

# SERVICE SCHEDULE

**AUZA IT Services and Consultancy Inc.**

**Service Level Agreement – Managed Services and Security Operations**

**Document Version: 1.1**

**Last Updated: 01 January 2026**

## 1. Purpose

This Service Schedule outlines the specific services, service components, and operational parameters applicable to a particular engagement with AUZA IT Services and Consulting Inc. (“AUZA”).

The Service Schedule provides structured detail on how services are delivered, including service descriptions, service boundaries, applicable dependencies, assumptions, and any service-specific conditions agreed between AUZA and the Client.

## 2. Relationship to Other Agreements

This Service Schedule forms part of, and is governed by, the applicable Master Service Agreement (“MSA”) between AUZA and the Client.

Where applicable, this Service Schedule also operates in conjunction with the Service Level Agreement (“SLA”).

In the event of a conflict, the following order of precedence applies:

1. This Service Schedule
2. Applicable Service Level Agreement
3. Master Service Agreement

## 3. Scope of Services

This Service Schedule applies only to the services expressly identified within it. The scope of services may include, as applicable:

- Managed Security Operations Center (SOC) services
- Managed Security Service Provider (MSSP) services

- Managed IT services
- Cybersecurity consulting and advisory services
- Incident response support
- Platform management or monitoring services

Services not expressly included in this Service Schedule are excluded from the scope of the engagement.

## 4. Service Description and Components

This section defines the specific service components applicable to the engagement, which may include:

- Covered service types and tiers
- Monitored systems, assets, or environments
- Included service activities and deliverables
- Reporting and communication mechanisms

Detailed service descriptions may be further refined in appendices to this Service Schedule, where applicable.

## 5. Service Boundaries and Exclusions

This Service Schedule defines the operational boundaries of the services provided. Unless expressly stated otherwise, services exclude:

- Hands-on remediation or system changes
- Management of client-owned infrastructure
- Services outside agreed operating hours
- Support for unsupported or unmanaged technologies

Any exclusions or limitations specific to the engagement shall be documented in this Service Schedule or an associated appendix.

## 6. Dependencies and Assumptions

Service delivery under this Service Schedule may be dependent on:

- Availability and quality of required telemetry, logs, or data sources
- Client-provided access, credentials, and approvals
- Third-party tools, platforms, or services

AUZA's service commitments are based on the assumption that such dependencies are met and maintained throughout the engagement.

## 7. Service Levels (If Applicable)

Where services are subject to service level commitments, the applicable Service Level Agreement governs performance standards, response targets, and escalation procedures. Only services expressly designated as covered under the SLA are subject to service level commitments

## 8. Change Management

Changes to the services defined in this Service Schedule, including additions, removals, or modifications, must be agreed in writing by the Parties.

Approved changes may result in updates to scope, fees, service levels, or delivery timelines and may be documented through a revised Service Schedule or formal change order.

## 9. Term and Applicability

This Service Schedule becomes effective on the date specified in the applicable engagement documentation and remains in effect for the duration of the services described herein, unless terminated in accordance with the MSA.

Termination or expiration of this Service Schedule does not affect other active service schedules unless expressly stated.

## 10. Availability of the Service Schedule

The official and current version of this Service Schedule is made available in PDF format through a secure download mechanism, ensuring controlled access and clarity regarding the service configuration applicable to the engagement.