Tapify – BYOD (Bring Your Own Device) Policy

Tapify does **not** allow employee or contractor personal devices (BYOD) to be used for carrying out official job responsibilities. All work must be performed using managed, secure devices that are provisioned and controlled by Tapify.

This policy ensures that production systems, customer data, and financial integrations (e.g., Supabase, Vercel, Plaid, Dwolla) are protected against unauthorized access and security risks. By prohibiting BYOD, Tapify maintains strict access control and reduces attack surface.

Enforcement:
- All work accounts and credentials are only accessible on Tapify-managed devices.
- No production or customer data may be accessed via personal devices.
- This policy is enforced via authentication checks, centralized logging, and endpoint security monitoring.