Vulnerability Management Policy

1. Purpose

The purpose of this policy is to establish consistent practices for the detection, assessment, and remediation of security vulnerabilities across Tapify’s systems, services, and infrastructure. This ensures that sensitive data, including financial and personal information, is protected in compliance with industry standards and Plaid requirements.

2. Scope

This policy applies to all production systems, development environments, and employee or contractor devices that connect to Tapify’s services. It covers applications deployed on Vercel, databases hosted on Supabase, and related third-party integrations.

3. Vulnerability Scanning

- Tapify uses automated tools such as GitHub Dependabot and npm audit to detect software dependencies with known vulnerabilities. - Vercel and Supabase provide managed infrastructure with ongoing vulnerability monitoring and patching. - Periodic manual reviews are conducted to ensure coverage beyond automated tools.

4. Remediation Process

Vulnerabilities are categorized by severity and remediated within the following Service Level Agreements (SLAs): - Critical severity: patched within 7 days - High severity: patched within 14 days - Medium severity: patched within 30 days - Low severity: patched as part of routine updates

5. Monitoring & Reporting

- All vulnerabilities are tracked in Tapify’s internal issue tracker. - Status of vulnerability remediation is reviewed in weekly development meetings. - Logs of scans and patching activities are retained for compliance verification.

6. Enforcement

Failure to comply with this policy may result in disciplinary action, up to and including termination of access for employees or contractors. This policy will be reviewed and updated annually or as required by changes in the threat landscape.