Effective October 1, 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.

Server Monitoring and Management – Provider will perform server monitoring and management including, alert monitoring and management of servers, periodic reporting and performance tuning, and prioritization of alerts to identify high-priority incidents. Provider will also perform remote remediation services as needed, and backup software monitoring and management. The Service Fee does not include major hardware / software upgrades or replacements or new server installations.

Endpoint Monitoring and Management – Provider will perform endpoint monitoring and management including, alert monitoring & management of desktops, prioritization of alerts to identify high-priority incidents, remote remediation services as needed, configuration backups, firmware updates as required by manufacturer, and reporting and performance tuning. The Service Fee does not include hardware replacement or new hardware installations.

Help Desk Services – Provider will provide help desk support via client portal, e-mail, and phone. Provider has the ability to remotely control desktops to support employees. Unless otherwise included in an order, all help desk services will include unlimited remote support as required.

On-site Support - Upon request and subject to the limitations identified in the Order, for Services that are within the scope of this Service Attachment, Provider will also deliver support Services on-site at your location during normal business hours. For on-site support that is not included in the Order, Client will pay Provider's then-prevailing hourly rate.

Core Security Services – Provider will include in its services monthly Microsoft patch management, antivirus software and management, and remote software installations. Core Security Services also includes new / terminated employee setup and configuration.

Problem Management Services - Provider will undertake problem management as soon as the Provider's monitoring staff becomes aware of an incident. All incidents, with status or resolution, will be documented by posting updates to the Problem (Incident) Ticket Tracking System assigned to Client ("Problem Tickets").

© Scott & Scott, LLP

MANAGED SECURITY 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.

Managed Detection & Response - Managed Detection and Response (MDR) is a cybersecurity service that combines technology and human expertise to proactively hunt for, detect, and respond to threats across an organization's IT environment. MDR provides 24/7 monitoring, in-depth threat analysis, and hands-on incident response. It covers endpoints, networks, and cloud systems, helping businesses quickly contain and remediate attacks.

Firewall, Anti-malware, and Intrusion Detection – Depending on Firewall installed in client net, Provider will configure firewall traffic policies, apply updated firmware when applicable, and configure changes when needed. With respect to the firewall, Provider will include the following:

- Intrusion Prevention - provides real-time protection against network threats, including spyware, SQL injections, cross-site scripting, and buffer overflows.
- URL Filtering - blocks known malicious sites, and delivers granular content and URL filtering tools to block inappropriate content.
- Gateway Antivirus - continuously updated signatures, identify and block known spyware, viruses, trojans, worms, rogueware and blended threats – including new variants of known viruses.

Security Risk Assessment

- Malware and Vulnerability Review – Using one or more tools to determine the existence of malware or vulnerabilities.
- Personally Identifiable Information ("PII") – Review practices related to PII, including location, treatment, and risk mitigation.
- Report – Provider's findings will be included in a Risk Assessment Report.

Network Discovery - generates a visual map of all nodes on your network, making it easy to see where you may be at risk.

Reputation-Based Threat Prevention - Cloud-based web reputation service that aggregates data from multiple feeds to provide real-time protection from malicious sites and botnets, while dramatically improving web processing overhead.

Spam Prevention - Real-time, continuous, and highly reliable protection from spam and phishing attempts.

© Scott & Scott, LLP

Application Control – Provides the ability to allow, block, or restrict access to applications based on a user's department, job function, and time of day.

Threat Detection & Response - Security data collected from the firewall is correlated by enterprise-grade threat intelligence to detect, prioritize and enable immediate action against malware attack.

Intelligent Antivirus – leverages signature-less anti-malware solution that relies on artificial intelligence to automate malware discovery.

DNS Filtering - detects and blocks malicious DNS requests, redirecting users to a safe page with information to reinforce security best practices.

Anti-malware - Provider will provide and install anti-malware software of Provider's choosing for each Device covered by the Order. While Provider will make reasonable effort to ensure Client Devices and Client's network are safe from viruses, malware, bugs, hacking, phishing schemes or defective or malicious files, programs or links ("Harmful Content"), of any kind whether now known or hereinafter invented, Provider does not guarantee that Client computers or network cannot be infected by Harmful Content. Where this does happen, Provider will provide commercially reasonable Services to mitigate the Harmful Content. Additional Services will be available upon mutual agreement of the parties.

Remote Access - Provider will install remote access and remote monitoring and management software on Client's Devices possibly other equipment at Client's office. Client grants permission to Provider to install any remote access or remote monitoring and management software deemed necessary by Provider.

Client-Side DNS Filtering - Provider will acquire and will assign an appropriate number of licenses to support the deployment of client-side DNS Filtering on all laptop systems. The DNS filtering is designed to detect and block malicious DNS requests, redirecting users to a safe page with information to reinforce security best practices and to protect laptops while away from the corporate network.

Security Awareness Training & Phishing Simulations - Provider will acquire and will assign an appropriate number of licenses to support the client environment. The Service will schedule phishing campaigns to send at random times during a specified period. The campaigns are trackable and fully customizable designed to keep track of every user's participation, making all cybersecurity education accountable and measurable.

