# Schedule of Services

> **Effective May 22, 2026. This Schedule of Services supersedes and replaces all prior versions.**

This Schedule of Services describes the services Methodology IT ("Provider") may deliver to Client under the Master Services Agreement. The specific services delivered to Client at any given time are defined by the active recurring service tier and any add-on services set forth on Orders, Proposals, or Statements of Work executed between Provider and Client. Capitalized terms not defined here have the meanings given in the Master Services Agreement.

This Schedule references the following Service Attachments, which are incorporated by reference and which provide additional detail for specific service families: the Service Attachment for Managed Services; Managed Compliance Services; Co-managed Services; Artificial Intelligence Services; and Cloud and Hosting Services. Use of Third-Party Services Providers is subject to the Schedule of Third-Party Services.

---

## 1. Service tiers

Provider offers three standard service tiers. Each tier is sold on a per-User, per-month basis. The tier selected on the active Order applies to all Users at the Client unless the Order specifies otherwise.

### 1.1 Core — Essential protection with business-hours support

Includes:

- Managed endpoint protection (anti-malware / EDR-lite)
- Help Desk support during business hours (8×5), Monday through Friday, 8:00 AM – 5:00 PM local time, excluding Provider holidays
- Basic email protection (anti-spam, anti-phishing)
- Monthly operating system and third-party application patching
- Quarterly IT check-in meeting
- Standard IT documentation maintained in Provider's documentation platform
- Network monitoring and management for one primary site (see § 2.3)

### 1.2 Complete — 24x7 monitoring, compliance, and AI-powered security

Includes everything in Core, plus:

- Advanced endpoint detection and response (EDR) supported by 24×7 Security Operations Center
- DNS security filtering on managed devices, on-network and off-network
- AI-assisted threat detection and managed threat hunting
- Advanced email protection with data loss prevention
- Identity threat detection and response (ITDR) for Microsoft 365 or Google Workspace identities
- Security awareness training and simulated phishing campaigns
- CIS-aligned security baseline configuration and ongoing alignment review
- Quarterly compliance reporting
- Monthly IT leadership meeting (technology business review)
- Priority response with elevated handling
- Microsoft 365 or Google Workspace tenant management (configuration, identity, governance, alerts)
- Server backup (see § 2.6.1) for up to one production server, additional servers billed per § 3
- Cloud-to-cloud backup of Microsoft 365 or Google Workspace data (see § 2.6.2)
- 4 hours of onsite support per month, non-cumulative (see § 2.7.2)

### 1.3 Total — All-inclusive IT, productivity, and managed device

Includes everything in Complete, plus:

- 24×7 unlimited remote support
- Microsoft 365 Business Premium license (per User) provisioned through Provider
- A business-class laptop or desktop with manufacturer warranty (per User), refreshed on a defined lifecycle (see § 2.1.3)
- Business VoIP phone with cloud calling service (per User)
- Monthly compliance reporting
- AI productivity and Microsoft Copilot management
- AI workflow automation review and implementation (subject to the Service Attachment for Artificial Intelligence Services)
- Full incident response planning and tabletop exercise
- 12 hours of onsite support per month, non-cumulative (see § 2.7.2)
- Device lifecycle management — procurement, deployment, refresh, and end-of-life handling for managed Devices

# 2. Service descriptions

The following descriptions define the scope of each service. Whether a particular service is included for Client at any given time depends on the active tier and any add-ons on the Order.

## 2.1 Managed endpoint services

**2.1.1 Endpoint monitoring and management.** Provider will deploy remote monitoring and management ("RMM") software to managed endpoints (desktops, laptops, tablets where supported). Provider will monitor endpoint health, performance, and security signals; prioritize and respond to alerts; perform remote remediation; apply operating system and third-party application patches according to Provider's standard patching policy; and provide periodic reporting.

**2.1.2 Endpoint protection.** Provider will install, configure, and manage endpoint protection software on managed endpoints. The specific product is determined by Provider and identified in the Schedule of Third-Party Services. Provider will tune detection policies, respond to detections, and maintain agent health.

**2.1.3 Device lifecycle management (Total tier).** For Clients on the Total tier, Provider will procure, configure, deploy, and refresh business-class endpoints on a 4-year refresh cycle per User. Devices remain the property of Provider unless an Order specifies otherwise. Damaged or lost Devices outside of warranty coverage may be billed to Client.

