TrustBridge MVP Data Encryption Standards v1.0

Prepared by: Cybersecurity Team

Project: TrustBridge MVP

1. Purpose

This document defines the encryption standards and data protection controls for the TrustBridge MVP. The objective is to ensure confidentiality, integrity, and protection of SME business data in compliance with NDPR principles.

2. Encryption in Transit

All data transmitted between client and server must be encrypted using:

• HTTPS enforced across all environments

• TLS version 1.2 or higher

• HTTP Strict Transport Security (HSTS) enabled

This prevents interception of login credentials, transaction data, and uploaded files.

3. Encryption at Rest

All stored data must be encrypted using industry-standard encryption:

• Supabase PostgreSQL encryption (AES-256)

• Encrypted storage buckets for uploaded files

• No plaintext storage of sensitive data

This ensures that even if database access is compromised, stored data remains unreadable.

4. Password & Authentication Security

• Passwords hashed using bcrypt (managed by Supabase Auth)

• Minimum password length: 8 characters

• JWT-based session authentication

• Session expiration enforced (recommended: 1 hour)

No passwords or authentication tokens are stored in plaintext.

5. Token & API Security

• All JWT tokens must be signed with a strong server-side secret key

• Confirmation tokens must have expiration limits (72 hours)

• Tokens must be invalidated after use

This prevents token replay attacks and unauthorized access.

6. Backup & Recovery Protection

• Automated daily database backups enabled

• Restricted database access to authorized roles only

• Secure storage of backup files

Backup security ensures data availability without compromising confidentiality.

7. NDPR Alignment

• Data minimization principles applied

• Explicit user consent required for data processing

• Users may request account deletion

These controls align with Nigerian Data Protection Regulation (NDPR) standards.