Services *Dictionary*

Last Updated: June 12, 2026

Covered

> Users, devices, servers, domains, or systems that are expressly identified in a SOW as within the scope of services. Items not expressly identified are not Covered and are not within scope. This complements the defined terms in the Master Terms and Conditions ("**Terms**") including the defined terms "Devices," "Environment," and "Unknown Devices."

Business Hours

> 8:00 a.m. to 5:00 p.m. Eastern Time, Monday through Friday, excluding federal holidays.

Rate Card

> Simple Tech's published schedule of hourly labor rates, project rates, one-time fees, and pass-through pricing, as updated from time to time by Simple Tech.

1. Core Managed Services

These are the atomic services that appear, in various combinations, across SimpleCare plan tiers.

Workstation Monitoring and Management

> Remote monitoring, alerting, and management of covered end-user devices (desktops and laptops). Includes health and performance monitoring, routine patching of the operating system and supported third-party applications, firmware updates where applicable, configuration baseline enforcement, and remote remediation of alerts. Does not include hardware replacement or new device procurement.

Server Monitoring and Management

> Remote monitoring, alerting, and management of covered physical or virtual servers. Includes scheduled maintenance and reboots, Active Directory and user management on the server, backup job monitoring where a backup service is in place, patching, and support for supported third-party software installed on the server. Billed per server. Does not include hardware replacement, major software upgrades, or new server deployments.

Help Desk and Remote Support

> Day-to-day remote technical support for covered users and devices during Business Hours. Support is accessed through the Simple Tech ticket portal, support email, or support telephone line. Covers troubleshooting, routine configuration changes, standard end-user assistance, and recurring support requests customary for the applicable service tier. Does not include project work, migrations, environment redesigns, on-site services, or after-hours work.

After-Hours Support

> Remote support outside of Business Hours. Available either ad-hoc at Rate Card rates or under a monthly After-Hours Retainer add-on. Not included in any standard plan.

On-Site Support

> In-person technical support at a Client location. Not included in standard plans. Available on request at then-current Rate Card rates, subject to minimum-hour billing and travel considerations.

Client Onboarding

> One-time setup and transition work performed at the start of an engagement, including device enrollment in management tooling, deployment of the applicable security stack, Microsoft 365 or Google Workspace tenant review and configuration, documentation of the environment, and user provisioning. Billed as a one-time fee under the Rate Card; not included in recurring plan pricing.

User Onboarding and Offboarding (Ongoing)

> Setup of new employees (account creation, license assignment, device preparation, mailbox configuration, standard application installation) and offboarding of departing employees (account disable, license reclamation, mailbox handling, data preservation per Client policy). Included in recurring plan pricing for covered users. Remote device setup is included; on-site work, same-day shipping, and data migration are not included.

Vendor Support Liaison

> Acting as Client's technical point of contact with the third-party vendors identified in the SOW (for example, Microsoft, Google, line-of-business application vendors, internet service providers, telephony providers). Includes opening and managing support cases and coordinating resolution. Does not include payment of third-party support or incident fees, which remain Client's responsibility.

Quarterly IT Management Meeting

> Scheduled remote business review, typically quarterly, covering service delivery, outstanding items, recommended improvements, security posture, and upcoming planning items.

Hardware Assessment Report

> Periodic report summarizing the condition, age, warranty status, and supportability of the Client's covered hardware, intended to support lifecycle and budget planning.

Identity-Only Coverage

> Reduced-scope coverage for users who need identity and email protection but do not have a managed endpoint — for example, contractors, seasonal staff, shared-mailbox users, or users on unmanaged personal devices. Priced as an add-on to each SimpleCare plan. Excludes endpoint management, endpoint backup, and device-level support.

Line-of-Business Application Support

> Installation, updates, troubleshooting, and vendor liaison for Client line-of-business applications (for example, QuickBooks, practice-management software, ERP systems, CRM systems). Support is limited to installation, configuration, user access, and first-line troubleshooting; does not include application administration, custom development, database administration, or licensing costs for the application itself. Covered applications must be identified in the SOW.