**2.1.4 Mobile device management.** Where Client uses Microsoft Intune, Jamf, or another supported MDM platform, Provider will configure and maintain device compliance policies, application deployment, and conditional access integration. MDM platform licensing is separate.

## 2.2 Managed server services

Server management is billed per managed Server as a separate line item (see § 3). Provider may, at its discretion, discount or waive the per-Server fee based on the overall scope and value of the engagement.

**2.2.1 Server monitoring and management.** Provider will monitor managed Servers (physical or virtual) for health, performance, capacity, and security signals; prioritize and respond to alerts; perform remote remediation; apply operating system and supported application patches; perform periodic configuration backups; and provide periodic reporting and performance tuning.

**2.2.2 Out of scope (Server).** The per-Server fee does not include: major hardware or software upgrades; operating system migrations; new server installations; hardware repair or replacement; or work outside of Provider's standard patching and management policies. These are delivered as project work and quoted separately.

## 2.3 Managed network services

Network management is included in all service tiers for one primary site, covering up to one (1) firewall, four (4) network switches, and eight (8) wireless access points. Additional sites and devices in excess of the included counts are billed as line items per § 3.

**2.3.1 Network monitoring.** Provider will monitor managed network Devices for availability, performance, and security signals; respond to alerts; and provide periodic reporting.

**2.3.2 Network management.** Provider will configure and maintain firewall policies, switch configurations, and wireless network configurations; apply firmware updates when applicable; make configuration changes as needed; and maintain network documentation.

**2.3.3 Firewall security services.** Where the Client's firewall supports them, Provider will configure and maintain: intrusion prevention; URL filtering; gateway antivirus; application control; geographic filtering; and other unified threat management capabilities supported by the device.

**2.3.4 Internet circuits and ISP coordination.** Provider does not provide internet connectivity. Provider will coordinate with Client's ISP on Client's behalf for incident triage and basic provisioning support; ISP contracts and billing remain Client's responsibility.

**2.3.5 Network discovery.** Provider will periodically generate a topology map of devices on Client's managed network.

## 2.4 Managed security services

The security services described in this section are included in Complete and Total tiers; certain components may be available to Core tier Clients as add-ons. The specific tools used to deliver these services are identified in the Schedule of Third-Party Services.

**2.4.1 Endpoint detection and response with managed SOC.** Provider engages a third-party Managed Detection and Response ("MDR") provider that operates a 24×7 Security Operations Center. The MDR provider monitors endpoint telemetry, performs threat hunting, isolates compromised endpoints, and escalates verified incidents to Provider.

**2.4.2 Identity threat detection and response (ITDR).** Provider monitors Microsoft 365 or Google Workspace identity activity for indicators of compromise (impossible-travel logins, suspicious mailbox rules, OAuth grant anomalies, privileged action abuse) and responds to verified incidents.

**2.4.3 DNS security filtering.** Provider deploys client-side DNS filtering on managed endpoints to detect and block requests to known malicious domains, on-network and off-network. Category-based content filtering is available on request.

**2.4.4 Email security.** Provider configures advanced email protection above the native protections of Client's email platform, including anti-spam, anti-phishing, impersonation detection, malicious link rewriting, and data loss prevention scanning for outbound mail.

**2.4.5 Security awareness training and phishing simulation.** Provider assigns an appropriate number of training licenses for Client Users, schedules ongoing training campaigns, and runs simulated phishing campaigns at randomized intervals. Per-User completion is tracked and reported.

**2.4.6 Multi-factor authentication and single sign-on.** Provider will configure MFA for compatible applications and, where applicable, single sign-on integrations. Provider will work with Client to define and document MFA and identity policies aligned to current best practices.

**2.4.7 Security log management and SIEM.** Where in-scope under the Order or the Service Attachment for Managed Compliance Services, Provider will deploy SIEM data collection across managed Devices and configure log retention. Provider will analyze and prioritize log entries, respond to events requiring action, and maintain retention aligned to applicable compliance requirements.

**2.4.8 Vulnerability and risk assessment.** Provider will periodically scan managed Devices and the managed network for vulnerabilities, review configuration against the CIS baseline, and review practices related to personally identifiable information (PII). Findings are summarized in a Risk Assessment Report.

