Effective May 20, 2026. These Service Descriptions supersede and replace all prior versions.

Schedule of Services

MANAGED SERVICES

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

Provider, through its Third-Party Services Providers will make its best effort to ensure the security of Client's information through third-party security software ("Security Software"). Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this Service is subject to the applicable Third-party Service Providers agreements regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client acknowledges that Third-Party Service Providers and their licensors own all intellectual property rights in and to the Security Software. Client will not engage in or authorize any activity that is inconsistent with such ownership. Client acknowledges and agrees to be bound by any applicable Third-Party Service Provider agreements regarding terms or use or end user licensing terms, and Client understands that any applicable agreement regarding terms of use or end user licensing is subject to change without notice.

CORE Services Include:

Element	Component	Description
Server and Application Support *(Including MBTS Cloud Servers as noted in Section 3)*	Server Performance Monitoring (Applications, Hardware, and O/S)	Monitoring of the ongoing health, performance, and errors in Server class for server class OS applications and hardware components as well as errors in server-based Operating Systems (Windows, VMware, etc).
	Server Maintenance (hardware and O/S)	Maintenance of server equipment to ensure reliability and continued high quality service. Optimizing hard drive performance, clearing logs & temp files and other check listed maintenance items.

© Scott & Scott, LLP

	Microsoft Windows O/S Management	Hardware Patches, Feature Release, Hot fixes are updated on a regular basis to servers. This will be applied on Server class OS running on Server class hardware.
	Unlimited Remote Server Support and Troubleshooting	Remotely support Server class OS running Server class hardware and troubleshoot software and / or hardware issues during business hours.
	Unlimited Onsite Server Support and Troubleshooting	On an as needed basis during business hours.
Network Support Services	Router and Managed Switch Availability and Performance Monitoring	Monitor the ongoing availability and connectivity of networking hardware as well as performance bandwidth, traffic and errors of networking hardware.
	Unlimited Remote/Onsite Support and Troubleshooting for Routers and Managed Switches	Remotely support and troubleshoot software and or hardware issues during business hours. After-Hours support for critical issues.

© Scott & Scott, LLP

Disaster Recovery and Backup Support Services	Monitored Backup Solution	Monitor success, failure or errors related to your on-site and/or cloud backup solution.
Security Support Services	Availability / Connectivity Monitoring, and Security Performance Monitoring - Firewalls	Monitor availability and connectivity of the firewall to ensure the device is active. Monitor the health and operation of the firewall, including security incidents reported, network traffic, and device availability.
	Firewall Management	Maintain system version software and operating system of the firewall, continually manage policy and configuration changes; coordinate necessary service outages to minimize access and security interruptions.
	Password Management	Maintain and manage secure credential storage and password management systems, password policy standards; coordinate user access updates, credential rotations, and secure sharing practices to minimize security risks and unauthorized access
	Security Updates & Patching	Maintain and deploy security updates, operating system patches, and supported software fixes; coordinate necessary maintenance windows to minimize service interruptions and reduce security vulnerabilities.
	Endpoint & Cloud Protection	Maintain and manage endpoint and cloud security protection tools, monitor threat detection and response alerts, and coordinate remediation actions to reduce malware, ransomware, and unauthorized access risks.

© Scott & Scott, LLP

	Phishing Awareness & DarkWeb Scanning	Maintain and manage security awareness training and phishing simulation programs, monitor dark web exposure for compromised credentials and account risks; coordinate user notifications and remediation actions to reduce cybersecurity threats and unauthorized access.
	Privileged Access Management	Maintain and manage privileged access controls and approval workflows, monitor elevated permission requests, and coordinate access changes to reduce administrative risk and unauthorized system changes.
	MFA	Maintain and manage multifactor authentication controls, monitor enrollment and access activity, and coordinate user authentication updates to reduce unauthorized access risks.
IT Consulting Services	Network Health Review Meetings	Regularly scheduled meetings to review a multitude of network health reports and use it as an opportunity to prioritize projects, plan budgets and discuss other solutions that can improve the network.
	Reporting, technical analysis, technical usage, business impact	Regular reports that have analysis of technical issues. They include: Windows patch levels/success, backup performance, O/S errors, security issues, application compliance and more.
		Consultation for specific ongoing client needs, including: • Strategic Planning • HIPAA Compliance • Disaster Recovery • Technology Coordination • Vendor Liaison

© Scott & Scott, LLP

Desktop Services:

Desktop Support Services	Desktop Endpoint Patch Management	Management and monitoring of Windows patches from central console. Also includes popular third-party such as Adobe and Java.
	Desktop Endpoint Protection Management	Every desktop connected to the client network is required to run antivirus software. This forms the second line of defense against viruses - ensuring that if infected files are opened on client computers, the virus is identified and file access stopped, preventing further infection.
(Included with FULL Services Plan)	Unlimited Remote Workstation Support & Troubleshooting	Remotely support desktop workstations running Windows 11/10 or supported Mac OS & troubleshoot software and or hardware issues during business hours. Includes basic maintenance activities such as defrags, patch management, disk cleanup, check disk etc.
	Unlimited Onsite Workstation Support and Troubleshooting	Onsite support to troubleshoot software and or hardware issues during business hours.

**Provider does not provide internet connection. Client is responsible for providing internet connection to use the Service.

THESE DESCRIPTIONS ARE SUBJECT TO CHANGE ANY TIME WITHOUT NOTICE.

© Scott & Scott, LLP