# Service Attachment for Co-managed Services

**Effective May 22, 2026. This Service Attachment for Co-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 co-managed engagements — arrangements in which Client maintains internal information-technology personnel ("Internal IT") and Provider supplements that team with specific services, tools, and expertise identified on the Order. Co-managed engagements differ from fully managed engagements in that day-to-day operational responsibility remains with Client's Internal IT, and Provider's scope is limited to the specific functions identified on the Order.

## 1. Scope

Provider will deliver the co-managed services identified on the Order. The services available under this Attachment are described in § 2. Each Order will identify which services are included, the staffing model, the volume of in-scope users or devices, the relationship between Provider and Client's Internal IT, and any specific exclusions.

This Attachment is not a substitute for the Service Attachment for Managed Services. In a co-managed engagement, Provider does not assume general responsibility for the operation, security, availability, or compliance of Client's environment unless a specific function is explicitly named on the Order.

## 2. Services

The following are the categories of services Provider offers under this Attachment. The specific services included for Client are set forth on the Order.

### 2.1 Co-managed tooling and licensing

Provider may provide Client's Internal IT with access to Provider's tool stack — including remote monitoring and management (RMM), endpoint detection and response (EDR), DNS filtering, Microsoft 365 / Google Workspace governance, documentation, security awareness training, password management, and similar platforms — under a co-managed access model. Tools are licensed to Provider; Client's Internal IT receives operator-level access for the duration of the Service Term. Specific tools in scope are identified on the Order; vendors are identified in the Schedule of Third-Party Services.

### 2.2 Tier 2 and Tier 3 escalation

Provider will accept escalations from Client's designated Internal IT contacts for incidents and requests beyond Internal IT's resolution capability or capacity. Escalation channels, response targets, and any included escalation hours per month are defined on the Order. Service levels for escalation work follow the Service Level Objectives unless otherwise modified on the Order.

### 2.3 After-hours and overflow coverage

Provider may provide after-hours, weekend, or overflow Help Desk coverage on behalf of Client. Coverage windows, response targets, and routing rules are defined on the Order. After-hours coverage may be delivered as a fixed monthly fee, as a block-of-hours, or as time-and-materials at the rates set forth in the Schedule of Services.

### 2.4 Security operations services

Provider may extend its managed security operations to co-managed Clients, including 24×7 monitoring through Provider's third-party Managed Detection and Response (MDR) provider, identity threat detection and response, DNS security filtering, security awareness training and phishing simulation, and SIEM operations. These services may be sold independently of fully managed services and are subject to the descriptions in the Schedule of Services and the Service Attachment for Managed Services.

### 2.5 Project and professional services

Provider may deliver project work — migrations, deployments, security remediation, infrastructure projects, etc. — to co-managed Clients under separate Statements of Work governed by this Attachment and the Master Services Agreement.

### 2.6 Strategic and advisory services

Provider may serve as virtual Chief Information Officer (vCIO) or technology advisor to Client and Client's Internal IT, including regular technology business reviews, technology roadmaps, budget and procurement support, and vendor strategy. Meeting cadence is defined on the Order; typical engagements are monthly or quarterly.

### 2.7 Documentation platform access

Provider may provide Client's Internal IT with access to Provider's documentation platform, with Client's environment and procedures documented and maintained collaboratively. Access is co-extensive with the Service Term.

### 2.8 Compliance support

Provider may deliver compliance services to co-managed Clients under the Service Attachment for Managed Compliance Services. The presence of Internal IT does not change the scope or structure of compliance services, but division of responsibility for control implementation will be specified on the applicable Order.

## 3. Division of responsibility

Each Order will include a responsibility matrix identifying, for each in-scope function, which party is Responsible (does the work), Accountable (owns the outcome), Consulted, and Informed (a RACI matrix). In the absence of a specific assignment on the Order, the following defaults apply:

- **Day-to-day operations** — Internal IT
- **Tier 1 Help Desk** — Internal IT
- **Tier 2 / Tier 3 escalation** — Provider, where escalation is in scope
- **24×7 security operations and incident detection** — Provider, where security services are in scope
- **Patching and configuration policy** — joint; Provider sets policy where Provider's tools enforce it, Internal IT executes
- **Identity lifecycle (joiner / mover / leaver)** — Internal IT executes; Provider supplies tooling and audit support
- **Network management and changes** — Internal IT, with Provider available for design review and escalation
- **Vendor management** — Internal IT for vendors in Client's primary stack; Provider for Provider-supplied tooling
- **Strategic planning and budgeting** — joint; Provider advises, Client decides
- **Compliance program execution** — joint per Service Attachment for Managed Compliance Services
- **Regulatory communications, legal matters, executive reporting** — Client

# 4. Provider responsibilities

## 4.1 Service delivery

Provider will deliver the in-scope services in a professional and workmanlike manner and in alignment with the Service Level Objectives applicable to co-managed engagements.

## 4.2 Tool provisioning and access management

Provider will provision Internal IT operator accounts for the tools in scope, maintain those accounts for the duration of the Service Term, and revoke access upon termination or change in Internal IT personnel as notified by Client.

