Tapify Asset Management Policy

Tapify maintains continuous visibility and security oversight into all network endpoints connected to our corporate and production environments. This includes both cloud-hosted infrastructure and developer endpoints (e.g., laptops and authorized devices).

1. Endpoint Discovery

- All production systems are hosted on Vercel and Supabase, providing centralized dashboards for endpoint management.
- Developer endpoints are registered and managed through Git-based workflows and environment-level access controls.
- Any new endpoint attempting access must be explicitly authorized via role-based access policies.

2. Endpoint Monitoring

- Cloud dashboards (Vercel, Supabase) are continuously monitored for endpoint activity.
- Supabase audit logs provide full visibility into queries and authentication events.
- MFA (multi-factor authentication) is required for all accounts accessing production systems.

3. Endpoint Security Controls

- Access to endpoints follows the principle of least privilege.
- Sensitive keys and secrets are managed through encrypted environment variables.
- Device-level controls include password protection and OS-level security features.

4. Continuous Visibility

- Alerts are enabled for unusual login attempts, failed queries, or suspicious API calls.
- Periodic reviews are conducted to ensure all active endpoints remain compliant.
- Any decommissioned endpoints are revoked immediately through credential rotation.

Approval and Maintenance

This Asset Management Policy is maintained by Tapify’s security and compliance lead. It will be reviewed at least annually or following any material change in our infrastructure.