Data Encryption Policy

Document ID: POL-SEC-002
Version: 3.1

1. PURPOSE

This policy defines encryption requirements for payment data protection in transit and at rest, ensuring compliance with PCI-DSS and industry standards.

2. ENCRYPTION IN TRANSIT

All payment data transmitted over networks must use TLS 1.3 or higher, strong cipher suites (AES-256-GCM), Perfect Forward Secrecy, and certificate pinning for critical connections.

3. ENCRYPTION AT REST

Payment data stored in databases must use AES-256 encryption, Hardware Security Modules (HSM) for key management, and Transparent Data Encryption (TDE).