## 4.3 Communication and coordination

Provider will maintain regular communication with Client's designated technical lead per the cadence on the Order — typically a weekly or biweekly working session for operational matters and a monthly or quarterly business review for strategic matters.

## 4.4 Change management and notification

Provider will follow a documented change management process for changes Provider initiates affecting Client's in-scope systems: prior notification to Client's technical lead, documented approval, scheduled implementation, and post-change communication. Emergency changes (security incident response, critical patching) may proceed with retrospective notification.

## 4.5 Documentation

Provider will maintain Provider-side documentation of in-scope services, tooling, escalation procedures, and Client environment as relevant to Provider's delivery.

# 5. Client responsibilities

## 5.1 Internal IT capacity

Client will maintain qualified Internal IT personnel sufficient to deliver the functions assigned to Internal IT in the responsibility matrix. Sustained gaps in Internal IT capacity may, at Provider's discretion, require Provider to either expand scope through an amended Order or limit deliverables to remain within the co-managed structure.

## 5.2 Designated contacts

Client will designate a primary technical contact and a primary executive contact for the engagement. Provider will accept escalation requests, change approvals, and decisions only from

designated contacts.

### 5.3 Cooperation, information, and access

Client will provide Provider with timely access to facilities, systems, networks, and personnel reasonably required for delivery of the Services, and will share information necessary for Provider to understand Client's environment, business priorities, and operational practices.

### 5.4 Notification of changes

Client will notify Provider of changes that may materially affect Provider's delivery, including but not limited to changes in Internal IT personnel; changes to Client's network, identity platform, or major applications; new sites, acquisitions, or divestitures; and changes in regulatory exposure.

### 5.5 Notification of incidents

Client will notify Provider promptly of known or suspected security incidents, service outages, or other operational events that may require Provider's involvement under the responsibility matrix.

### 5.6 Adoption of recommendations

Where Provider makes recommendations regarding security, compliance, infrastructure, or process — particularly where in-scope tooling depends on configuration that Internal IT must execute — Client is responsible for Internal IT's adoption or rejection of those recommendations. If Internal IT declines a recommendation, Client accepts responsibility for the consequences of that decision.

### 5.7 Tool stewardship

Internal IT operators using Provider-supplied tools will use those tools in accordance with Provider's stated policies and the tool vendor's terms. Internal IT will not share Provider-issued credentials, will not configure tools in ways that materially impair Provider's monitoring, and will not extend access to third parties without Provider's consent.

## 6. Tool access, license, and ownership

Tools and platforms Provider makes available to Internal IT remain licensed to Provider. Client and Client's Internal IT receive a limited right to use those tools for the duration of the Service Term in accordance with Provider's policies and the underlying vendor's terms.

### 6.1 No sublicensing

Internal IT may not extend tool access to Client's affiliates, customers, contractors (other than properly engaged Internal IT contractors), or any third party without Provider's consent.

### 6.2 Termination

Upon termination of this Attachment, Provider will revoke Internal IT operator access to Provider-licensed tools within thirty (30) days. Where Client wishes to acquire its own direct licensing of an equivalent tool, Provider will reasonably support transition planning and, where the vendor permits, configuration export.

### 6.3 Data portability

Documentation, ticket history, monitoring history, and similar data generated during the engagement is Client Data with respect to Client's environment. On termination, Provider will provide Client a reasonable export of Client-specific data per the Master Services Agreement. Where data is held within third-party platforms whose export capabilities are limited, Provider will provide what the vendor's export tooling makes available.

## 7. Exclusions

The following are excluded from this Attachment unless explicitly added by an Order:

- General responsibility for the operation, security, availability, or compliance of Client's environment beyond the specific in-scope functions
- Day-to-day Tier 1 Help Desk operations
- Hardware procurement, repair, replacement, or lifecycle management
- Software licensing other than co-managed tooling provided under § 2.1
- Project work, migrations, and major implementations (delivered under separate Statements of Work)
- Compliance services other than as included under the Service Attachment for Managed Compliance Services
- Forensic investigation and breach-response work extending beyond the initial response support
- Custom software development
- End-user training other than security awareness training where security services are in scope

Provider is not responsible for failures to deliver Services caused by Internal IT's failure to perform functions assigned to Internal IT; Client's failure to maintain qualified Internal IT capacity; Client's failure to adopt Provider's reasonable recommendations; expired manufacturer warranty or vendor support on Client equipment; alterations or modifications made by Internal IT or others without notification to Provider; loss of internet connectivity; Force Majeure; or other causes outside Provider's reasonable control.

## 8. Data, security, and acceptable use

Client Data handled by Provider in connection with co-managed services is governed by the data security, confidentiality, and ownership terms of the Master Services Agreement. Internal IT operators using Provider-supplied tools will comply with Provider's acceptable use expectations and the underlying vendor's terms of service. Provider reserves the right to suspend tool access for operators whose use of the tools violates these expectations, with notification to Client.

## 9. Fees and term

Fees for the Services are set forth on the Order. Term, renewal, and termination of this Attachment are governed by the Master Services Agreement.

---

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