Dark Web Monitoring - Provider will monitor and scan underground marketplaces, forums, and data dumps for compromised credentials, sensitive data, or mentions of client business name — helping to proactively identify breaches or data leaks.

Multi-Factor Authentication Services / Password Credential Management Services – Provider will configure two-factor authentication for compatible software applications, institute single sign-on services for compatible software applications and customized security policies and procedures. After performing a security assessment and assessing the state of Client's existing policies and procedures pertaining to network security (if any), Provider will work with Client to prepare a new or revised set of policies and procedures that incorporate cutting edge best practices and that take advantage of the other Services delivered by Provider.

© Scott & Scott, LLP

Security Operations Center – The Services include:

- Advanced Malware Protection supported by Security Operations Center (SOC).
- Deployment of advanced malware protection applications to all Windows based devices on customer network.
- 24x7 SOC service analyzes quarantined applications and files, reducing false positives.

Immediate risk identification – Provides rapid recognition of thousands of viruses and malware attack variants, including crypto mining attacks, as well as the root causes of these malicious behaviors, by quickly identifying and diagnosing corrupt source processes and system settings.

Incident Response - Provider will assist Client in the hours immediately following a data breach to identify the likely source of the breach and to begin formulating an appropriate response to the breach. However, any assistance with data breach-remediation efforts past the first twenty-four (24) hours following a breach – including but not limited to breach-notification planning, in-depth forensic examinations of the source of a breach, and significant, post-breach systems reconfiguration – are not within the scope of this Service Attachment. If Client requests Provider's assistance with such activities, Provider will prepare a separate Service Attachment for Project Services that will specify what the charges will be for such assistance.

Zero Trust Access Management - Enforces identity verification and least-privilege access across applications and resources.

Zero Trust Endpoint Management: Validates the security posture of every device before granting access.

Security Information & Event Management (SIEM) - Centralized log analysis and correlation for advanced threat detection

DATA BACKUP AND DISASTER RECOVERY SERVICE

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 separate Order including those Services.

Local Backups - Using customer provided hardware and software (backup software), backups will be performed on the basis specified in the Order. Client owns the hardware and software agents (backup software) used to perform the backups. If Client subscribes to periodic Server Maintenance, Provider will review the backups during Maintenance and notify Client of backup failures. Client will notify the Provider of any failures, and upon request, perform simple on-site tasks (e.g., powering down and rebooting hardware).

Remote Backups - Provider, through its Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information. Data files are backed up via a third-party client-side desktop/server software application (the "Application"), encrypted, and then sent to a storage server at third-party vendor's data center facility. There is no local copy of the backed-up data. Data files can be restored from the cloud but the server itself cannot be recovered or "booted" in the cloud. Therefore, this service is not considered a disaster recovery solution. All data is backed up via a third-party client-side desktop/server software application (the "Application"). Provider will monitor the backups daily, notify Client of any failures, and work with third-party to resolve backup failures.

© Scott & Scott, LLP

Cloud Backup - Provider, through its Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information. Data is backed up via a third-party client-side desktop/server application, encrypted, stored locally on a Provider-owned storage device ("Provider Owned Storage"), and then sent to a third-party owned storage server at the Third-Party Services Provider's data center facility. Provider will monitor the status of all scheduled backup jobs, notify Client of Provider-owned storage failures and corrective actions. Provider will also provide remote administrative services of Data Backup Service as requested by Client. Offsite Backup copies will have one-year retention unless specified in Order. Upon termination of these Services, Provider will request return of the backup hardware and remove the Application from Client systems.

Disaster Recovery

Provider will work with Client to develop a comprehensive disaster-recovery plan that incorporates the Services to be delivered under this Service Attachment.

If Client experiences an event precipitating a major, multi-user loss of data, Client may notify Provider that a data loss event has occurred.

FILE BACKUP AND RECOVERY

Provider will create, monitor, and modify up to the number of file backup jobs listed in the Order. Provider will also notify Client by email of backup drive failures and corrective actions.

Upon request, Provider will remotely restore files, subject to the number of operations listed in the Order.

CLOUD AND HOSTING SERVICES

Public Cloud - Provider will move all Client's data to a cloud computing platform, allow Client to have access to data via virtual desktop from Client's own devices or device provided by Provider, and manage the cloud environment for Client.

Hybrid Cloud - Provider will move some of Client's data to a cloud computing platform, and upon Client's request, place a server on premises at Client's location. Any Client data being moved shall be agreed to by the parties in writing prior to moving with specific instructions as to identify which data will be moved, managed or unmanaged by Provider. Any Client data being moved or managed shall be specifically identified as to the location of the data on a particular server. Any Client data not being moved, or that is not specifically identified by Client will be considered not managed. Provider shall not be responsible for the identification, classification, or location of the data. Client is solely responsible for its data up to the outermost point of Provider's firewall with the public internet (the "Demarcation Point"). Once data has been identified, classified, its final location determined, and moved past the Demarcation Point, Provider shall then become responsible for Client data. Provider will also manage the cloud environment for client and provide hardware that will be owned by Provider and will be licensed using an appropriate license agreement.