Remote Access and VPN Management

> Configuration and ongoing management of Client remote-access infrastructure, including site-to-site VPN, client VPN, Remote Desktop Protocol gateways, and zero-trust network access solutions. Includes policy configuration, user access management, and firmware or agent updates. Does not include network redesign, ISP changes, or hardware procurement for remote-access infrastructure unless separately scoped.

Printer and Multifunction Device Support

> Deployment of printer drivers and print queues, configuration of network printers and multifunction devices, scan-to-email setup, and first-line troubleshooting. Does not include printer hardware repair, toner or consumables procurement, or management of production print environments. Multifunction device vendor coordination is provided where the vendor is listed under the Vendor Support Liaison service.

IT Documentation and Runbooks

> Creation and maintenance of Client-specific IT documentation, including network diagrams, system inventories, vendor contacts, administrative credential storage (in the managed password manager), and standard operating procedures for recurring tasks. Documentation is maintained in Simple Tech's internal systems and made available to Client upon reasonable request, subject to the transition provisions of Terms Section 6.5(d).

BYOD (Bring-Your-Own-Device) Support

> Where Client permits employees to access Client resources from personally owned devices, Simple Tech may provide limited configuration support (for example, Microsoft 365 mobile app setup, MFA enrollment, conditional-access configuration). Personal devices are not Covered, are not subject to endpoint management or endpoint backup, and are not within scope for troubleshooting issues unrelated to Client resource access.

Remote Work Support Boundaries

> Simple Tech supports Client-owned, Covered devices regardless of physical location. Simple Tech does not support Client employees' home internet connections, home networking equipment, personal peripherals, or family-member devices, and is not responsible for performance issues attributable to home-network conditions.

2. Security Services

These services protect covered endpoints, identities, email, and the overall attack surface. Specific inclusions vary by SimpleCare plan tier; atomic services are defined here without reference to which tier includes them.

Endpoint Detection and Response (EDR)

> A managed EDR agent is deployed to covered endpoints to detect suspicious behavior, block known threats, and support investigation and response. Delivered through third-party security platforms selected by Simple Tech.

Managed Detection and Response (MDR) with 24/7 SOC and SIEM

> Continuous, 24x7 threat monitoring, triage, and response performed by a third-party Security Operations Center, together with SIEM log collection and correlation. MDR does not guarantee prevention of all incidents; the service is designed to detect and respond as quickly as reasonably possible.

DNS Filtering

> DNS-layer filtering on covered endpoints to block known malicious, phishing, and policy-violating domains, including protection when devices are off the corporate network.

Patch Management

> Managed patching of operating systems and supported third-party applications on covered endpoints and servers. Patch windows, approval workflows, and reboot policies are configured per Client environment.

Privileged Access Management (PAM) and Ransomware Encryption Protection

> Endpoint protection capabilities that limit local administrative privilege, elevate privileges on a task basis, and detect unauthorized encryption activity associated with ransomware.

Application Control

> Policies on covered endpoints that restrict which applications may execute, reducing the attack surface for unknown or untrusted software.

Vulnerability Management

> Periodic scanning of covered endpoints and servers for known vulnerabilities, with remediation performed through patching or configuration changes where supported. Does not include remediation requiring hardware replacement or major software upgrades outside the managed scope.

Microsoft 365 Identity Threat Detection and Response

> Monitoring of Microsoft 365 identities for signs of compromise, including suspicious sign-ins, mailbox rule abuse, privilege escalation, and data exfiltration patterns.

Email Security — Anti-Phishing, Anti-Spam, and Malicious Link Protection

> Filtering of inbound email for phishing, spam, and malicious links and attachments. On plans that include Microsoft 365 Business Premium, delivered through Microsoft Defender for Office 365; on other tiers, delivered through third-party email security platforms selected by Simple Tech.