**2.4.9 Incident response.** Provider will assist Client in the hours immediately following a confirmed security incident — identifying likely source, performing initial containment, and beginning to formulate a response. Detailed forensic investigation, breach-notification planning, and post-incident remediation projects extending beyond twenty-four (24) hours are scoped and billed separately under Project Services.

## 2.5 Managed Microsoft 365 and Google Workspace services

Tenant management is included in Complete and Total tiers. Licensing is sold separately unless specifically included (Total tier includes Microsoft 365 Business Premium for each User).

**2.5.1 Tenant configuration and governance.** Provider will configure and maintain tenant-level settings, security defaults, conditional access policies, mailbox and SharePoint governance, retention, and audit logging in alignment with Provider's standard baseline and any applicable compliance framework.

**2.5.2 Identity lifecycle.** Provider will provision and deprovision Users in alignment with Client's joiner/mover/leaver process, manage group memberships, and maintain license assignments. Standard onboarding and offboarding workflows are included; non-standard requests are handled as Help Desk tickets.

**2.5.3 License management and procurement.** Provider will sell Client's Microsoft and Google licensing through Provider's distribution relationships at published rates. Licensing is invoiced monthly and is subject to the underlying vendor's terms.

**2.5.4 Microsoft Copilot and AI productivity (Total tier).** Provider will manage Copilot licensing, governance, data exposure policies, and User enablement. Additional AI workflow automation is delivered under the Service Attachment for Artificial Intelligence Services.

## 2.6 Managed backup and disaster recovery

**2.6.1 Server backup.** Server backup is included for one (1) production Server on Complete and Total tiers. Additional Servers and Core-tier Server backup are billed per § 3. Backups are taken on a schedule defined in the Order, stored locally on Client-owned hardware where applicable, and replicated to a Provider-designated cloud destination. Provider will monitor backup job status daily, notify Client of failures, and work with the underlying Third-Party Services Provider to resolve failures. Retention defaults to one (1) year unless otherwise specified on the Order.

**2.6.2 Microsoft 365 / Google Workspace cloud-to-cloud backup.** Cloud-to-cloud SaaS data backup of Microsoft 365 or Google Workspace data (mailboxes, OneDrive / Drive, SharePoint / shared drives, and where supported, Teams / chats) is included on Complete and Total tiers and is available as an optional add-on on Core. Provider will monitor backup health, perform requested restores, and maintain default retention of one (1) year unless extended retention is purchased.

**2.6.3 Endpoint backup (optional add-on).** Endpoint backup is not bundled into any tier. For most Clients, Microsoft 365 / Google Workspace cloud sync and OneDrive / Drive Known Folder redirection sufficiently protect User data on endpoints. Where Client's workflows require local-data backup (offline-heavy applications, large media files, etc.), endpoint backup is sold as an add-on per § 3.

**2.6.4 Disaster recovery planning.** Provider will work with Client to develop and maintain a written disaster-recovery plan that incorporates the backup services in scope. The plan is reviewed at least annually. Disaster declaration and major recovery operations may exceed the scope of routine backup services and may be quoted separately if significant out-of-band effort is required.

**2.6.5 Restore testing.** Provider will perform a documented restore test at least annually for in-scope backup services and provide the results to Client.

## 2.7 Help desk and onsite support

**2.7.1 Remote support.** Provider provides Help Desk support via Client portal, email, and telephone. Support hours and inclusions vary by tier:

- **Core:** 8×5 business hours (Mon–Fri, 8:00 AM – 5:00 PM local time, excluding Provider holidays). Remote support is included.
- **Complete:** 8×5 business hours for routine support. After-hours support is available for security incidents at no additional charge; non-emergency after-hours work may be billed.
- **Total:** 24×7 unlimited remote support.

**2.7.2 Onsite support.** Onsite support is provided during normal business hours at the Client's primary site. Travel beyond thirty (30) miles from the nearest Provider office or designated technician is billed at $0.85 per mile.

| TIER | ONSITE INCLUDED PER MONTH | HOURLY RATE BEYOND INCLUDED | MINIMUM |
|---|---|---|---|
| Core | None — remote first | $225/hour | 2 hours |
| Complete | 4 hours, non-cumulative | $225/hour | 2 hours |
| Total | 12 hours, non-cumulative | $175/hour (discounted) | 2 hours |

After-hours non-emergency work is billed at $300/hour. Declared security incident response extending beyond the first twenty-four (24) hours is billed at $375/hour. Project labor is billed at $225/hour (standard) or $275/hour (senior engineer / architect) per the applicable Statement of Work.

