Effective January 20, 2026. This Service Attachment for Managed Services supersedes and replaces all prior versions.

Service Attachment for Managed Services

This Service Attachment is between Provider (sometimes referred to as “we,” “us,” or “our”), and the Client found on the applicable Order (sometimes referred to as “you,” or “your”) and, together with the Order, Master Services Agreement, and other relevant Service Attachments, forms the Agreement between the parties the terms to which the parties agree to be bound.

The parties further agree as follows:

SERVICES

Provider will deliver only the Services itemized in the Services section of the Order. Additional Services may be added only by entering into a new Order including those Services.

Provider’s (typical) business hours are Monday – Friday, 8:00 am – 5:00pm Eastern Time.

Help Desk Support:

Help desk support is available during normal business hours. After-hours support is intended for critical systems outages. After-hours support may incur additional charges as defined by the Order.

On-site Support:

It is Provider’s intention to provide remote support whenever possible. On-site support is available once it is determined by Provider that the support cannot be provided remotely. Typically, this will be due to hardware issues or network connectivity issues. On-site support may incur additional charges as defined by the Order.

License

Provider hereby grants Client the right to access and use only those software solutions and other information technology Services specified on the Order during the Term. Those Services may be hosted on servers operated by one or more third parties.

License Restrictions

As between the parties, Provider retains all right, title and interest in and to the Services and their various components, along with all intellectual property rights associated therewith. Other than as expressly set forth in this Service Attachment, no license or other rights in or to the Services are granted to you, and all such licenses and rights are hereby expressly reserved. In addition, Client shall not:

© Scott & Scott, LLP

- Modify, copy or create derivative works based on the Services or on any Provider Materials;
- Create Internet "links" to or from the Services, or "frame" or "mirror" any content forming part of the Services, other than on your own intranet(s) or otherwise for your own internal business purposes;
- Distribute or allow others to distribute any copies of any Provider Materials or any part thereof to any third party;
- Rent, sell, lease or otherwise provide any third party with access to the Services or to any Provider Materials, or to any copy or part thereof, or use the Services or any Provider Materials for the benefit of a third party; or
- Remove, modify or obscure any copyright, trademark or other proprietary-rights notices that are contained in or on any Provider Materials.
- Reverse engineer, decompile, or disassemble the Provider Materials, except to the extent that such activity is expressly permitted by applicable law.

For purposes of this Service Attachment, “Provider Materials” means any text, graphical content, techniques, methods, designs, software, hardware, source code, data (including Reference Data), passwords, APIs, documentation or any improvement or upgrade thereto, that is used by or on our behalf to provide the Services.

Third-Party Service Providers

Some components of the Services may be provided through or licensed from Third-Party Service Providers, including but not limited to third-party software, products or services.

Provider, and not those third parties, will provide any and all technical support related to the Services, including support related to those third-party components. However, under certain circumstances, pursuant to the terms of applicable third-party license or services agreements, Provider may be obligated to provide certain information to those third parties regarding the Services and/or regarding your identity. Client consents to such disclosures.

Client understands and agrees that third-party services will be warranted only by the Third-Party Service Provider and only as and to the extent set forth in such provider’s license agreement, and that Provider will not be responsible, and makes no warranty, with respect to third-party services other than that which is expressly contained in the applicable Third-Party Services Provider’s agreements.

Third-party software publishers, including but not limited to, Microsoft will be intended third-party beneficiaries of the Agreement, with the right to enforce provisions of the Agreement and to verify compliance. If any third-party software publisher believes in good faith that Client is not complying with its end-user terms and conditions (“End-User License Agreement” or “EULA”), Provider will cooperate in good faith with the third-party publisher to investigate and remedy the non-compliance.

Within thirty (30) days of the termination of this Agreement, Provider shall remove, or cause to be removed, all copies of Client’s Services and/or Provider Materials from the Client’s devices, or otherwise render the software, the Services and/or the Provider Materials permanently unusable. Furthermore, Provider shall require that Client return or destroy all copies of the software, the Services and/or the Provider Materials that it received. Client shall reasonably cooperate and assist, as needed, with all such activities.

