M365 Security Advisory Service

(For use with 360 Visibility Service Order)

This Service Schedule describes the M365 Strategic Advisory Service and must be read in conjunction with:

- The executed Service Order between Customer and 360 Visibility
- 360 Visibility Service Level Agreement (SLA) Schedule available at: https://www.360visibility.com/terms-and-conditions/#360-visibility-service-level-agreement-sla-schedule

In the event of conflict between this Schedule and the Service Order, the Service Order shall govern with respect to term, pricing, renewal, and general commercial terms.

1. Service Overview

The M365 Strategic Advisory Service (the "Service") provides the Customer with recurring expert oversight of their Microsoft 365 cloud environment. 360 will act as a strategic partner, performing regular technical audits and providing actionable intelligence to improve security posture, ensure compliance, and maximize the value of the Customer's Microsoft licensing.

2. Technical Audit & Review Scope

360 will perform a recurring technical audit of the following Microsoft security pillars within the Customer's tenant:

- Identity & Access (Entra ID): Review of Conditional Access (CA) policies, Multi-Factor Authentication (MFA) gaps, stale account/device cleanup, and Privileged Identity Management (PIM) hygiene.
- Endpoint Security (Intune & MDE): Review of Microsoft Defender for Endpoint health status and Microsoft Intune compliance/configuration policies for Windows and mobile platforms.
- Collaboration & Content (MDO & Purview): Audit of Microsoft Defender for Office 365 (anti-phishing, safe attachments, and safe links) and review of Microsoft Purview data loss prevention (DLP) alerts. Additionally, 360 will perform a Teams Governance review including:
    - External Sharing Policies: Audit of guest access settings, external collaboration controls, and meeting/chat policies with unmanaged users
    - Team Lifecycle Management: Identification of abandoned or stale Teams, orphaned Teams without owners, and enforcement of naming conventions
    - Compliance & Retention: Review of retention policies applied to Teams conversations and files, including holds for legal/compliance purposes
    - Teams Sprawl Assessment: Analysis of team proliferation patterns, duplicate teams, and recommendations for consolidation or archival

- SaaS & Cloud Apps (MDA): Review of Microsoft Defender for Cloud Apps to identify anomalous user behavior, "shadow IT," or unsanctioned application usage.
- Hybrid Identity (MDI): Review of Microsoft Defender for Identity health and alerts. This includes monitoring for on-premises lateral movement detection, sensitive group membership changes, and Domain Controller sensor health.
- Security Operations (Sentinel): Oversight of the Microsoft Sentinel workspace focusing on "Free Tier" data connectors. This includes health monitoring of data ingestion for:
    - Azure Activity Logs
    - Office 365 Audit Logs (SharePoint, Exchange, and Teams)
    - Microsoft Defender for Cloud Apps alerts

3. Deliverables & Consultation

For each service cycle, 360 will provide:

Monthly Deliverables:

- Prioritized Executive Report: A consolidated summary of security gaps, misconfigurations, and vulnerabilities, categorized by risk level (Critical, High, Medium, Low), delivered within 5 business days of the audit completion.
- Secure Score Trending Dashboard: Month-over-month tracking of Microsoft Secure Score across the four pillars: Identity, Device, Data, and Apps, with variance analysis highlighting improvements and regressions.
- Platform Roadmap Briefing: Guidance on upcoming Microsoft 365 feature releases, deprecated settings, or licensing changes relevant to the Customer's business.

Advisory Consultation:

- A 60-minute scheduled meeting with Customer stakeholders to review findings, discuss strategic direction, and prioritize remediation.
- Meeting Cadence: Monthly or Quarterly, based on Customer's operational availability and preference. Meetings will be scheduled at least 10 business days in advance.
- Note: Reports are delivered monthly regardless of meeting frequency. If meetings occur quarterly, the quarterly session will review the consolidated findings from the preceding three months.

4. Performance Measurement & Progress Tracking

Baseline & Benchmarking:

Upon service commencement, 360 will document the Customer's initial Microsoft Secure Score across all four security pillars (Identity, Device, Data, Apps) to establish a performance baseline.

Each monthly report will include:

- Current Secure Score (total and per-pillar breakdown)

- Month-over-Month Variance: Percentage change with identification of specific actions that improved or degraded the score
- Recommended Actions Queue: Top 5 prioritized Secure Score improvement actions ranked by impact-to-effort ratio
- Implementation Tracking: Status of previously recommended actions (Completed / In Progress / Not Started / Deferred)

Accountability Framework:

While 360 provides expert recommendations, the Customer retains final authority and responsibility for approving and implementing configuration changes. 360 will track recommendation adoption rates to help demonstrate value and identify implementation barriers during advisory consultations.

5. Remediation & Implementation

360 will provide technical guidance and "best practice" documentation for the Customer's internal IT team to implement recommended changes.