DMARC Configuration and Monitoring

> Setup, deployment, and ongoing monitoring of SPF, DKIM, and DMARC records for Client's email-sending domains, including reporting on authentication results and unauthorized sending sources. Available as a paid add-on and included in higher SimpleCare tiers.

Phishing Simulation and Security Awareness Training

> Automated phishing simulation campaigns and role-appropriate security awareness training for covered users, with reporting on workforce participation and performance.

Password Management

> A managed business password manager provisioned for all users across all SimpleCare plan tiers. Simple Tech considers a business password manager a baseline control for service delivery; this service is mandatory for covered users and cannot be waived at the user level.

Endpoint Security Assessment

> Automated assessment of the security configuration of covered endpoints, producing findings and prioritized remediation recommendations.

External Attack Surface Scanning

> Periodic scanning of Client's publicly reachable internet footprint (domains, subdomains, exposed services, certificates) to identify externally visible risks.

Network Uptime and Infrastructure Monitoring

> Monitoring of managed network infrastructure (firewalls, switches, access points) for availability and configuration drift.

Security Incident — Initial Response

> Initial-period assistance following a suspected data breach or security incident to help identify the likely source and begin formulating a response. Forensic investigation, breach notification, regulatory reporting, and post-incident rebuild work are not included in managed services and are delivered under a separate project engagement. Initial Response includes up to twenty-four (24) Business Hours of remote triage, beginning when Simple Tech first becomes aware of a suspected Security Incident, whether through Client report or detection by Simple Tech or its service providers. Any services beyond the Initial Response window, including forensic investigation, containment planning, eradication, recovery, notification support, or rebuild work, are out of scope unless separately agreed in writing.

Compliance Attestation and Evidence Support

> Where Client is subject to a compliance framework (for example, HIPAA, PCI-DSS, CMMC, SOC 2, NIST), Simple Tech will provide evidence of security controls within scope of its managed services (for example, patch reports, backup reports, endpoint configuration exports, security awareness training records) to support Client's attestations and audits. Simple Tech does not certify Client compliance, does not render a compliance opinion, and does not represent that the managed services alone bring Client into regulatory compliance. See Terms Section 4.3.

Cyber Insurance Renewal Support

> At Client's request, Simple Tech will assist Client in completing cyber-insurance renewal questionnaires by providing factual information about the security controls Simple Tech manages on Client's behalf. Simple Tech's responses are limited to services actually delivered and do not include representations about Client systems or processes outside Simple Tech's managed scope. Client is responsible for reviewing, verifying, and signing the questionnaire.

Shadow IT and Unsanctioned Application Policy

> Applications, cloud services, and SaaS subscriptions adopted by Client or Client employees without Simple Tech's knowledge or without being added to the Covered scope ("Shadow IT") are not within scope of any managed service. Simple Tech is not responsible for security incidents, data exposure, or operational issues arising from Shadow IT. Simple Tech may recommend discovery and remediation of Shadow IT as a project engagement.

Data Residency and Sovereignty

> Where Client has specific data residency or sovereignty requirements (for example, data must remain within the United States or a specific jurisdiction), such requirements must be identified in the SOW. Absent such identification, Simple Tech makes no representation regarding the physical location of Client data processed or stored by third-party platforms. Data residency commitments are limited to those provided by the underlying third-party platforms.

3. Data Protection and Backup Services

Backup services reduce the risk of data loss and support recovery; they do not guarantee complete or successful recovery in every circumstance.

Workstation Backup

> Image and file-level backup of covered workstations to a third-party cloud repository. Retention and restore scope as configured per Client environment.

Microsoft 365 Backup — Mailbox and SharePoint

> Daily backup of Microsoft 365 mailboxes and SharePoint content to a third-party cloud repository, with point-in-time restore available within the retention window.

Google Workspace Backup

> Daily backup of Google Workspace mailboxes and Drive content to a third-party cloud repository, with point-in-time restore available within the retention window. Available where Client uses Google Workspace as the primary email and collaboration platform.

