Tapify Security Policies

1. Governance

Tapify maintains a documented Information Security Policy and an operational information security program. This program is designed to identify, mitigate, and monitor information security risks across our systems, including cloud infrastructure, databases, and production services. Policies are reviewed annually and updated as needed to remain compliant with industry best practices and regulatory requirements.

2. Asset Management

Tapify uses cloud-native monitoring and endpoint management tools to maintain continuous visibility into all assets connected to corporate and production networks. We enforce inventory tracking of laptops, servers, and cloud instances. Automated discovery tools identify all endpoints, and alerts are configured for any unauthorized devices attempting to connect.

3. Vulnerability Management

Tapify conducts regular vulnerability scans against employee devices, contractor laptops, and production servers. Detected vulnerabilities are logged, prioritized, and remediated according to a defined SLA: critical issues within 24 hours, high severity within 72 hours, and medium severity within 7 days. Patching is verified via automated compliance checks.

4. Endpoint Security

Tapify enforces endpoint security across all employee and contractor machines as well as production assets. All systems are equipped with antivirus and anti-malware tools. Endpoint Detection & Response (EDR) agents are deployed for continuous monitoring. Multi-Factor Authentication (MFA) and least-privilege access are mandatory for system access. Logs are continuously monitored to detect and mitigate malicious activity.

These policies ensure Tapify maintains a strong security posture while scaling operations with partners like Plaid and Dwolla.