Included onsite hours are non-cumulative — unused hours do not bank into future months. Sustained excess use beyond the included allowance may, at Provider's discretion, prompt a tier-upgrade conversation rather than per-hour billing.

**2.7.3 Response targets.** Response targets and service levels are defined in the Service Level Objectives document.

## 2.8 Vendor and third-party application management

Provider will act as Client's first point of contact for incidents involving in-scope third-party applications and services (line-of-business applications, telephony, ISPs, printer fleets, etc.). Provider will open, manage, and close tickets with these vendors on Client's behalf. Vendor contracts, billing, and ultimate service ownership remain with Client unless explicitly assumed by Provider in an Order.

## 2.9 IT leadership and strategic services

**2.9.1 Quarterly IT check-in (Core).** Provider will meet with Client quarterly to review service performance, open items, and upcoming priorities.

**2.9.2 Monthly IT leadership meeting (Complete and Total).** Provider will meet with Client monthly to deliver a technology business review including service performance, security and compliance posture, project status, budget tracking, and strategic recommendations.

**2.9.3 Annual technology planning.** Once per year, Provider will conduct a structured technology planning session covering hardware lifecycle, software lifecycle, security roadmap, compliance roadmap, and budget recommendations.

### 2.10 Documentation

Provider will maintain documentation of Client's environment in Provider's documentation platform, covering devices, network, identities, third-party services, vendor contacts, and operational procedures. Documentation is the property of Provider; at termination, Provider will provide Client with a reasonable export of Client-specific documentation per the Master Services Agreement.

---

## 3. Add-ons and line items

The following services are sold as add-ons in addition to the per-User tier pricing. Pricing is published on Provider's then-current rate sheet; Provider may discount or waive any line item at its discretion based on the overall scope and value of the engagement.

| ADD-ON | BILLING BASIS |
|---|---|
| Managed Server (physical or virtual) | Per Server, per month |
| Additional firewall (beyond one included) | Per device, per month |
| Additional network switch (beyond four included) | Per device, per month |
| Additional wireless access point (beyond eight included) | Per device, per month |
| Additional managed site | Per site, per month |
| Cloud desktop (Azure Virtual Desktop / hosted desktop) | Per User or per session host, per month — see Service Attachment for Cloud and Hosting Services |
| Endpoint backup | Per Device, per month |
| Onsite support beyond included | Per hour, plus travel beyond thirty (30) miles |
| Microsoft / Google licensing | Per license, per month |
| Project services | Fixed-fee or time-and-materials per Statement of Work |
| Artificial intelligence services | Per Service Attachment for Artificial Intelligence Services |
| Managed compliance services (HIPAA, SOC 2, PCI, CMMC, etc.) | Per Service Attachment for Managed Compliance Services |
| Co-managed services | Per Service Attachment for Co-managed Services |
| Verkada physical security (cameras, access, intercom) | Per device or per quote |

## 4. Service availability and prerequisites

Provider's ability to deliver the services described in this Schedule depends on Client maintaining the following:

- Active, supported versions of operating systems and managed applications

- Active manufacturer warranties or active support contracts on managed hardware where applicable
- Reasonable internet connectivity at managed sites
- Cooperation with Provider's standard policies for patching, MFA, identity management, and security baselines
- Timely access to facilities, networks, and systems as needed for delivery

Provider's pricing assumes Client environments are at a baseline state of currency. Significant remediation required to bring an environment to the baseline state is scoped and billed as Project Services and is not included in recurring service fees.

## 5. Out of scope

Except where explicitly included in this Schedule, an Order, or a Service Attachment, the following are not included in recurring service fees and are quoted separately:

- Major hardware or software upgrades, replacements, or migrations
- Operating system, platform, or cloud migrations
- New server, network, or site installations
- Data center moves, office moves, and physical infrastructure work
- Cabling, electrical, conduit, rack space, and similar physical infrastructure
- Forensic investigation and breach-response work extending beyond the first twenty-four (24) hours following a security incident
- Custom software development outside of AI workflow automation under the Service Attachment for Artificial Intelligence Services
- Hardware repair, where not covered by manufacturer warranty
- Third-party software or service costs not specifically included in a tier

These Service Descriptions may be revised by Provider with reasonable notice. Material changes will be communicated to Client at least sixty (60) days before they take effect.