Synthetic Users Encryption Policy

Version: 1.7

Effective Date: 11 November 2025

Owner: Security & Compliance Lead

Approved by: CTO

1. Purpose

This policy defines how Synthetic Users encrypts and protects data to ensure confidentiality, integrity, and compliance with applicable data protection regulations such as GDPR, SOC 2, and ISO 27001.

2. Scope

This policy applies to all Synthetic Users systems, applications, databases, backups, and communication channels that process, transmit, or store company or customer data.

It applies to all employees, contractors, and third parties with access to Synthetic Users infrastructure.

3. Objectives

- Ensure all sensitive data is encrypted both **in transit** and **at rest**.
- Define encryption standards and approved algorithms.
- Establish controls for encryption key management and access.

- Maintain compliance with regulatory and contractual obligations.

4. Data Classification

All data shall be classified according to sensitivity:

- **Public:** Information intended for public disclosure.
- **Internal:** Non-public business information.
- **Confidential:** Customer data, credentials, or system configurations.
- **Restricted:** Personal data, authentication secrets, and encryption keys.

Encryption requirements apply to **Confidential** and **Restricted** data classes.

5. Encryption Requirements

5.1 Data in Transit

- All communications between clients, APIs, and internal services must use **TLS 1.2 or higher**.
- Non-encrypted protocols (HTTP, FTP, etc.) are prohibited unless tunneled through secure channels (e.g., SSH, VPN).
- Certificates must be issued by trusted Certificate Authorities (CAs).

5.2 Data at Rest

- All databases, file systems, and backups must use **AES-256 encryption** or stronger.
- AWS S3, Postgres, and Render-managed services must have encryption at rest enabled by default.
- Portable devices and removable media (if used) must employ full-disk encryption.

6. Key Management

- Encryption keys are managed by **AWS Key Management Service (KMS)**.
- Keys are generated and rotated in accordance with AWS best practices.
- Access to keys is restricted to authorized personnel through **role-based access control (RBAC)**.
- Keys are never hard-coded, stored in source control, or shared over unsecured channels.
- Compromised or obsolete keys must be revoked immediately.

7. Secrets Management

- Application credentials, API tokens, and encryption keys are stored in secure vaults (e.g., **Render environment variables**, **1Password**, or **Bitwarden**).
- Sharing of passwords or credentials is strictly prohibited.
- Access logs and secret retrieval events are monitored.

8. Monitoring and Compliance

- Encryption configurations are periodically reviewed during internal audits.
- Automated scanning tools verify TLS configurations and encryption status.
- Non-compliance or deviations are remediated immediately.

9. Incident Response

In the event of a suspected or confirmed compromise of encryption keys or encrypted data:

- The Security Lead must be notified immediately.
- Incident response procedures shall be followed to revoke keys, rotate credentials, and restore encrypted systems.

---

10. Policy Review

This policy shall be reviewed **annually** or following major infrastructure, application, or compliance changes. Updates require approval by the CTO and Security & Compliance Lead.

---

11. References

- **Access Control Policy**
- **Password Management Policy**
- **Data Protection Policy**
- **Incident Response Plan**