Synthetic Users Data Loss Prevention (DLP) Policy

Version: 1.0

Effective Date: 15 February 2026

Owner: Security & Compliance Lead

Approved by: CTO

1. Purpose

This policy defines Synthetic Users' strategy for preventing unauthorized disclosure, exfiltration, or loss of sensitive data across all corporate and production environments.

2. Scope

This policy applies to all employees, systems, applications, and data processed by Synthetic Users, including customer data, intellectual property, and corporate information.

3. DLP Strategy

Synthetic Users implements a layered DLP approach combining policy-based controls, technical safeguards, and monitoring:

1. **Access Controls** — Role-based access control (RBAC) and least-privilege principles limit data access to authorized personnel only.
2. **Encryption** — All data is encrypted in transit (TLS 1.2+) and at rest (AES-256), preventing interception or unauthorized access.

3. **Authentication** — SSO with MFA is enforced for all access to production and corporate systems, eliminating shared or weak credentials.
4. **Monitoring & Detection** — Centralized logging and audit trails track data access and movement across systems.

---

4. DLP Solutions

4.1 Corporate Environment

- **Google Workspace DLP Rules:** DLP rules are configured within Google Workspace to detect, flag, and prevent the sharing of sensitive data (e.g., credentials, personal information, confidential business data) via email, Drive, and other Workspace services.
- **Policy Enforcement:** Google Workspace DLP rules are configured to scan outbound emails and shared documents for sensitive content patterns and block or warn on policy violations.

4.2 Source Code & Development Environment

- **GitHub Secret Scanning:** Enabled across all repositories to detect accidentally committed secrets, API keys, tokens, and credentials. Alerts are routed to the security team for immediate remediation.
- **Branch Protection:** All production branches require peer review before merge, reducing the risk of sensitive data being committed to the codebase.

4.3 Infrastructure

- **Network Segmentation:** Production systems are isolated within cloud provider security boundaries (AWS Security Groups, Render network isolation).
- **Immutable Backups:** Backup data stored in S3 with Object Lock prevents unauthorized modification or deletion.
- **Data Segregation:** Customer data is logically segregated by workspace, enforced at the application level.

---

5. DLP Violation Response Procedures

When a DLP policy violation is detected, the following procedure applies:

5.1 Detection & Alerting

- Google Workspace DLP alerts and GitHub secret scanning alerts are routed to the security team.
- Centralized logging captures data access anomalies for review.

5.2 Triage & Classification

Severity	Description	Response Time
Critical	Confirmed exfiltration of customer or confidential data	Within 1 hour
High	Attempted exfiltration or exposed secret/credential	Within 4 hours
Medium	Policy violation without confirmed data loss (e.g., DLP rule trigger on internal share)	Within 24 hours
Low	Informational alert, no data at risk	Within 72 hours

5.3 Containment

- Revoke or rotate any exposed credentials immediately.
- Restrict access for the user or system involved pending investigation.
- Block the transmission channel if an active exfiltration is in progress.

5.4 Investigation & Remediation

- Determine the scope, cause, and impact of the violation.
- Document findings in the incident response log.

- Apply corrective actions (e.g., additional DLP rules, access restriction, training).

5.5 Notification

- If customer data is affected, follow the Incident Response Plan notification procedures, including GDPR 72-hour breach notification requirements where applicable.

5.6 Post-Incident Review

- Conduct a post-incident review within 5 business days.
- Update DLP rules and policies based on lessons learned.

---

6. Employee Responsibilities

- Employees must not transmit sensitive or confidential data via unauthorized channels.
- Employees must report suspected data loss incidents immediately to the security team.
- Violations of this policy may result in disciplinary action up to and including termination.

---

7. Review

This policy is reviewed annually or following any significant DLP incident.