IT SUPPORT / MANAGED SERVICES AGREEMENT

1. 1. Parties and Engagement

This Managed IT Services Agreement (the "Agreement") is entered into on [EFFECTIVE DATE] between [PROVIDER NAME], a [ENTITY TYPE] located at [PROVIDER ADDRESS] (the "Provider"), and [CLIENT NAME], a [ENTITY TYPE] located at [CLIENT ADDRESS] (the "Client"). The Provider will deliver managed information technology services for the Client environment described in Exhibit A. The Provider is an independent contractor responsible for its own personnel, taxes, insurance, and tools, and its personnel are not employees of the Client. The primary contacts are [PROVIDER SERVICE MANAGER AND EMAIL] and [CLIENT IT CONTACT AND EMAIL], and the Client will designate at least one authorized approver for changes, purchases, and access requests.

2. 2. Covered Environment and Users

Covered assets are listed in Exhibit A and include [COVERED ASSETS, e.g., a stated number of workstations, laptops, servers, firewalls, switches, wireless access points, and cloud tenants] supporting up to [COVERED USER COUNT] users at [COVERED SITES]. Assets added during the term are covered from the date they are onboarded and are billed at the per-unit rates in Section 8; the Provider may decline to support an asset that is end of life, unsupported by its vendor, or unable to run the required management and security agents. Assets outside the list, including personal devices, unmanaged shadow systems, specialty industrial or medical equipment, and vendor-managed line-of-business applications, are excluded unless added by written amendment. The Client will maintain accurate asset and user counts and will notify the Provider of joiners, movers, and leavers within [USER CHANGE NOTICE, e.g., two business days].

3. 3. Services Included

The Provider will deliver: help desk support for covered users through [SUPPORT CHANNELS, e.g., phone, email, and a ticket portal]; remote monitoring and alerting on covered assets; operating system and third-party patch management on the schedule in Section 5; endpoint protection deployment and monitoring; backup configuration, monitoring, and restore testing as described in Section 6; user account administration including onboarding and offboarding; network device configuration management; vendor liaison with the third-party suppliers listed in Exhibit A; documentation of the environment; and a periodic technology review [REVIEW CADENCE, e.g., quarterly]. On-site attendance is included [ONSITE INCLUSION, e.g., up to a stated number of visits or hours per month] and further visits are billed at [ONSITE RATE].

4. 4. Service Levels and Response Targets

Support is provided during [SUPPORT HOURS, e.g., business days 8:00 a.m. to 6:00 p.m. local time] excluding [HOLIDAY LIST]. Incidents are classified as follows and carry these target first-response times: Severity 1, a complete outage or a security incident affecting the whole organization or a critical system, [SEV 1 RESPONSE, e.g., 30 minutes] with continuous effort until service is restored or a workaround is in place; Severity 2, a major function degraded or a group of users unable to work, [SEV 2 RESPONSE, e.g., 2 business hours]; Severity 3, a single user impaired with a workaround available, [SEV 3 RESPONSE, e.g., 8 business hours]; Severity 4, a request, question, or scheduled change, [SEV 4 RESPONSE, e.g., 2 business days]. Response targets measure the time to a substantive human response, not resolution, because resolution time depends on the fault, on vendors, and on parts availability. Out-of-hours emergency support is available at [AFTER HOURS RATE] or is included where marked here: [AFTER HOURS INCLUSION]. Where a target is missed in a month, the Client may request a service credit of [SERVICE CREDIT] on written request within [CREDIT REQUEST WINDOW, e.g., 30 days],

and service credits are the sole remedy for missed response targets.

5. 5. Patching, Maintenance, and Change Management

The Provider will apply critical security patches to covered assets within [CRITICAL PATCH WINDOW, e.g., seven days] of vendor release and routine patches on a [ROUTINE PATCH CADENCE, e.g., monthly] cycle, in the maintenance window of [MAINTENANCE WINDOW]. The Provider may delay a patch that is known to break a business-critical application and will inform the Client of the risk and the mitigation. Reboots required by patching will occur during the maintenance window unless the Client agrees otherwise. Changes that affect availability, security posture, or cost will follow a change process requiring approval from an authorized approver of the Client, except for emergency changes needed to contain an active incident, which the Provider may make immediately and will document within [EMERGENCY CHANGE NOTICE, e.g., 24 hours]. The Provider will maintain a written change log available to the Client.

