Synthetic Users Backup & Data Immutability Policy

Version: 1.0

Effective Date: 15 February 2026

Owner: Security & Compliance Lead

Approved by: CTO

1. Purpose

This policy defines how Synthetic Users ensures the integrity, immutability, and recoverability of backup data to protect against data loss, corruption, ransomware, and unauthorized modification.

2. Scope

This policy applies to all backup systems and data stores used by Synthetic Users, including database backups, file storage, and application data.

3. Backup Architecture

Data Type	Backup Method	Storage	Immutability
Database	Managed backups (MongoDB/PostgreSQL)	AWS regional storage	Provider-managed
Files & Objects	S3 storage with versioning	AWS S3	S3 Object Lock

Application State	Infrastructure-as-code, container images	Render, container registry	Immutable container images

4. Immutability Controls

4.1 S3 Object Lock

- Backup objects stored in AWS S3 are protected using **S3 Object Lock**, which prevents objects from being deleted or overwritten for a defined retention period.
- Object Lock is configured in **compliance mode**, ensuring that no user — including administrators — can alter or delete protected objects until the retention period expires.

4.2 Versioning

- S3 bucket versioning is enabled, maintaining a complete history of all object versions.
- Deletion of versioned objects creates a delete marker without permanently removing the data.

4.3 Access Controls

- Write and delete access to backup storage is restricted to automated backup processes only.
- No individual user has permissions to delete or modify backup objects directly.
- IAM policies enforce separation of duties between backup creation and backup deletion.

5. Backup Schedule and Retention

- Database backups are performed continuously with point-in-time recovery capability.
- File backups are maintained with versioning, retaining all versions for the configured retention period.
- Backup retention follows the Data Deletion and Retention Policy, with a maximum backup retention of 90 days after data deletion.

6. Recovery Testing

- Backup restoration is tested as part of annual disaster recovery exercises per the Disaster Recovery Plan.
- Full rebuild testing validates end-to-end recoverability from immutable backups.

7. Monitoring

- Backup job completion and integrity are monitored through centralized logging.
- Failed backup jobs trigger alerts for immediate investigation.
- Any attempt to modify Object Lock configuration triggers a security alert.

8. Review

This policy is reviewed annually or when changes to backup infrastructure occur.