Server Backup

> Backup of covered physical or virtual servers, including image and/or file-level backup as configured per Client. Billed per server (see Infrastructure in Section 6). Monitoring and restore-on-request are included; major disaster recovery rebuild work is out of scope and delivered under a separate project engagement.

Restore on Request

> Remote restoration of files, mailboxes, SharePoint or Drive items, or full systems from supported backup platforms, subject to the backup service's technical limits. Large-scale or disaster-level restores may be scoped as a project.

4. Microsoft 365 and Google Workspace Management

Microsoft 365 is Simple Tech's primary supported platform. Google Workspace is supported for Clients who use it as their primary email and collaboration platform, with a scope comparable to Microsoft 365 management.

Microsoft 365 Tenant and User Management

> Day-to-day administration of the Client's Microsoft 365 tenant, including user creation and deprovisioning, license assignment, group and mailbox configuration, password resets, and related administrative tasks. Microsoft 365 licensing fees are pass-through costs and are not included in the Service Fee unless expressly set forth in the SOW.

Microsoft Intune and Defender Management

> Where the Client's Microsoft 365 subscription includes Intune and Microsoft Defender for Office 365 (generally Microsoft 365 Business Premium and higher), Simple Tech will configure and manage device management policies, compliance policies, and email security policies within those products.

Google Workspace Tenant and User Management

> Day-to-day administration of the Client's Google Workspace tenant, including user creation and deprovisioning, license assignment, group and mailbox configuration, password resets, and related administrative tasks. Google Workspace licensing fees are pass-through costs and are not included in the Service Fee unless expressly set forth in the SOW.

DNS and Domain Management

> Configuration and ongoing management of DNS records for Client-owned domains that are identified in the SOW, including MX records, SPF/DKIM/DMARC records, CNAMEs, A records, and TXT records required for covered services. Does not include domain registration fees, domain transfers, or management of web hosting unless separately scoped.

AI Tool Configuration and Governance

> At Client's request, Simple Tech will assist Client with the configuration of Microsoft Copilot, Microsoft Copilot Studio, Google Gemini for Workspace, and similar artificial intelligence tools, including license assignment, tenant policy configuration, and data-governance settings (for example, sensitivity labels, DLP integration). AI tools are provided by third parties and are subject to their terms. Simple Tech does not warrant the accuracy, reliability, or fitness for purpose of any AI-generated output. See also Terms Section 4, which addresses Client responsibility for independent review of AI outputs.

5. Add-On Services

Add-ons are not included in any SimpleCare plan by default unless expressly listed in the SOW. Pricing is set in the Rate Card.

DMARC Monitoring (Add-On)

> DMARC reporting and monitoring service priced per domain. Included in higher SimpleCare tiers; available as an add-on for lower tiers.

After-Hours Retainer

> Flat-rate monthly retainer that entitles Client to after-hours remote support at included (non-premium) rates, subject to reasonable use. Intended for Clients who regularly operate outside Business Hours.

6. Infrastructure Services

Infrastructure services are priced per device or per server, independent of user-based SimpleCare plans. A Client typically subscribes to one or more user plans plus the infrastructure services that apply to their physical environment.

Managed Firewall

> Configuration, monitoring, firmware updates, and ongoing policy management of a covered firewall device. Billed per device. Does not include the firewall hardware or third-party subscription licensing, which are billed separately as pass-through costs.

Managed Switch

> Configuration, monitoring, firmware updates, and ongoing management of a covered managed network switch. Billed per device. Excludes switch hardware and cabling.

Managed Access Point

> Configuration, monitoring, firmware updates, and ongoing management of a covered wireless access point. Billed per device. Excludes access point hardware and cabling.

Managed Server

> Full managed-service coverage for a covered server (see Server Monitoring and Management in Section 1). Billed per server, in addition to any user-based SimpleCare subscription.

Server Backup (Per Server)

> Per-server backup service (see Server Backup in Section 3). Billed per server.

Managed NAS

> Configuration, monitoring, firmware updates, and management of a covered network-attached storage device. Does not include the NAS hardware or disks. Billed per device.

