

Email Signature Management Software

IT Vendor Evaluation Checklist

Complete for each vendor before shortlisting. Score each section independently.

Vendor:
Evaluated by:
Date:

01 Deployment Architecture

Goal: Confirm the tool does not modify your mail flow or introduce a third-party sending dependency.

- ☐ Vendor has provided a data-flow diagram showing exactly how signatures are inserted.
- ☐ Deployment does not require MX record changes.
- ☐ Outbound email does not pass through vendor servers to receive signature (API-based insertion confirmed).
- ☐ Vendor has documented what happens to email delivery if their service goes down.
- ☐ No Exchange connectors or mail transport rules required.

Deployment model: ☐ Server-side ☐ Client-side (add-in/agent) ☐ API-based (native insertion)

Notes: _____

02 Provisioning: SSO and SCIM

Goal: Confirm user lifecycle is automated through your identity provider, with no manual provisioning required.

- ☐ Platform supports SSO (Single Sign-On).
- ☐ SSO is certified with your identity provider.
- ☐ Platform supports SCIM provisioning.
- ☐ New user accounts are provisioned automatically when created in the identity provider.
- ☐ User updates (name, title, department) sync without manual intervention.
- ☐ Deprovisioning is automatic when a user is removed from the identity provider.
- ☐ Vendor has provided a SCIM configuration guide for your IdP.

IdP certified: ☐ Okta ☐ Azure AD ☐ Google Workspace ☐ Other

Notes: _____

03 Security and Compliance

Goal: Verify the vendor's certifications and data handling practices meet your requirements.

- ☐ SOC 2 Type II attestation provided and current.
- ☐ ISO 27001 certificate provided and current.

- ☐ GDPR compliance documented (Data Processing Agreement available).
- ☐ HIPAA readiness confirmed (if applicable).
- ☐ Vendor does not read, store, or access email content to apply signatures.
- ☐ Audit logs are available and exportable.

Data residency confirmed: ☐ US ☐ EU ☐ Other

Notes: _____

04 Cross-Platform Compatibility

Goal: Confirm signatures render correctly across every email client and device.

- ☐ Outlook desktop (Windows/Mac)
- ☐ Outlook Web App (OWA)
- ☐ Gmail web and mobile (iOS/Android)
- ☐ iOS/Android native Mail apps
- ☐ Signature visible to user in the compose window.
- ☐ No duplicate signatures in reply threads.

05 Policy Enforcement and Governance

Goal: Confirm the platform enforces brand standards without ongoing IT involvement.

- ☐ Specific fields can be locked (logo, colors, fonts).
- ☐ Role-based access control (RBAC) is available.
- ☐ Admin permissions can be segmented (Marketing vs. Compliance).
- ☐ Multiple signature templates assigned by department/role.

06 Employee Self-Serve and Marketing Handoff

Goal: Empower users and Marketing to manage content without IT tickets.

- ☐ Employees can update approved fields (phone, LinkedIn).
- ☐ Marketing can update templates without HTML/code.
- ☐ Campaign banners can be launched/scheduled by Marketing.
- ☐ Analytics and click tracking are available.

07 Support and Reliability

Goal: Confirm the vendor's support model is mission-critical.

- ☐ SLA for first response confirmed in writing.

- ☐ Uptime SLA confirmed (minimum 99.9%).
- ☐ Live support channel available during business hours.
- ☐ Onboarding support/deployment runbook included.

Notes: _____

08

Red Flag Review

Mark any that apply. Any checked item is a blocker.

- ☐ Email is routed through vendor servers (mail-flow dependency).
- ☐ No SSO or SCIM support.
- ☐ Signature is not visible to users in the compose window.
- ☐ Vendor could not provide SOC 2 or ISO certifications.

Evaluation Decision: _____

IT Sign-off: _____

Date: _____