Service Attachment for Managed Services

Effective May 22, 2026. This Service Attachment for Managed Services supersedes and replaces all prior versions.

This Service Attachment is between Methodology IT ("Provider") and the Client identified on the applicable Order. Together with the Master Services Agreement, the Order, the Schedule of Services, the Schedule of Third-Party Services, and any other applicable Service Attachments, it forms the Agreement between the parties. Capitalized terms not defined here have the meanings given in the Master Services Agreement.

This Attachment governs Provider's delivery of managed services described in the Schedule of Services — managed endpoints, servers, network, security, Microsoft 365 / Google Workspace, backup, and Help Desk. Cloud and hosting services, compliance services, co-managed engagements, artificial intelligence services, and project services are governed by their respective Service Attachments or Statements of Work.

1. Services

Provider will deliver the services identified on the active Order at the tier identified on the Order, as described in the Schedule of Services. Additional services may be added by entering into a new Order or amending the existing Order.

2. Help Desk

Provider's Help Desk is available during the hours associated with Client's service tier as set forth in the Schedule of Services. Tickets may be submitted via Client portal, email, or telephone. After-hours support is intended for critical incidents; routine after-hours requests may be deferred to the next business day or billed per the Schedule of Services.

3. Onsite support

Provider's intent is to resolve incidents remotely whenever possible. Onsite support is provided when remote resolution is impractical (typically hardware issues, network outages, or physical configuration work). Onsite hours included by tier, applicable rates, travel charges, and minimums are set forth in the Schedule of Services.

4. Provider responsibilities

4.1 Service delivery

Provider will deliver the in-scope services in a professional and workmanlike manner consistent with industry practice and aligned to the Service Level Objectives.

4.2 Standard policies

Provider maintains and applies the following standard policies across all managed Clients. Provider may update these policies from time to time without amendment to this Attachment, provided that no update materially decreases Service functionality available to Client:

- **Patching policy.** Operating system and supported third-party application patches are deployed on a defined schedule with appropriate pilot, ring, and rollback procedures.
- **Security baseline.** A CIS-aligned baseline configuration applied to managed endpoints, servers, and Microsoft 365 / Google Workspace tenants.
- **Identity policy.** Multi-factor authentication is required for all managed Users on Provider-managed identity platforms. Conditional access and risk-based policies are applied per Provider's baseline.
- **Privileged access policy.** Provider administers managed environments using dedicated, monitored privileged accounts separate from standard User identities.
- **Documentation policy.** Managed environments are documented in Provider's documentation platform and maintained on a defined cadence.

4.3 Data security and privacy

Provider will not use, edit, or disclose to any third party any electronic data or information stored by Provider on Client's behalf or transmitted to Provider using the Services ("Client Data"), except as required to deliver the Services, comply with applicable law, or as Client otherwise directs in writing. Provider will maintain the security and integrity of Client Data under Provider's direct control in accordance with Provider's published security practices. As between Provider and Client, all Client Data is owned exclusively by Client and constitutes Confidential Information under the Master Services Agreement.

4.4 Maintenance windows

Routine server, application, and infrastructure maintenance is performed during scheduled maintenance windows. Some applications, systems, or devices may be unavailable or degraded during those windows. Provider will publish standard maintenance windows in the Service Level Objectives document and provide reasonable advance notice of any non-routine maintenance expected to cause material disruption.

5. Client responsibilities

Client agrees to the following in support of Provider's delivery of the Services:

5.1 Cooperation and access

Client will provide Provider with timely access to facilities, networks, systems, and personnel as reasonably required for Provider to deliver the Services. Client will designate a primary point of contact and a backup point of contact authorized to make decisions and authorize work.

5.2 Adoption of recommendations

Provider may from time to time make recommendations regarding security, compliance, and best practice (for example, enabling MFA, deploying conditional access, replacing end-of-life hardware, applying security baselines). If Client declines to adopt a recommendation, Client accepts responsibility for any consequences arising from the declined recommendation, including but not limited to security incidents, regulatory findings, breach-notification costs, ransomware costs, forensic investigation, restoration, and similar costs.

5.3 Restorable backup before significant changes

Prior to any significant change Provider initiates at Client's request — including installations, migrations, upgrades, or replacements — Client is responsible for verifying that a current, restorable backup of any affected system exists. Where Client has subscribed to Provider's Backup Services for the affected system, this responsibility is satisfied through those services.

5.4 Minor onsite tasks

Provider may occasionally ask Client to perform simple onsite tasks (powering down or rebooting a device, swapping a cable, etc.). Client agrees to reasonably cooperate with such requests as a condition of remote service delivery.

5.5 Network and environment changes

Client will notify Provider in writing of significant proposed changes to its network or environment — additional sites, ISP changes, firewall replacements, identity-platform changes, major application

deployments, mergers and acquisitions — and will provide Provider with reasonable opportunity to comment before the change is implemented. Significant evaluation, design, or testing required to support Client-initiated change requests is not covered by recurring Service Fees and may be quoted as Project Services.

