STANDARD VENDOR ASSESSMENT

SEC-QST-2026

Sample Security Questionnaire

ORGANIZATION:	RESPONDENT:	REVIEW DATE:
Envelark Platform Architecture Team	**Daniel Kim -- Information Security**	**October 2026**

Standard Vendor Security & Technical Architecture Questionnaire Response

1. System Architecture & Email Data Handling

Q: How does Envelark process and store inbound email correspondence?

A: Envelark connects to standard IMAP/SMTP endpoints over TLS. Message metadata and headers are parsed into structured thread records for the client webmail interface.

2. Client-Side Rendering & CSS Containment

Q: How are third-party email styles and markup isolated from the host application?

A: Email HTML bodies are rendered within isolated shadow DOM or sandboxed template containers with scoped style boundaries to prevent style leakage or parent DOM mutation.

3. Cryptographic Attachment Indexing

Q: How are file attachments validated and fingerprinted?

A: Inbound attachments are hashed using SHA-256 algorithms upon reception. Fingerprints are displayed directly in the user interface to ensure document integrity.

4. API Authentication & Token Management

Q: How are developer API keys authenticated and scoped?

A: API requests use bearer authentication with Bearer elv_live_ tokens. Tokens are restricted to explicit permission scopes including mail:read, mail:send, and files:read.

SAMPLE - DEMO DATA
ENVELARK SHOWCASE - NOT REAL DATA