

### DNS Filtering - Schedule CS-4

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

#### Service Summary

Service Provider shall provide DNS Filtering services designed to reduce risks from malicious or inappropriate internet activity. DNS Filtering blocks access to known malicious domains, phishing sites, and other categories of restricted content before connections are established. This service provides a preventative layer at the network and endpoint level but does not guarantee complete protection against all web-based threats.

#### Scope of Services

- Deployment and management of DNS filtering agents or network-level controls on Covered Systems.
- Blocking of access to domains identified by global threat intelligence feeds as malicious or high-risk.
- Category-based filtering (e.g., adult content, gambling, known malware sites) as configured for Client policy.
- Administrative portal access for designated Client personnel.
- Reporting of blocked activity and filtering trends.
- Integration with supported devices, networks, and platforms as mutually agreed.

#### Exclusions

- Responsibility for end-user actions, including bypassing DNS filtering, connecting through VPNs, or using personal devices not under management.
- Detection or blocking of threats that do not rely on DNS resolution (e.g., direct IP connections).
- Protection against malicious activity occurring inside allowed services (e.g., links within Microsoft Teams or Slack).
- Support for unsupported or legacy systems not compatible with DNS filtering agents.
- Guarantee of 100% effectiveness; false positives and false negatives are inherent in all filtering technologies.

#### Client Responsibilities

- Ensure Covered Systems remain compatible with and properly configured for DNS filtering agents or controls.
- Notify Service Provider of policy changes, category requests, or filtering exceptions.
- Instruct end-users on safe browsing practices and escalation procedures for suspected issues.
- Promptly review and respond to Service Provider notifications regarding bypass attempts or filtering failures.

#### General Terms

- DNS Filtering is provided as a best-effort protective service. No filtering system guarantees complete threat prevention.
- Client acknowledges that DNS Filtering 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, email security filtering, security awareness training, and ongoing monitoring – to achieve stronger overall resilience.
- All response times for service requests related to DNS Filtering 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.