5.6 Server changes and repairs

Server hardware repair, replacement, or significant configuration change requires Provider authorization. Client agrees not to perform server-level changes without notifying Provider.

5.7 Software media and licensing

Except for software Provider supplies in connection with the Services, Client is solely responsible for obtaining and maintaining all required software licenses, including client access licenses and any required activation media or keys, for software installed in Client's environment.

5.8 Hardware warranty maintenance

Client equipment in scope for management must be maintained under an active manufacturer warranty or equivalent maintenance contract. Provider is not responsible for failure of equipment that is out of warranty, end-of-life, or otherwise unsupported by its manufacturer. Provider may designate specific equipment as obsolete or unsupportable and exclude it from coverage on reasonable notice.

6. Minimum environment standards

Client represents and warrants that its environment meets, or will be brought into alignment with, the following minimum standards. These are baseline requirements for Provider to deliver the Services at the agreed pricing.

6.1 General

- All operating systems on managed Devices are vendor-supported (not end-of-life).
- All managed software is genuine and properly licensed.
- All managed Devices receive operating-system and security patches on Provider's standard cadence.
- A vendor-supported, currently licensed business-class firewall protects Client's network at every managed site.
- Multi-factor authentication is enabled for all managed Users on Microsoft 365, Google Workspace, VPN, and other Provider-managed identity surfaces.
- Privileged administrator accounts are separate from standard User accounts.

6.2 Healthcare clients (HIPAA-regulated)

In addition to the general standards:

- An identity-management platform (Microsoft Entra ID, Okta, Google Workspace identity, or equivalent) governs all User access.
- Access logging and audit retention align to the Service Attachment for Managed Compliance Services where Client has subscribed.

6.3 Payment-card clients (PCI-DSS)

In addition to the general standards:

- Payment-processing network is segregated from the general user network.
- Wireless networks used by payment systems are segregated from guest and general-use wireless.
- An identity-management platform governs all User access to in-scope systems.

6.4 Effect of non-compliance

All costs required to bring Client's environment up to the Minimum Environment Standards are not included in this Attachment and will be quoted as Project Services. If Client's environment falls out of alignment with these standards during the Term and is not brought back into alignment within a reasonable cure period after written notice from Provider, Provider may suspend delivery of affected Services or terminate this Attachment on five (5) business days' advance written notice.

7. Provider-supplied equipment

Where the Order specifies Provider-supplied equipment (for example, business laptops or desktops included in the Total tier, or Provider-supplied firewalls and networking gear under specific Orders), the following applies.

7.1 Rental basis

Provider-supplied equipment is delivered on a rental basis. The Monthly Service Fee for such equipment includes use of the equipment, associated software and operating systems, and labor needed to install and maintain it.

7.2 Use restrictions

Client will use Provider-supplied equipment only for its intended business purpose and only at the location identified on the Order (or for portable devices, by the User to whom they are assigned). Client will not allow anyone other than Provider to service, modify, disconnect, or relocate Provider-supplied equipment without Provider's consent (not unreasonably withheld for ordinary User

mobility). Client will back up any critical business data stored on Provider-supplied equipment using Provider's Backup Services or equivalent.

7.3 Software ownership

Software installed by Provider on Provider-supplied equipment remains the property of Provider or its licensors. Client's interest is that of a licensee for the duration of the Service Term. Upon termination, Client will cease use and, on Provider's request, return or permanently delete the affected software.

7.4 Loss or damage

Provider-supplied equipment damaged or lost outside of manufacturer warranty coverage, or beyond ordinary wear and tear, may be billed to Client at fair replacement cost.

8. User credentials

In connection with Service delivery, Provider or its Third-Party Services Providers may issue credentials allowing Client Users to access Services ("User Credentials"). User Credentials are Provider Confidential Information. Client will not share User Credentials with any third party without Provider's prior written consent and will distribute credentials only to authorized employees. Provider may require Client Users to change passwords on reasonable notice. All User Credentials expire on termination of this Attachment.

9. License and proprietary rights

9.1 License grant

Provider grants Client a non-exclusive, non-transferable right during the Term to access and use the Services specified on the Order. Services may be hosted on Provider-controlled infrastructure, Client-controlled infrastructure, or third-party infrastructure.

9.2 Reserved rights

Other than the rights expressly granted in this Attachment, no rights in or to the Services, Provider Materials, or any intellectual property of Provider or its licensors are granted to Client. Client will not:

- modify, copy, or create derivative works of the Services or Provider Materials;
- create links to, frame, or mirror Provider Materials other than for Client's internal business purposes;
- redistribute, sell, rent, lease, or otherwise make the Services or Provider Materials available to any third party;

- remove or obscure proprietary notices on Provider Materials; or
- reverse engineer, decompile, or disassemble Provider Materials, except as expressly permitted by applicable law.