7. SimpleCare Plan Tiers — Reference Only

SimpleCare Micro

> Entry-level tier for very small environments. Uses a lighter security tool stack than higher tiers (no full 24/7 MDR layer) and Microsoft 365 Business Basic as the underlying Microsoft license. Identity-only coverage available as an add-on user type.

SimpleCare Business

> Standard managed IT and support tier for small business environments. Full managed endpoint security stack and Microsoft 365 management, without the full 24/7 MDR-grade security layer. Identity-only coverage available as an add-on user type.

SimpleCare Security

> Security-forward tier. Adds 24/7 Managed Detection and Response, Microsoft 365 identity threat detection, and additional security tooling on top of the Business tier. Identity-only coverage available as an add-on user type.

SimpleCare Secure+

> Enhanced security tier. Adds further security controls, DMARC monitoring, and expanded coverage on top of Security. Identity-only coverage available as an add-on user type.

SimpleShield Enterprise

> Top tier for environments with elevated security, compliance, or operational requirements. Includes the full Simple Tech security stack and expanded service-level commitments. Identity-only coverage available as an add-on user type.

8. Project Services

Non-recurring work delivered under Simple Tech's existing "Other Services" Statement of Work template, scoped and priced per engagement. Pricing is set in

the Rate Card or separately quoted in the Other Services SOW.

Cloud and Platform Migrations

> Migrations between on-premises and cloud platforms, between cloud providers (for example, Google Workspace to Microsoft 365), or between Microsoft 365 tenants. Includes discovery, planning, cutover, and post-migration support for a defined period.

Network Installation and Redesign

> Deployment of new network infrastructure or redesign of existing network environments, including firewalls, switches, access points, VLANs, and site-to-site connectivity.

Workstation Deployment Projects

> Imaging, provisioning, and deployment of new workstations in bulk. Priced on a per-device basis or as a project flat rate, depending on scope.

Server Builds and Deployments

> Specification, procurement, configuration, and deployment of new physical or virtual servers, including associated Active Directory, backup, and security configuration.

Extended Security Incident Remediation

> Incident response work extending beyond the initial response period defined in Section 2, including forensic analysis, coordinated containment, eradication, recovery, breach-notification planning support, and post-incident systems reconfiguration.

Office Moves and Site Build-Outs

> IT-side work to support office relocations or new-site openings, including network cabling coordination, equipment relocation, and cutover planning.

Hardware Procurement

> Procurement of hardware (workstations, servers, firewalls, switches, access points, network-attached storage, peripherals) on Client's behalf. Hardware costs are pass-through and billed in accordance with the Rate Card or a specific quote. Simple Tech is not the manufacturer and does not provide manufacturer warranty coverage.

Business Continuity and Disaster Recovery Planning

> Development or review of Client's business continuity and disaster recovery plans, including recovery time and recovery point objective analysis, documentation of recovery procedures, and coordination with Client's backup and infrastructure services. Where scoped in the SOW, includes tabletop exercises and periodic restore testing. This is planning and advisory work; actual recovery during an incident is handled under Extended Security Incident Remediation or a separate incident-response engagement.

Virtual CIO and Strategic Advisory

> Advisory-level engagements extending beyond the recurring Quarterly IT Management Meeting, including multi-year technology roadmap development, security strategy, IT budget planning, vendor consolidation analysis, and board-ready reporting. Delivered on a recurring retainer or project basis as set forth in the SOW. This is advisory work; Simple Tech does not act as a fiduciary.

Shadow IT Discovery and Remediation

> Discovery of unsanctioned applications and cloud services in use within Client's environment, assessment of associated risk, and coordinated remediation (consolidation onto sanctioned platforms, license recovery, data migration, decommissioning). Delivered as a project engagement.

9. Time and Materials / Break-Fix Services

For Clients who do not subscribe to a SimpleCare plan and instead engage Simple Tech on an as-needed basis. Engagements of this type are typically documented under Simple Tech's existing "Other Services" Statement of Work template (drafted by counsel) with appropriate scope and disclaimers.

