Service Level Objectives

Effective May 22, 2026. These Service Level Objectives supersede and replace all prior versions.

These Service Level Objectives ("SLOs") are between Methodology IT ("Provider") and the Client identified on the applicable Order. Together with the Master Services Agreement, the Order, the Schedule of Services, and the applicable Service Attachments, this document forms part of the Agreement.

These SLOs describe Provider's target levels of responsiveness for incidents and requests, the priority framework used to triage work, escalation paths, standard maintenance windows, and measurement methodology. **Targets stated in this document are objectives Provider commits to use commercially reasonable efforts to meet. Targets are not guarantees and do not give rise to service credits or monetary remedies unless explicitly set forth on an Order.** Where Client requires guaranteed service levels with financial remedies, Client may request a custom SLA which, if mutually agreed, will be attached to the Order.

1. Definitions

- **Business hours.** Monday through Friday, 8:00 AM to 5:00 PM Pacific Time, excluding Provider holidays. Provider holidays are published on Provider's website and updated annually.
- **24×7 hours.** All hours, all days. Applies to Clients on the Total tier and to Provider's Security Operations Center monitoring for Clients on the Complete tier and above.
- **Incident.** An unplanned interruption or degradation of service.
- **Request.** A planned activity initiated by Client — new User provisioning, software install, configuration change, scheduled maintenance, advisory question, etc.
- **Response.** Provider's first substantive engagement with the ticket — acknowledgment, classification, triage, initial diagnosis, or beginning of remediation. Response is **not** a final resolution.
- **Update.** A status communication to Client during the lifecycle of an in-progress incident or request.
- **Resolution.** Restoration of normal service operation, or delivery of the requested change, or acceptance of a workaround by Client.

2. Priority framework

Provider triages all tickets into one of four priority levels based on business impact at the time the ticket is opened. Priority is set by Provider at intake based on the facts presented and may be re-prioritized upward or downward as the situation evolves.

PRIORITY	DEFINITION	EXAMPLE
P1 — Critical	Service unavailable for all Users; major security incident in progress; business operations stopped	Server down affecting all Users; ransomware detected; M365 tenant-wide outage; site internet down with no failover
P2 — High	Significant degradation affecting many Users or a business-critical function	Email delivery failing; major application down for one department; firewall down with backup available; widespread login failures
P3 — Normal	Limited degradation affecting some Users or non-critical functions; business process can continue	Single application slow; individual User unable to access a specific resource; printer issues for a workgroup
P4 — Low	Single User impact or non-urgent request; routine change or question	One User's password reset; software install request; how-to question; non-urgent configuration request

3. Response targets

Response targets vary by service tier (as defined in the Schedule of Services) and priority. Targets are measured from the time the ticket is opened in Provider's ticket-tracking system.

3.1 Core tier (business hours 8x5)

PRIORITY	RESPONSE TARGET	UPDATE CADENCE DURING INCIDENT
P1 — Critical	Within 1 business hour	Every 1 hour until resolved
P2 — High	Within 2 business hours	Every 2 hours until resolved
P3 — Normal	Within 4 business hours	Daily until resolved
P4 — Low	Within 1 business day	At resolution

3.2 Complete tier (business hours 8x5 for routine; 24x7 security monitoring)

PRIORITY	RESPONSE TARGET	UPDATE CADENCE DURING INCIDENT
P1 — Critical	Within 30 minutes (during business hours); within 1 hour (after hours)	Every 1 hour until resolved
P2 — High	Within 1 business hour	Every 2 hours until resolved
P3 — Normal	Within 3 business hours	Daily until resolved
P4 — Low	Within 1 business day	At resolution

3.3 Total tier (24x7 unlimited remote support)

PRIORITY	RESPONSE TARGET	UPDATE CADENCE DURING INCIDENT
P1 — Critical	Within 15 minutes, 24×7	Every 30 minutes until resolved
P2 — High	Within 30 minutes, 24×7	Every 1 hour until resolved
P3 — Normal	Within 2 business hours	Daily until resolved
P4 — Low	Within 1 business day	At resolution

3.4 Resolution

Resolution times depend on the nature of the issue, dependencies on third parties (hardware vendors, software vendors, ISPs, etc.), the availability of Client personnel and resources, and the complexity of the underlying cause. Provider commits to commercially reasonable efforts to resolve incidents promptly and to keep Client informed throughout. **Provider does not commit to fixed resolution time targets** except where expressly set forth on an Order.

4. Security incident response

Confirmed security incidents — including detected malware, ransomware, account compromise, data exfiltration, and similar — are triaged at P1 regardless of the size of the affected population, and are escalated to Provider's Security Operations Center and, where Provider's Managed Security Services are in scope, to the third-party MDR provider.

