Effective June 7, 2024. This Service Attachment for Managed Security Services supersedes and replaces all prior versions.

Service Attachment for Managed Security 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, Schedule of Services, 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:

Provider will deliver only the Services itemized in the Services section of the Order. The following is a list of available Managed Services. Additional Services may be added only by entering into a new Order including those Services.

MANAGED SECURITY SERVICES

To the extent ordered by Client, Provider will deliver to Client the Managed Security Services ("Service") listed below. Unless otherwise indicated in the Order, Provider will deliver the Services on an ongoing basis.

- 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.

If included in the Order, the Services includes the following:

<u>Firewall, Anti-malware, and Intrusion Detection</u>

- Installation and configuration of firewall traffic policies.
- Apply updated firmware when applicable.
- Configuration changes when needed.
- Software services included on firewall:
    - Intrusion Prevention - provides real-time protection against network threats, including spyware, SQL injections, cross-site scripting, and buffer overflows.

© Scott & Scott, LLP

    - URL Filtering - blocks known malicious sites, and delivers granular content and URL filtering tools to block inappropriate content.
    - Gateway Anti-malware - continuously updated signatures, identify and block known spyware, malware, trojans, worms, rogueware and blended threats – including new variants of known malware.
- 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.
- 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.
- APT Blocker - detects and stops the most sophisticated attacks including ransomware, zero-day threats, and other advanced malware designed to evade traditional network security defenses.
- Data Loss Prevention – works to enforce compliance by scanning text and files to detect sensitive information attempting to exit your network, whether it is transferred via email, web, or FTP.
- 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 Anti-malware – 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.

<u>Security Risk Assessment</u>

- 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.

<u>Client-Side DNS Filtering</u>

Provider will acquire and will assign an appropriate number of licenses to support the deployment of client-side DNS Filtering on all systems.

The Service includes the following:

- Detects and blocks malicious DNS requests, redirecting users to a safe page with information to reinforce security best practices.
- Protect systems while away from the corporate network.

© Scott & Scott, LLP

Security Awareness Training & Phishing Simulations

Provider will acquire and will assign an appropriate number of licenses to support the client environment.

The Service includes the following:

- Scheduled phishing campaigns to send at random times during a specified period.
- Trackable, fully customizable training course campaigns. Keep track of every user's participation, making all cybersecurity education accountable and measurable.
- Full catalog of cybersecurity and compliance training courses.

Multi-Factor Authentication Services / Password Credential Management Services

- Two-factor authentication for compatible software applications.
- Single Sign-on services for compatible software applications
- 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.

Security Operations Center

- Advanced Malware Protection supported by Security Operations Center (SOC).
- Deployment of advanced malware protection applications to all Windows based devices on Client 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 cryptomining attacks, as well as the root causes of these malicious behaviors, by quickly identifying and diagnosing corrupt source processes and system settings.
- Ransomware rollback - quickly rollback files to previous safe versions through tracking changes in your devices and restoring them to an acceptable risk state.
- Network Vulnerability Scans – perform scans of internal and external networks for open ports and vulnerabilities on network attached devices.

Security Log Management.

- Configure log sources to capture and retain information without creating excessive logging.
- Limit user access to log files.
- Avoid logging sensitive or protected information.
- Secure the processes that generate logs.
- Identify and resolve logging errors.
- Analyze log entries, prioritize entries, and respond to those requiring action.

© Scott & Scott, LLP

Security Incident Event Management (SIEM) Services supported by SOC.

- Deployment of SIEM monitoring probes to monitor all critical network devices including; domain controller, firewalls, network switches, and routers. When meeting compliance requirements, deployment will include all Windows devices as well.
- Reporting for compliance requirements - generate daily reports and threat analysis outlines for three regulatory standards: HIPAA, PCI and NIST-800.
- SOC expertise and assistance.

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.

SUPPORT SERVICES

Coverage

Provider shall provide remote help desk and vendor management services through remote means during Provider's normal working hours.

