information Security Policy

Tapify is committed to safeguarding the confidentiality, integrity, and availability of data handled within its platform. This Information Security Policy establishes the practices and operational controls used to mitigate and monitor risks, aligned with Plaid's compliance requirements.

Governance & Oversight

1. Tapify operates a cloud-hosted architecture (Vercel + Supabase), ensuring physical and infrastructure security is managed by SOC 2 certified providers.
2. Internal processes define responsibilities for access control, monitoring, and auditing of sensitive operations.
3. Policies and controls are reviewed quarterly to ensure alignment with evolving compliance requirements.

Risk Identification & Mitigation

1. Data in transit is encrypted via TLS 1.2+; data at rest is encrypted with AES-256.
2. Supabase Row Level Security (RLS) ensures user- and role-based access is enforced at the database level.
3. Audit logs are maintained for database access, API activity, and payout transactions.
4. Principle of Least Privilege is applied for all access to production resources.

Monitoring & Incident Response

1. Vercel and Supabase provide system-level monitoring, error detection, and analytics.
2. Tapify's internal logging table records user actions and payout events for traceability.
3. Incidents are logged, investigated, and reported with corrective measures implemented to prevent recurrence.

Commitment

Tapify is committed to continuously improving its security posture. This policy is operationalized across the engineering and product lifecycle, ensuring data handled by Tapify remains secure and compliant with financial industry standards.