Schedule 1 - Managed IT Services Terms

Version: Standard Website Terms

1. Application and Scope

1.1 This Schedule applies where the Order Form includes managed IT support, service desk, monitoring, patching, endpoint management, user administration, server support, Microsoft 365 administration, infrastructure support, co-managed IT support, fully managed IT support or similar recurring IT management services.

1.2 The Company's obligations are limited to the supported users, devices, systems, applications, environments and sites expressly identified in the Order Form or otherwise accepted by the Company in writing. Anything not expressly included is out of scope.

1.3 The Company may maintain a service catalogue, onboarding checklist, support matrix and technical standards document for Managed IT Services. Those documents shall form part of the operational scope of the Service.

2. Onboarding, Baseline and Technical Standards

2.1 The Company may require an onboarding, discovery, audit, remedial or stabilisation phase before or during commencement of Managed IT Services.

2.2 If the Company identifies unsupported, end-of-life, insecure, materially under-licensed, unstable, undocumented or non-standard systems, the Company may: (a) exclude them from support; (b) support them on a reasonable endeavours basis only; (c) require remedial work as a condition of full service; or (d) charge separately for remediation, replacement or project work.

2.3 The Customer shall provide all administrative credentials, licences, asset information, diagrams, warranties, vendor contacts and access reasonably required for onboarding and ongoing support.

3. Support Requests and Service Management

3.1 The Customer shall log incidents and service requests using the channels and formats notified by the Company from time to time. The Company may require different channels for major incidents, password resets, emergency security events or changes.

3.2 The Company may refuse to action requests made by unauthorised persons and may require identity verification, approval workflows, multi-factor checks or written confirmations before carrying out sensitive actions.

3.3 Response and resolution targets, where agreed, shall be measured only during the relevant service window and shall exclude any time during which a ticket is awaiting Customer information, testing, approval, physical access, parts, vendor response or third-party action.

3.4 The Company may close, cancel or park tickets where the Customer fails to respond, fails to make a user or system available, or fails to provide required information after reasonable follow-up.

3.5 Unless expressly included in the Order Form, out-of-hours support, emergency call-out, weekend working, bank holiday working and attendance outside the standard support window are chargeable in addition at the Company's then-current rates.

3.6 Managed IT Services supplied on an "unlimited" or recurring fixed-fee basis are provided subject to fair, reasonable and proportionate use within the agreed support scope. The term "unlimited" does not mean unrestricted, excessive, abnormal, project-based, forensic, investigatory, abusive, vexatious, repetitive or no-fault-found usage.

3.7 Where the Company has investigated an issue and reasonably concluded that no fault is present, that the relevant system is operating substantially as intended, or that the concern cannot be substantiated by available evidence, any repeated or further requests relating to the same or substantially similar issue may, at the Company's discretion, be treated as chargeable services outside scope.

3.8 Where the Customer requests repeated investigation of suspected compromise, surveillance, intrusion, interception, manipulation, unauthorised access or similar security concerns and the Company's reasonable assessment, tooling, logs or third-party findings do not substantiate the existence of such issue, the Company may close the ticket, recommend remediation or security uplift work, require the matter to proceed as a separate chargeable project or specialist security engagement, and decline to provide further repeated investigative work within the recurring Charges.

3.9 If the Customer's ticket volume, frequency of requests, engineer demand, escalation pattern or operational behaviour is excessive, abnormal or disproportionate having regard to the contracted Services or the supported environment, the Company may review the commercial basis of the Services, reprice the Services, impose service controls, require a remediation plan, treat the affected work as out of scope, suspend support, or terminate the affected Services for cause.

3.10 The Company may suspend, limit or refuse service where the Customer's personnel engage in abusive, threatening, harassing, vexatious, persistently unreasonable or obstructive conduct, or where the Customer repeatedly rejects reasonable technical findings, refuses recommended remediation steps, or otherwise materially impedes efficient service delivery.