Initial Setup: As a one-time value-add, 360 will perform the initial activation of the Microsoft Sentinel workspace and connect the standard "Free Tier" Microsoft data connectors.

Note: Configuration of custom data connectors, logic apps, or complex KQL workbooks remains out-of-scope and is considered Project Work.

Minor Adjustments: At 360's discretion, "Minor Tasks" (defined as configuration changes requiring less than 30 minutes of effort) may be implemented by 360 during or immediately following the advisory session at no additional charge.

Out-of-Scope (Project Work): Major remediations, tenant-to-tenant migrations, or the initial deployment of previously unconfigured services are out-of-scope and require a separate Statement of Work (SOW).

6. Customer Responsibilities & Access

Administrative Access: Customer must maintain 360's Granular Delegated Admin Privileges (GDAP) with the necessary roles (e.g., Security Reader, Global Reader, or Intune Administrator) to perform audits.

Final Authority: While 360 provides expert recommendations, the Customer retains final authority and responsibility for approving and/or implementing any configuration changes.

7. Exclusions

This Service Schedule is strictly limited to the Microsoft 365 Cloud environment. The following are expressly excluded from this scope:

- Microsoft Azure Infrastructure is excluded, with the sole exception of the Log Analytics Workspace required to host Microsoft Sentinel for M365 logging purposes.

- On-premises servers, hardware, or networking equipment.
- End-user helpdesk support or "break-fix" troubleshooting.

On-premises Infrastructure: While 360 will audit the telemetry and alerts generated by MDI sensors on Domain Controllers, the physical maintenance, patching, and hardware management of on-premises servers remain the Customer's responsibility.

Terms & Conditions: M365 Security Advisory

1. Definition of "Minor Adjustments"

For the purposes of this Service, a "Minor Adjustment" is defined as a single configuration change or administrative task within the Microsoft 365 Admin Center, Entra ID, or Intune portal that can be completed within a thirty (30) minute window, including testing and documentation.

Limitations: Minor Adjustments are limited to a maximum of two (2) per service cycle (Monthly/Quarterly).

Exclusions: Any task that requires end-user interaction (e.g., re-enrolling a device), impacts more than 10% of the user base, or requires significant change management planning is excluded and will be quoted as Project Work.

2. Nature of Advisory Service (Non-Operational)

Customer acknowledges that the Strategic Advisory Service is primarily a consultative and reporting service.

Remediation: 360 is not responsible for the ongoing operational remediation of alerts, daily helpdesk tickets, or system failures unless specifically outlined in a separate Managed Service Agreement.

Incident Monitoring (Informational Only): As part of the monthly audit process, 360 will review Microsoft Defender incidents and alerts for anomalous or suspicious activity. If 360 identifies activity that appears to require immediate attention, we will make reasonable efforts to notify the Customer's designated contact via email or phone. However, 360 is not providing 24/7 security monitoring or incident response services under this agreement. Formal incident response, forensic investigation, or breach remediation requires a separate engagement.

Sentinel Health Monitoring: 360's oversight of the Microsoft Sentinel workspace is limited to health monitoring only, including verification that:

- Free-tier data connectors are actively ingesting logs
- No connector failures or configuration drift has occurred
- Log Analytics workspace has sufficient retention configured

360 does not perform active security operations, alert triage, threat hunting, or custom detection rule tuning within Sentinel unless outlined in a separate SOW.

No Guarantee of Security: While 360 provides recommendations based on industry best practices, the Customer acknowledges that no audit can guarantee 100% protection against cyber threats, and 360 is not liable for breaches occurring on systems managed or implemented by the Customer's internal staff.

3. Change Management & Approval

360 will not perform any "Minor Adjustments" or configuration changes without written or verbal authorization from the Customer's designated point of contact during the Advisory Consultation.

360 reserves the right to refuse a "Minor Adjustment" request if it is deemed high-risk or better suited for a formal Project engagement.

4. Continuity of Access

The Service fee is based on 360's ability to access the Tenant via Granular Delegated Admin Privileges (GDAP).

If 360 is unable to perform an audit due to revoked access, expired Microsoft Customer Agreements (MCA), or technical lockouts caused by the Customer, the monthly service fee remains due in full. 360 will make reasonable efforts to notify the Customer of access issues, but the responsibility for restoration lies with the Customer.

5. Licensing Requirements

Customer is responsible for procurement and payment of all necessary Microsoft 365 licensing (e.g., Business Premium, E3, E5) required to run the features being audited. If the Customer lacks the required licensing for a specific pillar (e.g., MDE or Entra P2), 360 will note this as a gap in the report but will not be able to perform the audit for that specific component. Customer is responsible for any Azure consumption costs associated with Microsoft Sentinel data ingestion (outside of free-tier connectors) and long-term log retention.