"Provider Materials" means text, graphical content, methods, designs, software, hardware, source code, data, passwords, APIs, documentation, and improvements thereto used by or on behalf of Provider to deliver the Services.

9.3 No high-risk use

Client acknowledges the Services are not fault-tolerant and are not warranted to be uninterrupted or error-free. Client will not use the Services in any application where failure could lead to death, serious bodily injury, or severe physical or environmental damage. Administrative, configuration, and non-control uses (storing configuration data, engineering tools, business systems whose failure would not cause physical harm) do not constitute high-risk use. Client will indemnify Provider against third-party claims arising from Client's high-risk use of the Services.

9.4 No illegal use

Client will not use the Services for any unlawful purpose or in violation of the rights of others.

10. Third-Party Services Providers

Components of the Services are delivered through or licensed from Third-Party Services Providers. The specific Third-Party Services Providers in use as of the Effective Date are identified in the Schedule of Third-Party Services, which Provider may update from time to time. Use of those services is subject to the applicable Third-Party Services Provider terms.

Provider will be Client's first point of contact for support of in-scope third-party components. Third-party components are warranted only by the underlying Third-Party Services Provider and only as set forth in that provider's agreement. Provider makes no warranty regarding third-party components beyond what is contained in the applicable third-party agreement.

Where required by applicable third-party license terms, third-party software publishers (including Microsoft) may be intended beneficiaries of this Agreement with rights to verify compliance and enforce relevant provisions. Provider will cooperate in good faith with any reasonable compliance investigation by such publishers.

Within thirty (30) days of termination, Provider will remove, or cause to be removed, all copies of Provider-supplied software and Provider Materials from Client's Devices, or otherwise render them permanently unusable. Client will reasonably cooperate with such removal.

11. Exclusions

The following are excluded from this Attachment and recurring Service Fees, and may be delivered as Project Services or other separately quoted work:

- Major hardware or software upgrades, replacements, or migrations
- New site, server, or major network installations
- Operating-system migrations, cloud migrations, identity-platform migrations
- Office moves, data-center moves, cabling, electrical, conduit, rack space, and physical infrastructure
- Hardware repair where not covered by manufacturer warranty
- Replacement, implementation, or significant customization of line-of-business software
- Custom software development (delivered, where applicable, under the Service Attachment for Artificial Intelligence Services or a separate Statement of Work)
- End-user training beyond what is provided in connection with newly delivered Provider-supplied equipment
- Printer hardware repair
- Disputes with third-party vendors that are not technical in nature (billing disputes, contract disputes, etc.)
- Services to remote computers or home systems not specifically in scope under an Order
- Forensic investigation and breach-response work extending beyond the first twenty-four (24) hours following a security incident

Provider is also not responsible for failures to deliver Services caused by:

- expired or absent manufacturer warranty or vendor support on Client equipment;
- alterations or modifications of Client equipment made by anyone other than Provider;
- defects or malfunctions in hardware or software not caused by Provider that materially impair Service delivery;
- network changes Client made without notification to Provider;
- task reprioritization or delays initiated by Client;
- Force Majeure events;
- Client actions or inactions contrary to Provider's reasonable recommendations;
- loss of internet connectivity at Client locations;
- power outages or UPS failures;
- third-party criminal activity (including ransomware, phishing, account compromise, and similar) — Provider's role in security incident response is set forth in the Schedule of Services; remediation costs are billable separately;
- intervals between an issue first occurring and Client reporting it to Provider.

12. Warranty disclaimer

Provider warrants that the Services will be performed materially in accordance with the Schedule of Services and the Service Level Objectives in a professional and workmanlike manner. Except as expressly stated in this Attachment or the Master Services Agreement, the Services are provided "as is." Provider does not warrant that the Services will be uninterrupted, error-free, or completely secure. Internet connectivity carries inherent risk that may result in loss of privacy, confidentiality, or data. Provider's obligations regarding security are those set forth in this Attachment and the Schedule of Services and no others.

Provider makes no warranty on behalf of Third-Party Services Providers, whose warranties (if any) are governed by their respective agreements. Client acknowledges that recovery of data using Backup Services may not be error-free or completed within any specific timeframe beyond what is set forth in the Service Level Objectives.

13. Fees and term

Fees for the Services are set forth in the Schedule of Services and on the applicable Order. Term, renewal, and termination of this Attachment are governed by the Master Services Agreement. Specific exit-assistance and data-return obligations on termination are set forth in the Master Services Agreement.

Provider may update this Service Attachment with at least sixty (60) days' written notice for material changes. Non-material updates (clarifications, corrections, policy references) may be made without notice provided they do not materially decrease Service functionality.