© Scott & Scott, LLP

No High-Risk Use

Client acknowledges that the Services are not fault-tolerant and are not guaranteed to be error-free or to operate uninterrupted. You shall not use the Services in any application or situation where the Services' failure could lead to death or serious bodily injury of any person, or to severe physical or environmental damage ("High-Risk Use"). High-Risk Use does not include utilization of the Services for administrative purposes, to store configuration data, engineering and/or configuration tools, or other non-control applications, the failure of which would not result in death, personal injury, or severe physical or environmental damage. Client agrees to indemnify and hold harmless Provider from any third-party claim arising out of Client's use of the Services in connection with any High-Risk Use.

No Illegal Use

Client shall not use the Services in any application or situation where the Services would be used for any illegal manner, for any unlawful purpose, or to violate the rights of others.

Restorable Backup

Prior to installation, or accessing, or using any Services specified on an applicable Order during the Term, Client shall create a full, complete, and restorable electronic backup of all systems which might be affected, in whole or in part, by the installation and/or maintenance of any software-solution and other information technology services specified on an applicable Order during the Term. Client shall, and does hereby, hold Provider harmless in the event of any damage to any system and applications software.

PROVIDER-SUPPLIED EQUIPMENT

Provider shall deliver the equipment and applications as identified in the Order ("Equipment"). Provider's delivery of that Equipment is on a rental basis only and is expressly subject to the terms of this Service Attachment pertaining to Provider-supplied Equipment.

Included Services

The Monthly Service Fee for Equipment includes all fees for the use of the Provider-owned hardware, software, operating systems, and all labor needed to install and maintain all hardware, software, operating systems delivered to client under this section.

Equipment Restrictions

All Equipment must be used by Client for the purpose for which it was intended. Client shall not abuse the Equipment or permit it to be serviced by anyone other than Provider. Neither Client nor Client's agent shall connect accessories supplied by anyone other than Provider to the Equipment without Provider's written consent, which shall not be unreasonably withheld. Client shall use the Equipment only in the manner contemplated by the manufacturer and in accordance with law. Client shall not allow anyone other than Provider to disconnect or move the Equipment from the location noted on the Order. Provider must be free to make any changes needed on the Equipment, including moving the equipment to another location, as deemed necessary by Provider only. Any critical business data stored on any Equipment must be backed up by Client.

Ownership of Provided Software

© Scott & Scott, LLP

Client acknowledges that its interest in any software installed by Provider on the Equipment is that of a licensee and that the software provided by Provider shall remain the property of Provider and must be returned if requested by Provider in furtherance of the Services or upon termination of this Agreement. Client further agrees to cease the use of any software or Equipment that remains the property of Provider upon cancellation or termination of this Attachment.

CREDENTIALS

Network Administrative Credentials – Provider must have exclusive network administrative credentials for Client's network. While it is providing Services, Provider will not release the network administrative credentials to Client or to any third party for any reason without a signed release acceptable to Provider. Upon termination, if Client has paid any and all required fees, including but not limited to, termination fees, remaining third-party service fees, and off-boarding fees, Provider will then release the network administrative credentials to Client.

User Credentials – User credentials are the property of Client, and Provider will not withhold individual user credentials to systems or applications.

Third-Party Global Admin Credentials (e.g., Microsoft tenant credentials) ("Client Credentials") - While it is providing services, Provider will not release Client Credentials to Client or to any third party for any reason without a signed release acceptable to Provider. Upon termination, if Client has paid any and all required fees, including but not limited to, termination fees, remaining third-party service fees, and off-boarding fees, Provider will then release Client Credentials to Client.

Third-Party Service Provider Credentials ("Provider Credentials") – In many instances, Provider licenses third-party tools and applications in order to assist with the provision of services to Client. Provider's Credentials for these tools (e.g., Duo, Kaseya, SentinelOne, Connectwise, etc.) will never be released to Client for any reason.

ADDITIONAL CLIENT OBLIGATIONS

Hardware Equipment

Client equipment must be maintained under a manufacturer's warranty or a current maintenance contract. Provider is not responsible for client equipment that is not maintained under a manufacturer's warranty or maintenance contract or that is otherwise out of order. All Service Fees assume equipment is under a manufacturer's warranty or maintenance contracts.

