

Email Security - Schedule CS-2

Effective Date: October 14, 2025 | Supersedes prior versions.

Service Summary

Service Provider shall provide cloud-based Email Security services designed to reduce risks from spam, phishing, malware, and other malicious email content. These services leverage industry-standard filtering platforms to inspect inbound and outbound email traffic, quarantine or reject high-risk messages, and provide administrative tools for review. Email Security is intended as a protective layer, not a guarantee against all email-borne threats.

Scope of Services

- Inbound email scanning for spam, phishing attempts, malware, and known malicious links/attachments.
- Outbound scanning to prevent distribution of malware or flagged content from Client mailboxes.
- Quarantine management, including periodic automated reports of held messages.
- Allow/deny list management (sender or domain whitelisting/blacklisting) upon Client request.
- Administrative portal access for designated Client personnel.
- Integration with Microsoft 365 or other supported email platforms as mutually agreed.

Exclusions

- Responsibility for end-user actions, including clicking links, opening attachments, or overriding quarantines.
- Protection against threats delivered via channels outside of email (e.g., SMS, cloud file shares, collaboration apps).
- Phishing campaigns delivered through QR codes (“quishing”) or other emerging attack formats.
- AI-generated or highly sophisticated phishing messages designed to mimic trusted senders without containing detectable malicious payloads.
- Social engineering attacks that rely on user trust or deception rather than technical exploits.
- Remediation of compromised accounts or malware infections beyond blocking or quarantining email messages.
- Support for unsupported or legacy email systems not covered by mutual agreement.
- Any guarantees of 100% filtering accuracy; false positives and false negatives are inherent in all filtering technologies.

Client Responsibilities

- Maintain current licensing for email platforms and ensure compatibility with Service Provider’s filtering tools.
- Provide Service Provider with necessary administrative access for setup, integration, and maintenance.
- Instruct end-users on safe email practices and escalation procedures for suspected phishing or malicious messages.
- Promptly notify Service Provider of changes in email domains, user counts, or configuration requirements.

General Terms

- Email Security is provided as a best-effort protective service. No filtering system guarantees complete threat prevention.

Email Security - Schedule CS-2

- Client acknowledges that Email Security is one element of a layered security strategy. While this Service reduces risk, no single control or combination of controls can guarantee complete protection or eliminate all vulnerabilities. Even the most advanced security systems remain subject to bypass or compromise. Service Provider strongly recommends implementing complementary safeguards – such as endpoint detection and response (e.g., Adlumin XDR), multi-factor authentication, conditional access policies in Microsoft 365/Intune/Entra ID, DNS filtering, security awareness training, and ongoing monitoring – to achieve stronger overall resilience.
- All response times for service requests related to Email Security are governed by the Service Level Objectives in Schedule A of the Master Service Agreement.
- Fees for this Schedule are billed in accordance with the Payment Terms of the Master Service Agreement. Required platform licensing is included in Service Provider's standard service fees unless otherwise specified. Additional costs (e.g., optional hardware, custom configurations, or third-party integrations outside standard service) may apply and will be billed separately.