Support Outside Normal Working Hours

Upon request, Provider shall perform emergency Services outside of normal working hours at the rates and according to the guidelines specified in the Order.

Maintenance Windows

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

CLIENT ENVIRONMENT STANDARDS

In order for Client's existing environment to qualify for Provider's Services, the following requirements must be met:

- All servers with Microsoft Windows Operating Systems must be running a supported version of Windows Server, have all of the latest Microsoft Service Packs and Critical Updates installed, and be patched within 30 days of the last patch.
- All desktop PC's and notebooks/laptops with Microsoft Windows Operating Systems must be running a supported version of Windows, have all of the latest Microsoft Service Packs and Critical Updates installed, and be patched within 30 days of the last patch.
- All server and desktop software must be genuine, licensed, and vendor-supported.
- All wireless data traffic in the environment must be securely encrypted.
- Provider may deliver on-site Equipment in order to meet service requirements, as needed.

© Scott & Scott, LLP

- Client's network environment must be configured with centralized authentication services such as Microsoft Active Directory or Radius services.

Healthcare Clients

- MS Active Directory, or similar identity-management system

PCI-DSS (credit card)

- Segregated payment network
- Segregated wireless network from payment network
- MS Active Directory, or similar 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.

ADDITIONAL CLIENT OBLIGATIONS

Minor On-Site Tasks

Provider may occasionally request Client staff to perform simple on-site tasks. Client shall comply with all reasonable requests.

Server Upgrades or Repair

Provider will authorize the conduct of all server upgrades or repair. Client shall not perform any of these actions without Provider notification.

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-factored authentication). 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 shall notify Provider via email of all significant proposed network changes and shall provide the opportunity for Provider to comment and follow-up.

Research Regarding Network Changes

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

© Scott & Scott, LLP

SERVICE FEES

Service Fees

For the Services described in this Service Attachment selected or ordered by Client, Client shall pay the Service Fees specified in the Order that is in effect at that time.

Client Delay

If Provider is unable to commence delivery of the Services on the Managed Services Start Date because of any failure on the part of Client (including but not limited to failure of Client to provide the Client resources in a timely manner), Client nonetheless will begin to incur Service Fees, which Client shall pay in accordance with this Service Attachment, beginning on the Managed Services Start Date.

EXCLUSIONS

We are 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 Malfunction – Anytime where 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 – Anytime a problem occurs resulting from a Client resource that are not under Provider's management or control.
- 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 that were contrary to our reasonable recommendations.
- Client Responsibilities - Any problems resulting from your failure to fulfill any responsibilities or obligations under our 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 Agreement.

© Scott & Scott, LLP

We are not responsible for failures 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 an uninterruptable power supply (UPS) or other power-protective equipment 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 affecting 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 cause 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.
- Hardware Equipment - Client equipment must be maintained under manufacturer's warranty or maintenance contract and in working order. Provider is not responsible for client equipment that is not maintained under manufacturer's warranty or maintenance contract or that is otherwise out of order. All fees, warranties, and liabilities against Provider assumes equipment is under manufacturer's warranty or maintenance contracts and is in working order.

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 specified in the Order.
- Software and Web Development - Any Services requiring software and web development work.
- Remote Computers - 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.

© Scott & Scott, LLP

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.

TERM AND TERMINATION

Term

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").

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.

Month-to-Month Services

If the Order specifies no Initial Term with respect to any or all Services, then we will deliver those Services on a month-to-month basis. We will continue to do so until one party provides written notice to the other party of its intent to terminate those Services, in which case we will cease delivering those Services at the end of the next calendar month following receipt of such written notice by the other party.

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 receipt of Client’s written notice.
- Provider terminates or suspends its business operations (unless succeeded by a permitted assignee under the Agreement).

© Scott & Scott, LLP

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 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 hinders 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 Project Services Attachment or Statement of Work 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, 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 consents 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