The initial response to a confirmed security incident follows the Incident Response procedure described in the Schedule of Services and the applicable Service Attachments. Detailed forensic investigation, regulatory notification support, and extended remediation extending beyond the first twenty-four (24) hours are scoped and billed separately.

5. Escalation

If Client believes a ticket is not progressing appropriately, the following escalation path is available.

1. **Within the ticket** — note the concern on the ticket and request escalation. The assigned engineer's manager will review within one (1) business day.
2. **Account-level escalation** — contact Client's designated Account Manager or technology business reviewer. The Account Manager will engage Operations management within one (1) business day.
3. **Executive escalation** — contact Provider's Chief Operating Officer or designated executive sponsor at the email address published on Provider's support portal. Executive escalation is reserved for issues unresolved at the prior escalation levels or for matters requiring leadership attention.

Escalation does not waive the ordinary triage process or guarantee re-prioritization, but it ensures the concern is reviewed by an appropriate level of management.

6. Maintenance windows

Provider performs routine maintenance during the following standard maintenance windows. Maintenance during these windows may cause brief service degradation or unavailability and does not count as an SLO miss.

WINDOW	SCHEDULE
Standard infrastructure maintenance	Saturday 10:00 PM – Sunday 4:00 AM Pacific Time
Endpoint patching	Per the Patching Policy published with the Service Attachment for Managed Services; typically the second and fourth Tuesday-through-Wednesday window monthly
Microsoft 365 and cloud platform maintenance	As scheduled by the underlying vendor; Provider does not control these windows
Emergency maintenance	As required to address security incidents or critical defects; communicated to Client with as much advance notice as conditions permit

Where Client requires advance notice of all maintenance affecting specific systems, Client may request a custom maintenance-notification policy on the Order.

7. Measurement methodology

7.1 Source of record

The source of record for ticket times, response times, update cadence, and resolution is Provider's PSA ticket-tracking system. Times not recorded in the PSA are not measurable for SLO purposes.

7.2 Clock start and stop

The response clock starts when the ticket is opened in the PSA. The clock stops upon Provider's first substantive engagement with the ticket. "Substantive engagement" excludes auto-acknowledgments and triage-only touches that do not advance the ticket.

The update clock starts at response and runs for the duration of the active incident. The update clock pauses while the ticket is in a "Waiting on Client" state (awaiting client information, decision, or access).

7.3 Excluded time

The following time is excluded from SLO measurement:

- Time the ticket is in a Waiting on Client state
- Time the ticket is in a Waiting on Vendor state (awaiting response from a third-party software, hardware, or service vendor)

- Time the ticket is in a Scheduled state (where the work is scheduled for a future date by mutual agreement)
- Standard maintenance windows
- Force Majeure events
- Time during which Client's environment is in a state that does not meet the Minimum Environment Standards in the Service Attachment for Managed Services

7.4 Reporting

For Clients on Complete and Total tiers, Provider includes SLO performance in the regular technology business review (monthly for Total, quarterly for Complete). Reports include average and 90th-percentile response times by priority, maintenance executed, and any incidents Provider believes fell short of objectives with a brief root-cause note.

8. Exclusions

These SLOs do not apply to the extent any of the following conditions exist:

- **After-hours requests on Core tier.** P3 and P4 requests submitted outside business hours are subject to business-hours response targets measured from the next business day.
- **Out-of-scope work.** Requests for services not in scope under Client's Order are subject to standard triage but not to SLO targets.
- **Non-compliant environments.** Where Client's environment does not meet the Minimum Environment Standards in the Service Attachment for Managed Services, SLOs may be suspended for affected services on reasonable notice from Provider.
- **Client delay.** Time spent waiting on Client decisions, access, information, or hardware is excluded from SLO measurement.
- **Third-party dependency.** Time spent waiting on third-party vendors not under Provider's control is excluded from SLO measurement, though Provider will continue to drive resolution.
- **Force Majeure.** Events beyond Provider's reasonable control.
- **Project work.** SLOs apply to incidents and routine requests, not to Project Services, which are governed by project plans, milestones, and Statements of Work.
- **Initial onboarding period.** During the first thirty (30) days of a new engagement (or longer if specified on the Order), Provider's SLO targets apply on a best-efforts basis as Provider builds environmental knowledge.

9. Remedies

Failure to meet these SLOs is not a breach of the Agreement and does not, by itself, give rise to a refund, credit, termination right, or other monetary remedy. The remedies available to Client for unsatisfactory service performance are those set forth in the Master Services Agreement, including the right to terminate for cause for material breach following Provider's failure to cure within the cure period.

Where Client requires service-level commitments with monetary remedies (service credits, refunds, or similar), Client may request a custom Service Level Agreement, which if mutually agreed will be attached to the Order and will supersede this document for the services it covers.

Provider may update these Service Level Objectives 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.