Provider in its reasonable opinion and supported by manufacturer information, may designate certain equipment as obsolete or defective, out of band, or end of life ("EOL"), and therefore exclude it from coverage under this Agreement.

Any equipment that is excluded from coverage due to lack of warranty, must be returned to being under warranty, at Client's expense, within no more than 30 days after the absence of warranty is discovered, provided a warranty is offered by the manufacturer. Any equipment found to unsupported and/or end of life by manufacturer, or which may be deemed to be defective beyond reasonable repair, and which cannot be brought under manufacturer's warranty due to warranty services no longer being available for said equipment, must be

© Scott & Scott, LLP

replaced, at Client's sole expense, within no more than 45 days after its discovery and communication thereof by Provider to Client.

Minor On-Site Tasks

Provider may occasionally ask Client to perform simple on-site tasks to assist our team with troubleshooting and/or installing new equipment (e.g., powering down or restarting a computer, checking cable connections, short-distance moving and/or connection of computers & peripherals, etc.). Client agrees to cooperate with all reasonable requests for remote assistance.

Client understands and agrees that Services are provided with the understanding of assistance from Client's staff, and Client will make someone available who can assist Provider in their task of addressing a Service request. Client agrees that it is at Provider's sole discretion whether to send a Provider resource/technician to Client location.

Server Upgrades or Repair

Provider will authorize, at its sole discretion, all necessary server upgrades or repairs. Client agrees not to perform any of these actions without Provider's explicit direction.

Software Media

Client shall obtain and supply all necessary software media with installation keys (if any) upon request.

Except for any software provided by Provider in connection with the Services, Client is solely responsible for obtaining all required software licenses, including all client access licenses, if any, for the software products installed on your computers.

Security and Regulatory Recommendations

Although it is under no obligation to do so, from time to time, Provider may make recommendations regarding regulatory compliance, safety and security related to Client's network and practices (e.g., multi-factor authentication, or "MFA"). If Client fails to adopt or implement the recommended protocols, Client is responsible for any and all damages related to regulatory, security, privacy, or data protection, including but not limited to fines, data breach notification, malware or ransomware costs, restoration, forensic investigation, restoring backups, or any other costs or damages related to Client's refusal to implement the recommended protocols.

NETWORK CHANGE COORDINATION

Significant Changes to Client's Network

Client will notify Provider via email of all significant proposed network changes and will provide us with a reasonable opportunity to comment and follow-up regarding those proposed changes.

Research Regarding Network Changes

Evaluation of network change requests sometimes will require significant research, design, and testing by Provider. These types of requests are not covered by this Service Attachment and will be billed at Provider's then-current rates for time and materials.

SUITABILITY OF EXISTING ENVIRONMENT

© Scott & Scott, LLP

Minimum Standards Required for Services

Client represents, warrants and agrees that its existing environment meets the following requirements or will obtain upgrades to its existing environment to meet the following requirements ("Minimum Standards"):

- All servers must be running a supported version of an operating system with all of the latest recommended patches and updates installed.
- All desktop PC's and notebooks/laptops must be running a supported version of the operating system with all of the latest recommended patches and updates installed.
- All server and desktop software must be genuine, licensed and vendor-supported.
- Provider must have exclusive administrative credentials to all Client network systems, or, if services are to be co-managed, the Client's (and any third-party MSP's specific agreement to the terms of the Shared Responsibilities Addendum.
- The environment must have a currently licensed, vendor-supported hardware firewall between the internal network and the internet.
- There must be an outside static IP address assigned to a network device, allowing secure VPN access.
- MS Active Directory, and/or MS EntraID/AzureAD, or other approved identity-management system

PCI-DSS (credit card)

- Segregated payment network
- Segregated wireless network from payment network
- MS Active Directory, EntraID/AzureAD, or other identity-management system

All costs required to bring Client's environment up to these minimum standards are not included in this Service Attachment.

If Client's environment fails to satisfy the above requirements at any time during the Service term, Provider may suspend further delivery of the Services and/or terminate this Service Attachment upon five (5) business days' advance, written notice.