6. 6. Backup, Recovery, and Business Continuity

The Provider will configure and monitor backups of the systems listed in Exhibit A with a backup frequency of [BACKUP FREQUENCY], a retention period of [RETENTION PERIOD], and storage in [BACKUP LOCATIONS, e.g., local appliance plus offsite or cloud copy]. Target recovery objectives are a recovery point objective of [RPO] and a recovery time objective of [RTO] for the systems designated as critical, and these are targets rather than guarantees. The Provider will perform test restores [RESTORE TEST FREQUENCY, e.g., quarterly] and will report the results to the Client. Backups cover only the systems and data listed in Exhibit A; data held in unmanaged services, personal accounts, or local device storage outside the managed folders is not backed up. The Client acknowledges that no backup system eliminates the risk of data loss and that recovery from ransomware or a major failure may require rebuild time beyond the stated objectives.

7. 7. Security Responsibilities and Incident Response

The Provider will deploy and monitor endpoint protection, apply the hardening baseline described in Exhibit A, manage administrative access using least privilege, enforce multi-factor authentication on the systems that support it, and maintain logging on covered assets. The Client is responsible for security decisions within its business, for approving recommended controls, for user awareness training unless purchased from the Provider, and for the consequences of declining a recommended control, which the Provider will record in writing. On becoming aware of a suspected security incident affecting covered assets, the Provider will notify the Client without undue delay and in any event within [SECURITY NOTICE PERIOD, e.g., 24 hours], will take reasonable containment steps, and will assist with investigation at [INCIDENT RESPONSE RATE] beyond the first [INCLUDED IR HOURS] hours. The Provider does not warrant that the environment cannot be breached, and the Client remains responsible for its own regulatory notification obligations, insurance, and legal reporting.

8. 8. Fees, Onboarding, and Out-of-Scope Work

The Client will pay a monthly fee of [MONTHLY FEE], calculated as [FEE BASIS, e.g., a per-user or per-device rate applied to the counts in Exhibit A], invoiced monthly in advance and due within [PAYMENT TERM, e.g., 15 days]. A one-time onboarding fee of [ONBOARDING FEE] covers discovery, documentation, agent deployment, and remediation of the environment to a supportable baseline; work required to reach that baseline beyond the onboarding fee is quoted separately. Excluded from the monthly fee and billed separately: project work such as migrations, rollouts, and office moves; hardware, software licenses, and subscriptions, which are purchased in the name of the Client; after-hours and emergency work outside included coverage; support caused by the Client or a third party making unapproved changes; and recovery work following an incident. Rates for out-of-scope work are [PROJECT RATE]. Fees may be adjusted once per [RATE REVIEW PERIOD, e.g., 12 months] on [RATE

CHANGE NOTICE, e.g., 60 days] written notice, and the Client may terminate without penalty before an increase takes effect.

9. 9. Client Responsibilities

The Client will provide safe access to sites and systems, maintain an accurate inventory of users and assets, and ensure users cooperate with the Provider and follow reasonable acceptable use and security policies. The Client will maintain valid licenses and support contracts for its software and hardware, will fund replacement of equipment the Provider identifies as end of life or unsupportable, and accepts that the Provider cannot guarantee performance or security on unsupported systems. The Client will not make material changes to the environment, including adding servers, changing network configuration, or granting third-party access, without informing the Provider, and additional work created by unapproved changes is billable. The Client is responsible for the content and legality of its data and for its own regulatory compliance obligations.

10. 10. Credentials, Access, and Documentation

Administrative credentials for the environment belong to the Client. The Provider will store them in a managed password vault, will limit access to personnel who need it, will use named accounts rather than shared logins where the system supports it, and will remove access for its personnel who leave the engagement within [PERSONNEL OFFBOARDING PERIOD, e.g., one business day]. All domains, cloud tenants, subscriptions, and licenses will be registered in the name of the Client. The Provider will maintain current documentation of the environment, including network diagrams, asset inventory, license records, vendor contacts, and recovery procedures, and will make it available to the Client on request during the term and at termination. The Provider will not withhold credentials or documentation as leverage in a commercial dispute, provided undisputed amounts due are paid.