4. Remote Tooling, Monitoring and Access

4.1 The Customer authorises the Company to deploy, operate, maintain and update remote monitoring and management agents, scripts, security tooling, patching agents, automation tooling, MDM profiles, EDR software, remote support tools and similar utilities on supported systems.

4.2 The Customer shall not remove, disable, interfere with or restrict such tooling without the Company's prior written consent.

4.3 The Customer acknowledges that monitoring is limited to systems on which the relevant tooling has been successfully deployed and remains operational. The Company shall have no responsibility for blind spots, missed alerts or unsupported systems not properly onboarded.

5. Service Boundaries and Exclusions

5.1 Unless expressly included in the Order Form, Managed IT Services do not include: (a) project work, migrations, upgrades, tenant-to-tenant moves, site moves, new deployments or major changes; (b) support for bespoke applications, line-of-business applications or third-party systems for which the Company does not have administrative access or vendor support rights; (c) structured cabling, electrical works, data recovery, forensic investigation or evidential preservation; (d) software development or scripting beyond routine administrative automation; (e) hardware replacement, warranty claims or vendor field engineering; or (f) compliance, certification or audit representation services.

5.2 Onsite attendance, where not expressly included, shall be chargeable in addition, including travel time, mileage and accommodation where applicable.

6. Customer Responsibilities

6.1 The Customer shall remain solely responsible for: (a) maintaining valid software licences, subscriptions, warranties and vendor support contracts; (b) ensuring all users comply with security policies and acceptable use requirements; (c) promptly notifying the Company of joiners, movers, leavers, access changes, suspected compromise and business-critical deadlines; (d) maintaining internet connectivity, power, environmental controls and physical security; and (e) keeping appropriate local and cloud backups unless backup services are expressly included.

6.2 The Customer shall review and implement the Company's recommendations promptly. The Company shall not be liable for any loss, outage, compromise or non-compliance caused or contributed to by the Customer's refusal, delay or failure to implement a reasonable recommendation.

6.3 In a co-managed environment, the Customer remains responsible for the acts and omissions of its internal IT personnel and any third-party support providers. The Company shall not be liable for incidents, outages, misconfigurations, security weaknesses or data loss caused or contributed to by shared administration, competing changes, undocumented changes, parallel support arrangements or withheld information.

7. Backups, Patching and Security

7.1 Unless backup services are expressly included in the Order Form or another applicable Service Schedule, the Customer remains solely responsible for backup, restore testing, retention, disaster recovery and business continuity.

7.2 Even where backup, patching, anti-malware, device control, email security or similar security functions are included, the Company does not warrant that all threats, faults, vulnerabilities, data loss events or outages will be prevented, detected or remediated.

7.3 Patch deployment may be deferred, sequenced, excluded or rolled back where the Company reasonably considers that compatibility, change management, business timing, vendor advice or service stability requires it.

7.4 If the Customer refuses or delays implementation of security baselines, critical patches, MFA, endpoint protection, backup scope, access restrictions or other minimum controls reasonably required by the Company, the Company may suspend support, exclude affected systems from scope, annotate the environment as non-compliant, terminate the affected Services for cause and continue to charge in accordance with the Agreement.

8. Third-Party Liaison

8.1 The Company may liaise with third-party software vendors, internet providers, hosting providers, print vendors, security vendors and other support organisations on the Customer's behalf, but the Company does not assume responsibility for their performance or outcomes.

8.2 Time spent by the Company liaising with third parties may be chargeable unless expressly included in the applicable support scope.

9. Exit and Transition

9.1 On termination or expiry of Managed IT Services, the Company may remove agents, remote tooling, credentials, policies, configurations and management artefacts deployed by or on behalf of the Company.

9.2 Any knowledge transfer, asset register collation, documentation tidy-up, handover pack, administrative transfer or transition assistance shall be chargeable and subject to prepayment.