EXCLUSIONS

Provider is not responsible for failures to provide Services that are caused by the existence of any of the following conditions:

- Expired Manufacturer Warranty or Support - Parts, equipment or software not covered by a current vendor/manufacturer warranty or support.
- Alterations and Modifications not authorized by Provider - Any repairs made necessary by the alteration or modification of equipment other than that authorized by Provider, including alterations, software installations or modifications of equipment made by Client's employees or anyone other than Provider.
- Hardware or Software Malfunction – Any time there is a defect or malfunction in any hardware or software not caused by Provider that adversely affects Provider's ability to perform the Services.
- Client Resource Problems – Any time a problem occurs resulting from a Client resource that are not under Provider's management or control.

© Scott & Scott, LLP

- Network Changes - Any changes Client may have made to the networking environment that were not communicated to or approved by Provider.
- Task Reprioritization - Any problems or failures related to a prioritization or reprioritization of tasks by Client.
- Force Majeure - Any problems resulting from a Force Majeure Event as described in the Master Services Agreement.
- Client Actions - Any problem resulting from Client actions or inactions.
- Client Responsibilities - Any problems resulting from Client's failure to fulfill any responsibilities or obligations under the relevant Agreements.
- Internet Connectivity Loss - Any loss of internet connectivity that occurs at Client locations for any reason.
- Software Maintenance - Any maintenance of applications software packages, whether acquired from Provider or any other source.
- Remote Computers - Home or remote computers that are not covered under the relevant Agreements.

Provider is not responsible for failure to provide Services that occur during any period of time in which any of the following conditions exist:

- Problem Ticket Management - The time interval between the initial occurrence of a desktop malfunction or other issue affecting functionality and the time Client reports the desktop malfunction or issue to Provider.
- Power Supply Malfunction – Instances where the battery, electricity, power-protective equipment or uninterruptable power supply (UPS) malfunctions and renders Provider unable to connect to the network or troubleshoot the device in question.
- Third-Party Criminal Activity - Provider is not responsible for criminal acts of third parties, including but not limited to hackers, phishers, crypto-locker, and any network environment subject to ransom. Client agrees to pay ransom or hold provider harmless for any activity effecting network security on your environment related to third-party criminal activity. Any costs or fees to rebuild or service machines are provided and sold separately by Provider.
- Malware - Provider is not responsible for any harm that may be caused by Client's access to third party application programming interfaces or the execution or transmission of malicious code or similar occurrences, including without limitation, disabling devices, drop dead devices, time bombs, trap doors, Trojan horses, worms, malware, viruses and similar mechanisms. Any costs or fees to rebuild or service machines are provided and sold separately by Provider.

The following list of items are excluded from the scope of included Services, and may incur additional charges or require a separate billable project:

- Software Maintenance – Unusual work that results from a failed software patch or update that results in an interruption in Client's business, with the exception of Microsoft Windows updates and patches.
- Programming Modifications – Any programming (modification of software code) and program (software) maintenance occurs.
- Training - Any training service of any kind, unless otherwise agreed to in an Order.

© Scott & Scott, LLP

- Software and Web Development - Any Services requiring software and web development work.
- Remote Computers – Unless otherwise specified in an Order, home or remote computers that are not covered under the Agreement.
- Replacement Software – Implementation of new or replacement software.
- Relocation / Satellite Office – Office relocation/satellite office setup.
- Equipment Refresh – Any non-workstation equipment refreshes.
- Incident Response – Provider will assist Client in the hours immediately following a data security incident to identify the likely source of the incident and to begin formulating an appropriate response. 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 an Order that will specify what the charges will be for such assistance.

The following list of items are costs that are considered separate from the Service pricing:

- Costs Outside Scope of the Service – The cost of any parts, equipment, or shipping charges of any kind. The cost of any software, licensing, or software renewal or upgrade fees of any kind. The cost of any third-party vendor or manufacturer support or incident fees of any kind. The cost of additional facilities, equipment, replacement parts, software or service contract.

The following is a list of Services Provider does not perform:

- Printer Hardware Repair - Printer hardware repair or maintenance work.
- Third-party Vendor Disputes - The management or involvement with disputes or charges with any third-party vendor, other than issues relating to the technical services.

