Synthetic Users Email Security Policy

Version: 1.0

Effective Date: 15 February 2026

Owner: Security & Compliance Lead

Approved by: CTO

1. Purpose

This policy defines how Synthetic Users secures its email communications to prevent phishing, malware delivery, data exfiltration, and unauthorized information sharing.

2. Scope

This policy applies to all employees using Synthetic Users' corporate email system (Google Workspace).

3. Email Platform

Synthetic Users uses **Google Workspace** as its corporate email and collaboration platform. All email security controls are implemented through Google Workspace's built-in security features.

4. Email Security Controls

4.1 Use of External Email Services

- Employees must use their corporate Google Workspace email (@syntheticusers.com) for all internal and sensitive business communications.
- As a cloud-native, remote-first organization, public external email and messaging services are used for legitimate business purposes such as customer communication, vendor coordination, and collaboration.
- A blanket technical block on public email services is not enforced, as it would impair normal business operations without materially improving security.
- Instead, the following compensating controls are in place:
  - SSO and MFA for access to all corporate systems.
  - Role-based access control (RBAC) limiting data access to authorized personnel.
  - Google Workspace DLP rules detecting and preventing sensitive data sharing.
  - Centralized logging and monitoring of email activity.
  - Security awareness training on phishing and social engineering risks.

4.2 Attachment Scanning

Google Workspace provides built-in inbound and outbound email scanning:

- **Malware Scanning:** All email attachments are automatically scanned for viruses, malware, and malicious code by Google's threat detection systems before delivery.
- **Phishing Protection:** Advanced phishing and spoofing protection is enabled, including link scanning, sender authentication verification (SPF, DKIM, DMARC), and suspicious content warnings.
- **Encrypted Attachment Scanning:** Google Workspace scans password-protected attachments and archives where possible.
- **Quarantine:** Emails identified as malicious are quarantined and not delivered to the recipient.

4.3 Auto-Forwarding Prohibition

- Automatic email forwarding to external addresses is **disabled** at the organizational level in Google Workspace Admin settings.
- Employees may not configure email rules that forward corporate email to personal or external accounts.
- This setting is enforced via Google Workspace Admin policy and cannot be overridden by individual users.

4.4 Data Loss Prevention

- Google Workspace DLP rules are configured to detect and prevent the sharing of sensitive data via email, including credentials, personal information, and confidential business data.
- DLP violations are logged and flagged to the security team per the Data Loss Prevention Policy.

---

5. Email Authentication

Synthetic Users enforces the following email authentication standards:

- **SPF (Sender Policy Framework)** — Defines authorized mail servers for @syntheticusers.com.
- **DKIM (DomainKeys Identified Mail)** — Signs outbound emails to verify authenticity.
- **DMARC (Domain-based Message Authentication)** — Enforces policy on messages that fail SPF/DKIM checks.

---

6. Encryption

- All emails in transit are encrypted using TLS.
- Google Workspace enforces TLS for both sending and receiving where supported by the recipient's mail server.

- For highly confidential communications, employees may use Google Workspace's confidential mode (expiration, revoke access, prevent forwarding/download).

7. Employee Responsibilities

- Do not open suspicious attachments or click on unverified links.
- Report phishing attempts using Google Workspace's built-in "Report phishing" feature.
- Do not use corporate email for personal communications.
- Do not share credentials or sensitive data via email unless encrypted.

8. Review

This policy is reviewed annually or when changes to the email platform or security configuration occur.