Time and Materials Support

> Ad-hoc remote or on-site technical support delivered at hourly Rate Card rates, with no recurring obligation. Support is delivered on a best-effort basis during Business Hours. After-hours support, where available, is billed at after-hours rates. No managed monitoring, managed security, or proactive maintenance is provided under Time and Materials support unless expressly added under a separate SOW.

10. Minimum Requirements

Pursuant to Terms Section 4.1(h), Simple Tech requires Clients to maintain the following "Minimum Requirements" as an ongoing condition of service delivery. Any Device, Environment component, or software failing to meet these Minimum Requirements may be excluded from coverage in Simple Tech's sole discretion, and any services required to bring non-compliant items up to these standards are out-of-scope and will be quoted and billed separately.

Supported and Licensed Operating Systems

> All servers, desktops, laptops, and other covered devices must run an operating system that is (a) currently supported by the manufacturer (not in an "end-of-life" or "end-of-support" state), (b) genuinely licensed, and (c) kept current with all manufacturer-issued service packs and critical updates.

Active Third-Party Support Contracts

> All covered devices must be covered under currently active manufacturer or vendor support contracts, and all server and desktop software subject to the services must be genuinely licensed and supported by the applicable third-party provider.

Endpoint Protection

> The Environment must have a currently licensed, up-to-date, and third-party-supported endpoint protection solution (antivirus, EDR, or equivalent) protecting all servers, desktops, laptops, and email. Where Simple Tech delivers endpoint protection under an applicable SimpleCare plan, this requirement is satisfied by the Simple Tech-managed stack.

Backup Solution

> The Environment must have a currently licensed, third-party-supported backup solution in place for all systems and data for which recovery is expected. Where Simple Tech delivers backup under an applicable service, this requirement is satisfied by the Simple Tech-managed solution.

Hardware Firewall

> The Environment must have a currently licensed, third-party-supported hardware firewall deployed between the internal network and the public internet at each covered location.

Wireless Network Security

> All wireless data traffic within the Environment must be secured with, at minimum, WPA2 encryption using a strong pre-shared key or enterprise authentication. WEP, open networks, and deprecated encryption standards are not supported.

Multi-Factor Authentication on Administrative Access

> Multi-factor authentication must be enforced on all administrative accounts for Microsoft 365, Google Workspace, firewalls, remote-access gateways, and any system with access to Client-sensitive data.

11. Response Time Targets

Services are provided on a best-effort basis. Simple Tech prioritizes support requests based on business impact and severity, as determined by Simple Tech in its reasonable discretion. Simple Tech may reclassify or adjust ticket priority as additional facts become known. Simple Tech uses commercially reasonable efforts to respond to covered support requests within the target response times below during Business Hours. These response times are targets only, are not guarantees, and failure to meet any target response time does not constitute a breach of the SOW or the Terms.

PRIORITY	DEFINITION	EXAMPLE	TARGET
Emergency	Complete outage of core covered systems materially preventing	Server down, network failure, Microsoft 365 or Google Workspace outage affecting business	1–2 business hours

PRIORITY	DEFINITION	EXAMPLE	TARGET
	business operations, with no reasonable workaround	operations, active ransomware event	
High	Major issue significantly impacting a covered user or covered system, with no reasonable workaround	User unable to work, major application failure, significant access issue	Within 4 business hours
Medium	Partial loss of functionality or reduced performance where operations can continue	Application errors, file access issues, performance degradation	Within 8 business hours
Low	General support request, routine issue, or informational request	How-to questions, minor issues, non-urgent requests	Next business day

In smaller environments, a single-user issue will not automatically be classified as an Emergency unless it completely prevents business operations and no reasonable workaround exists. Internet outages caused by third-party carriers or providers will not be classified as Emergency unless Simple Tech determines otherwise in its reasonable discretion. Response targets apply only to Covered support requests properly submitted through Simple Tech's designated support channels and measure initial response time only, not time to resolution, remediation, or restoration.