RIGHT TO ACT AS AGENT AND SITE PREPARATION

- Client designates Provider to act as agent for Client in ordering necessary services or entering trouble tickets from phone service carriers and internet access providers, whenever applicable. Client agrees to (a) furnish and install all conduit, raceway or low smoke cable and to create all holes and wireways through concrete, plaster, metal floors, walls or ceilings which may be required for the installation of the Equipment, (b) provide all commercial AC power circuits required for the operation of the Equipment, (c) pay for all electrical current necessary for the operation of the Equipment and (d) provide a suitable space for the operation of the Equipment consistent with the recommendations of the manufacturer, including, but not limited to, providing a dry and dust-free environment. Provider shall have no duty, responsibility or obligation to make any structural alterations or adjustments to the premises to install the Equipment. Client shall provide Provider with reasonable access to the premises during Provider's working hours and shall furnish elevator service when necessary as well as heat, light, sanitary facilities, electrical power and protection of the Equipment from theft during installation. Provider is not responsible for restoring Client's premises to its original condition upon removal or relocation of any or all of the Equipment.

© Scott & Scott, LLP

VOIP INDEMNIFICATION

In addition to your indemnification obligations in the MSA, you shall defend, indemnify, and hold harmless Provider, its officers, directors, employees, affiliates and agents and any other service provider who furnishes services to you in connection with this agreement, from any and all claims, losses, damages, fines, penalties, costs and expenses (including, without limitation, reasonable attorneys' fees) by, or on behalf of, you or any third party or user of the Service relating to the absence, failure or outage of the Service, including Emergency Calling Service dialing and/or inability of you or any third person or party or user of the Service to be able to dial 911 or to access emergency service personnel.

PROVIDER OBLIGATIONS

In addition to delivery of the Services, Provider accepts the following obligations under this Service Attachment:

Data Security and Privacy

In addition to its other confidentiality obligations under this Service Attachment, Provider shall not use, edit or disclose to any party other than Client any electronic data or information stored by Provider, or transmitted to Provider, using the Services ("Client Data"). Provider further shall maintain the security and integrity of any Client Data under Provider's direct control, in accordance with any parameters described in this Service Attachment.

As between Provider and Client, all Client Data is owned exclusively by Client. Client Data constitutes Confidential Information subject to the terms of the MSA, and shall be returned to Client upon request, provided that Client is current in all payments, termination fees, and third-party service fees. Provider may access Client's User accounts, including Client Data, solely to respond to service or technical problems or otherwise at Client's request.

Maintenance Windows

Routine server and application maintenance and upgrades will occur during scheduled maintenance windows, and some applications, systems or devices may be unavailable or non-responsive during such times.

WARRANTY

- Provider warrants that the Services will be performed materially in accordance with the service documentation previously provided for the Services in a professional and workmanlike manner.
- **HOWEVER, PROVIDER DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR COMPLETELY SECURE. THERE ARE RISKS INHERENT IN INTERNET CONNECTIVITY THAT COULD RESULT IN THE LOSS OF YOUR PRIVACY, CONFIDENTIAL INFORMATION, AND PROPERTY. WE HAVE NO OBLIGATION TO PROVIDE SECURITY OTHER THAN AS STATED IN THIS SERVICE ATTACHMENT. WHILE THE SERVICES ARE DESIGNED TO IMPROVE THE PROBABILITY OF THE PROTECTION AND RECOVERY OF INFORMATION COMPARED TO THE CLIENT'S CURRENT METHODS EMPLOYED, PROVIDER MAKES NO CLAIMS OR WARRANTIES THAT DATA BACK-UPS AND DATA / SERVER / DESKTOP RECOVERIES USING THE SERVICES WILL BE ERROR FREE**

© Scott & Scott, LLP

OR THAT ALL RECOVERIES CAN BE PERFORMED WITHIN A CERTAIN TIME FRAME.