Private Cloud or Software Subscriptions - Provider will maintain all Client's data on premise at Client's location, manage the cloud environment and software subscriptions for Client, provide unmanaged cloud environment and software subscriptions for Client, and provide

© Scott & Scott, LLP

hardware that will be owned by Provider and will be licensed using an appropriate license agreement.

Third-Party Cloud & SaaS Vendors - Provider will provide, install, and support the Third-Party Cloud or software-as-a-service vendors listed on the Order, including but not limited to Microsoft. 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 software is subject to the applicable third-party cloud or software-as-a-service vendor's agreement regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client agrees to be bound by any applicable third-party cloud or software-as-a-service vendor's agreements regarding terms or use or end user licensing, and Client understands that any applicable agreement regarding terms of user or end user licensing is subject to change by any Third-Party vendor or software-as-a-service provider without notice.

VOIP AND COLLABORATION SERVICES

Provider will deliver the Voice over Internet Protocol ("VoIP") and associated telephony and collaboration services specified and selected by you on the Order or Proposal. Additional Services may be added only by entering into a new Order including those Services.

The VoIP Services may be provided or delivered by Provider through the use of third-party vendors listed on the Order or Proposal. Use of the VoIP Services are subject to any applicable third-party vendor agreements. Client acknowledges and agrees to be bound by those thirdparty vendor agreements. Provider shall not be responsible for any third-party vendor service failures when accessing or using the Services. Client agrees to be bound by any applicable third-party vendor's agreements regarding terms and conditions or end user licensing, and Client understands that any applicable agreement regarding terms and conditions or end user licensing is subject to change by any third-party vendor without notice.

Network cabling, conduit, electrical, rack space, and any other required construction or trenching are additional charges are not included with the Service.

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

RETAINED IT SERVICES

Provider will deliver associated Retained IT services specified and selected by you on the Order or Proposal. Additional Services may be added only by entering into a new Order including those Services.

Retained IT Services may be provided or delivered by Provider through the use of third-party vendors listed on the Order or Proposal. Use of the Retained IT Services are subject to any applicable third-party vendor agreements. Client acknowledges and agrees to be bound by those third-party vendor agreements. Provider shall not be responsible for any third-party vendor service failures when accessing or using the Services. Client agrees to be bound by any applicable third-party vendor's agreements regarding terms and conditions or end user licensing, and Client understands that any applicable agreement regarding terms and conditions or end user licensing is subject to change by any third-party vendor without notice.

© Scott & Scott, LLP

Secure Workstation Plans

Secure Workstation Base - Keep every workstation protected, patched, and recoverable. This plan provides the essential building blocks for workstation security and continuity:

- **Remote Monitoring & Management (RMM):** 24/7 monitoring and proactive maintenance.
- **Endpoint Detection & Response (EDR):** AI-driven threat detection and rapid response to attacks.
- **Patch Management:** Automated security and software updates to reduce vulnerabilities.
- **File & Folder Backup:** Reliable daily backups to protect against accidental deletion or corruption.

Secure Workstation Ascend - Enhanced protection with layered defenses and greater recovery options. Everything in the Base Plan, plus:

- **DNS Filtering:** Blocks malicious websites and prevents phishing attempts before they reach your users.
- **Long-Term Retention:** Extended backup retention for compliance and peace of mind.
- **Image Backup:** Full system backup for complete workstation restoration in case of failure.

Secure User Plans

Secure User Base - Focused on protecting the individual user, their credentials, and their productivity tools:

- **Microsoft 365 Backup:** Safeguards email, OneDrive, SharePoint, and Teams data against loss or deletion.
- **Dark Web Monitoring:** Alerts if user credentials are found on the dark web.
- **IT Documentation:** Maintains detailed IT records for faster support and continuity.

Secure User Ascend - Advanced user security with proactive monitoring, filtering, and training. Includes everything in the Base Plan, plus:

- **Managed Detection & Response (MDR):** Proactive monitoring and response to detect and neutralize sophisticated threats.
- **Spam Filtering:** Blocks phishing, malware, and unwanted emails before they reach user inboxes.
- **Security Awareness Training:** Empowers employees to recognize and avoid cyber threats.

Secure Server Plans

Secure Server Base - Foundational server protection to ensure uptime and data safety.

© Scott & Scott, LLP

- **Remote Monitoring & Management (RMM):** Proactive monitoring and maintenance to minimize downtime.
- **Endpoint Detection & Response (EDR):** Advanced protection against malware and ransomware with rapid rollback capabilities.
- **Cloud Backup:** Reliable, secure offsite backups to safeguard critical business data.

Secure Server Ascend - Comprehensive server defense with deeper monitoring and compliance readiness. Everything in the Base Plan, plus:

- **Security Information & Event Management (SIEM):** Centralized log analysis and correlation for advanced threat detection.
- **Event Log Monitoring:** Real-time tracking of system and security logs to identify anomalies.

**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