11. 11. Personnel and Non-Solicitation

The Provider will assign qualified personnel, will supervise and pay them, and remains responsible for their acts and omissions and their compliance with this Agreement. The Provider may use subcontractors for specialist work and remains fully responsible for them. Personnel with access to Client systems will be subject to the standard screening process of the Provider, described here: [SCREENING DESCRIPTION]. During the term and for [NON-SOLICIT PERIOD, e.g., 12 months] afterward, neither Party will knowingly solicit for employment any individual of the other who was directly involved in the services, except through general public job postings, and a breach entitles the other Party to a placement fee of [PLACEMENT FEE] as the exclusive remedy.

12. 12. Term, Termination, and Offboarding

The initial term is [INITIAL TERM, e.g., 12 months] from [SERVICE START DATE], renewing automatically for successive periods of [RENEWAL TERM] unless either Party gives [NON-RENEWAL NOTICE, e.g., 60 days] written notice before the end of the then-current term. Either Party may terminate for a material breach not cured within [CURE PERIOD, e.g., 15 days] after written notice, and the Provider may suspend non-critical services after written notice if an undisputed invoice is more than [SUSPENSION TRIGGER, e.g., 30 days] overdue. On termination for any reason, the Provider will, within [OFFBOARDING PERIOD, e.g., 15 days], deliver all administrative credentials, environment documentation, asset and license inventories, backup copies and restoration instructions, and any Client data it holds, and will remove its agents and remote access tools from covered assets. Transition assistance beyond that handover is available at [TRANSITION RATE] and will be provided in good faith to any successor provider.

13. 13. Warranties, Limitation of Liability, and Indemnification

The Provider warrants that the services will be performed in a professional and workmanlike manner by qualified personnel using reasonable care. Except as expressly stated, the services are provided without further warranty, including implied warranties of merchantability and fitness for a particular purpose, and the Provider does not warrant uninterrupted operation, that data loss will not occur, or that the environment cannot be compromised. Neither Party is liable for indirect, incidental, consequential, or special damages, or for lost profits, revenue, or data, and the total aggregate liability of the Provider will not exceed the fees paid by the Client in the [LIABILITY CAP PERIOD, e.g., six months] preceding the event giving rise to the claim, except in cases of gross negligence or willful misconduct. Each Party will defend and indemnify the other against third-party claims arising from its own breach of this Agreement or violation of law. The Provider will maintain [INSURANCE REQUIREMENTS, e.g., general liability, professional liability, and cyber liability coverage] and will provide a certificate on request.

14. 14. Confidentiality, Data Protection, and General Provisions

Each Party will keep confidential the non-public information of the other, including systems information, security configurations, business data, and pricing, will use it only to perform this Agreement, and will protect it with at least reasonable care, indefinitely for security configurations and for [CONFIDENTIALITY PERIOD, e.g., three years] otherwise. Where the Provider processes personal data on behalf of the Client, it will do so only on documented instructions and the Parties will execute a data processing addendum where applicable law requires one. This Agreement is governed by the laws of the State of [GOVERNING STATE], disputes will be brought in the courts located in [VENUE COUNTY AND STATE] after escalation to senior representatives, and this Agreement with its exhibits is the entire agreement between the Parties. Amendments must be in writing and signed, neither Party may assign without consent except to a successor of substantially all of its business, and neither Party is liable for delay caused by events beyond its reasonable control, including vendor outages, utility failures, and supply chain disruption.

15. 15. Signatures

By signing below, both Parties confirm they have read and agree to this Agreement as of the Effective Date. PROVIDER: [PROVIDER NAME]. Signature: _____. Printed Name: [PROVIDER SIGNER NAME]. Title: [TITLE]. Date: [DATE]. CLIENT: [CLIENT NAME]. Signature: _____. Printed Name: [CLIENT SIGNER NAME]. Title: [TITLE]. Date: [DATE]. This Agreement may be executed in counterparts, and electronic signatures have the same effect as original signatures on a single document.

16. Disclaimer

This template is provided for general informational purposes only and is not legal advice. Managed IT engagements intersect with data protection law, breach notification statutes, sector-specific regulation such as healthcare and financial services rules, and insurance requirements that vary by jurisdiction and industry. Review and adapt this document for your own environment, and consult a licensed attorney and your insurer before using it where regulated data or critical infrastructure is involved. Use of this template does not create an attorney-client relationship with ScanContract.