- **IN ADDITION, CLIENT ACKNOWLEDGES THAT THIS AGREEMENT CONVEYS NO WARRANTIES, EXPRESS OR IMPLIED, BY ANY THIRD-PARTY VENDORS OF SOFTWARE PRODUCTS MADE AVAILABLE TO CLIENT BY PROVIDER AND THAT THOSE VENDORS DISCLAIM ANY AND ALL LIABILITY, WHETHER DIRECT, INDIRECT OR CONSEQUENTIAL, ARISING FROM THE SERVICES.**

SERVICE FEES

Onboarding Fee

Prior to the delivery of the Services, Provider may charge an Onboarding Fee in order to deploy and configure the Services under this Service Attachment. Provider will identify the Onboarding Fee in an initial invoice, and Client shall pay the Onboarding Fee, as set forth in the Master Services Agreement ("MSA"). Provider shall have no obligation to continue with the delivery of any Services under this Service Attachment until it receives payment for the Onboarding Fee.

Service Fees Increases

In addition to the Service Fee increases described in the MSA, Provider may adjust the fees for the following reasons:

End-User or Network Growth. During the term of an Order, if the number of users or devices in Client's environment or the Service or Equipment types or quantities to be covered within the scope of the Order exceeds the numbers, types or quantities previously ordered, Provider may apply an adjustment to the total Service Fees. Client shall pay all Service Fees owed as they become due following any such adjustment.

Similarly, during the term of an Order, if the number of users or devices in Client's environment or the Service or Equipment types or quantities to be covered within the scope of the Order is less than the numbers, types or quantities previously ordered, upon request, Provider will apply an adjustment to the total Service Fees. Client shall pay all Service Fees owed as they become due following any such adjustment. However, under no circumstances may any such adjustments result in a number of users or devices in Client's environment or in any Service or Equipment types or quantities to be covered within the scope of the Order that is less than the numbers, types or quantities ordered at the time Client signed that Order.

"User" means Client's employees, consultants, contractors or agents who are authorized to use the Service and have been supplied user identifications and passwords by Client (or by Provider upon Client's request). Users do not include any customers of Client or other third parties.

"Device" means any equipment included in the Services, whether owned by Client or provided by Provider for Client's use, including, but not limited to computers, printers, servers, routers, and mobile or handheld microcomputers as well as the software necessary to operate such equipment.

TERM AND TERMINATION

Term

© Scott & Scott, LLP

This Service Attachment is effective on the date specified on the Order (the “Service Start Date”). Unless properly terminated by either party, this Attachment will remain in effect through the end of the term specified on the Order (the "Initial Term"). If no term is listed on the Order, then the initial term shall be thirty -six (36) months from date of Order acceptance.

Renewal

"RENEWAL" MEANS THE EXTENSION OF ANY INITIAL TERM SPECIFIED ON AN ORDER FOR AN ADDITIONAL TWELVE (12) MONTH PERIOD FOLLOWING THE EXPIRATION OF THE INITIAL TERM, OR IN THE CASE OF A SUBSEQUENT RENEWAL, A RENEWAL TERM. THIS SERVICE ATTACHMENT WILL RENEW AUTOMATICALLY UPON THE EXPIRATION OF THE INITIAL TERM OR A RENEWAL TERM UNLESS ONE PARTY PROVIDES WRITTEN NOTICE TO THE OTHER PARTY OF ITS INTENT TO TERMINATE AT LEAST SIXTY (60) DAYS PRIOR TO THE EXPIRATION OF THE INITIAL TERM OR OF THE THEN-CURRENT RENEWAL TERM. ALL RENEWALS WILL BE SUBJECT TO PROVIDER’S THEN-CURRENT TERMS AND CONDITIONS.

Early Termination by Client With Cause

Client may terminate this Service Attachment for cause following sixty (60) days’ advance, written notice delivered to Provider upon the occurrence of any of the following:

- Provider fails to fulfill in any material respect its obligations under the Service Attachment and fails to cure such failure within thirty (30) days following Provider’s confirmation of receipt of Client’s written notice of such breach. .
- Provider terminates or suspends its business operations (unless succeeded by a permitted assignee under the Agreement).

Early Termination by Client Without Cause

If Client has satisfied all of its obligations under this Service Attachment, then no sooner than ninety (90) days following the Service Start Date, Client may terminate this Service Attachment without cause during the Initial or a Renewal Term (the “Term”) upon sixty (60) days’ advance, written notice, provided that Client pays Provider a termination fee equal to any discounts or concessions provided, plus fifty percent (50%) of the recurring, Monthly Service Fees remaining to be paid from the effective termination date through the end of the Term, based on the prices then in effect.

Termination by Provider

Provider may elect to terminate this Service Attachment upon thirty (30) days’ advance, written notice, with or without cause. Provider has the right to terminate this Service Attachment immediately for illegal or abusive Client conduct. Provider may suspend the Services upon ten (10) days’ notice if Client violates a third-party’s end user license agreement regarding provided software. Provider may suspend the Services upon fifteen (15) days’ notice if Client’s action or inaction hinder Provider from providing the contracted Services.

Effect of Termination

As long as Client is current with payment of: (i) the Fees under this Attachment, (ii) the Fees under any Order for off-Boarding, and/or (iii) the Termination Fee prior to transitioning the Services away from Provider’s control, then if either party terminates this Service Attachment,

© Scott & Scott, LLP

Provider will assist Client in the orderly termination of services, including timely transfer of the Services to another designated provider. Client shall pay Provider at our then-prevailing rates for any such assistance. Termination of this Service Attachment for any reason by either party immediately nullifies all access to our services. Provider will immediately uninstall any affected software from Client's devices, and Client hereby consent to such uninstall procedures.

Upon request by Client, Provider may provide Client a copy of Client Data in exchange for a data-copy fee invoiced at Provider's then-prevailing rates, not including the cost of any media used to store the data. After thirty (30) days following termination of this Agreement by either party for any reason, Provider shall have no obligation to maintain or provide any Client Data and shall thereafter, unless legally prohibited, delete all Client Data on its systems or otherwise in its possession or under its control.

Provider may audit Client regarding any third-party services. Provider may increase any Fees for Off-boarding that are passed to the Provider for those third-party services Client used or purchased while using the Service.

Client agrees that upon Termination or Off-Boarding, Client shall pay all remaining third-party service fees and any additional third-party termination fees.

© Scott & Scott, LLP

ADDENDUM
Shared Responsibilities between Internal IT/MSP and MSSP

Overview:

As Exceed Cybersecurity and IT Services (referred to hereafter as "MSSP") and Client Internal IT and/or MSP (referred to hereafter as "Internal IT/MSP") are entering into a parallel relationship with overlapping services and responsibilities to provide comprehensive security and IT support to mutual clients, below is an explanation of shared responsibilities regarding the execution of this relationship. This is not intended to be an exhaustive list of responsibilities, rather a summarily established guideline. The terms of the Managed Service Attachment to which this Addendum is attached shall control over any contrary provision of this Addendum.

Roles and Engagement:

MSSP specializes in advanced security solutions including End User Security Training and Phishing

Simulation, Password Management Systems, Next Gen Antivirus (NGAV), Managed Extended

Detection and Response with a Security Operations Center (MXDR/SoC), Security Ingestion and

Event Management (SIEM), Advanced Email Security, Vulnerability Management, Web Content Filtering, Zero Trust Endpoint Protection, Software as a Service (SaaS) Monitoring and Alerting, software licensing in a security context, and development and support of Written Information Security Plans.

Internal IT/MSP specializes in general helpdesk support, network and device patch management, and software licensing in a general support system context.

Both companies will collaborate closely to ensure seamless integration of services for mutual clients. Communication channels will be established for efficient issue resolution, reporting, and project management.

Shared Responsibility Matrix:

Service	MSSP Responsibilities	Internal IT/MSP Responsibilities	Minimum Security Plan Required
General Helpdesk Support	Provide security-specific escalation support, including investigation of potential incidents and ensuring secure resolution.	Provide day-to-day incident resolution, user support, and non-security-related troubleshooting.	All Plans
Network and Device Patch Management	Monitor and verify patches for vulnerabilities; ensure reporting on critical updates impacting security posture.	Plan and deploy patches across devices and systems; maintain documentation for patch management activities.	All Plans
Software Licensing	Manage and track licenses for security tools (e.g., SIEM, EDR); ensure compliance with securityrelated licensing agreements.	Manage and track licenses for general IT tools (e.g., productivity software); handle renewals and troubleshooting of licensing issues.	All Plans
End User Security Training and Phishing Simulation	Develop and deliver tailored training programs; monitor phishing simulation results and escalate significant findings for further action.	Deploy training software on end-user devices and ensure participation; monitor end-user compliance and escalate as needed.	Plan 1 - Basic
Firewall Management	Configure and manage firewall rules to align with security policies; monitor traffic for threats and respond to potential breaches.	Provide awareness and assist with on-site troubleshooting; escalate complex issues or security events to MSSP.	Plan 1 - Basic
Dark Web Monitoring	Perform continuous monitoring for exposed credentials or sensitive information on the dark web; escalate actionable intelligence.	Stay informed of findings and assist in implementing preventive measures or remediation.	Plan 1 – Basic
Technology Business Reviews	Plan and conduct strategic security reviews; provide recommendations for improving the organization's security posture.	Participate in reviews, ensure adherence to action plans, and align IT initiatives with security objectives.	Plan 1 - Basic
Password Management Systems	Deploy and manage secure password tools; monitor for suspicious activity and ensure compliance with password policies.	Roll out password tools to users; ensure end-user adoption and adherence to password policies.	Plan 1 - Basic
Advanced Email Security	Deploy and configure email security tools (e.g., anti-phishing, antispam); monitor email activity and respond to threats.	Monitor end-user compliance and report unusual emailrelated issues to MSSP for deeper investigation.	Plan 2 - Advanced

© Scott & Scott, LLP

MXDR/SoC	Provide 24/7 monitoring, threat detection, and incident response services; escalate issues to Internal IT for remediation where needed.	Support on-site incident remediation; provide context and feedback for escalated incidents.	Plan 2 - Advanced
Security Ingestion and Event Management (SIEM)	Deploy, configure, and maintain the SIEM platform; analyze logs and correlate events to identify potential threats.	Ensure logs are properly generated from IT systems; provide support for event investigation and remediation.	Plan 2 - Advanced
Zero Trust Endpoint Protection	Configure and manage Zero Trust policies on endpoints; monitor compliance and respond to any deviations.	Ensure endpoints are properly configured for Zero Trust compliance; provide end-user support for access issues.	Plan 2 - Advanced
SaaS Monitoring and Alerting	Monitor SaaS applications for suspicious activity; provide alerts and actionable insights for incidents.	Manage end-user permissions and ensure SaaS applications are configured to meet operational requirements.	Plan 3 - Elite
Vulnerability Management	Perform scans, assess vulnerabilities, and develop remediation plans; provide prioritization guidance for critical findings.	Execute remediation plans for identified vulnerabilities; ensure timely patching and configuration updates.	Plan 3 - Elite
Secure Access Service Edge (SASE)	Deploy and manage SASE infrastructure; monitor traffic for threats and enforce security policies.	Manage local connectivity and ensure systems are properly routed through SASE infrastructure; escalate network issues as needed.	Plan 3 - Elite
Secure DNS	Configure and monitor DNS for threats, ensuring it aligns with security policies; respond to DNSrelated security incidents.	Manage DNS records for operational needs; escalate DNS issues or suspicious activity to MSSP.	Plan 3 - Elite
Deep Packet Inspection for Endpoints	Deploy and monitor deep packet inspection tools to identify suspicious activity; respond to alerts.	Ensure endpoints are properly configured for inspection; escalate findings requiring advanced analysis.	Plan 3 - Elite
Web Content Filtering	Configure and manage web filtering policies; monitor for access to malicious or inappropriate sites and respond to incidents.	Ensure web filtering tools are deployed to end-user devices; report issues or policy violations to MSSP.	Plan 3 - Elite
Written Information Security Plan	Develop, maintain, and update the WISP to reflect current security practices; ensure compliance with regulatory requirements.	Review and adhere to the WISP; assist in implementing security practices outlined in the plan.	Plan 3 - Elite

Exclusions:

MSSP Exclusions:

- All general IT and end user support.
- Licensing management for non-security software.
- Physical hardware maintenance and service.

Internal IT/MSP Exclusions:

- Advanced security solutions beyond basic endpoint and server protection.
- Security consulting and specialized security training.
- Development and implementation of comprehensive security strategies beyond basic network and device patch management.

© Scott & Scott, LLP