Effective March 04, 2025. This Service Attachment for Penetration Testing Services supersedes and replaces all prior versions.

Service Attachment for Penetration Testing 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:

Description of Services

Provider will deliver only the Services itemized in the Services section of the Order. The following is a list of available Services. Additional Services may be added only by entering into a new Order including those Services. The Services are designed to assess the security of Client's computer networks. These Services are designed to identify, evaluate, and report on vulnerabilities and potential threats within Client's network infrastructure. The key components of the Services include:

- **Network Scanning**: Conducting thorough scans of the Client's network to identify active devices and potential points of vulnerability.
- **Vulnerability Assessment**: Evaluating the identified vulnerabilities in the network infrastructure to determine the risk level and potential impact on the Client's operations.
- **Security Auditing**: Reviewing and analyzing the security measures currently in place to identify weaknesses or non-compliance with industry best practices and standards.
- **Ethical Hacking**: Simulating cyber-attack scenarios to test the effectiveness of security protocols and identify vulnerabilities that could be exploited by malicious actors.
- **Reporting**: Providing detailed reports that include findings, evidence of testing, analysis of vulnerabilities, and recommendations for security enhancements.

Provider may use one or more of the following steps in providing the Services:

- **Initial Consultation**: Working with the Client to understand their network architecture, key assets, and specific areas of concern.

© Scott & Scott, LLP

- **Planning and Preparation**: Developing a tailored testing plan that outlines the methodologies, tools, and techniques to be used, ensuring minimal disruption to the Client's operations.
- **Testing Execution**: Conducting the penetration tests as per the agreed plan, which may include, but is not limited to, network penetration, application testing, wireless network testing, and social engineering tactics.
- **Vulnerability Analysis**: Analyzing the results of the tests to identify and categorize vulnerabilities based on their severity and potential impact.
- **Post-Testing Review**: Meeting with the Client to discuss the findings and provide an initial overview of vulnerabilities and security gaps.
- **Report Delivery**: Delivering a comprehensive report that details the findings, methodologies used, evidence of testing, and practical recommendations for remediation and enhancing security posture.
- **Feedback and Follow-Up**: Offering the Client an opportunity to provide feedback on the Services and discussing potential follow-up actions or retesting if required.

ADDITIONAL CLIENT OBLIGATIONS

Access and Cooperation

Client will provide necessary access to all relevant systems, networks, and information as required for the Services. Client shall also ensure full cooperation from its staff and third-party contractors if necessary.

Data Backup

Ensure comprehensive backup of all data and systems prior to the commencement of testing to prevent data loss or system downtime.

Legal and Regulatory Compliance

Client is responsible for ensuring that the penetration testing is conducted in compliance with all applicable laws and regulations. This includes obtaining necessary consents and approvals if the testing involves third-party systems or data.

Disclosure of Known Risks

Inform Provider of any known risks, sensitive data, or critical systems that require special consideration during testing.

Security Measures Post-Assessment

Implement appropriate security measures to address vulnerabilities identified in the reports. Client is responsible for the decision and action regarding these recommendations.

Notification of Changes

Inform Provider of any significant changes to the network or systems that may affect the scope or safety of the penetration testing.

Hardware Equipment

© Scott & Scott, LLP

Client equipment must be maintained under manufacturer's warranty or maintenance contract or is 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 manufactures warranty or maintenance contracts or is in working order.

Provider in its reasonable opinion and supported by manufacturer information, may designate certain equipment as obsolete or defective, and therefore exclude it from coverage under this Agreement.

Minor On-Site Tasks

Provider may occasionally ask you to perform simple on-site tasks. You agree to cooperate with all reasonable requests.

Project Coordination

Provider will coordinate with the appropriate contractors and Client representative to ensure the below are completed appropriately.

Worksite Responsibilities

- Provide access to the work site during agreed upon times for work to be performed during Provider's normal business hours.
- Ensure that during agreed-upon work times, client shall provide keys, ID badges, security clearance, parking, and access to loading docks as may be required by Provider.
- Clear the schedule in room(s) or office during these times so that Provider is not interrupted and forced to stop work prematurely. This includes Client personnel inquiring about the status or functionality of the project prior to the completion of the installation.
- Client understands that if work is stopped at their request that it may result in changes to project schedule or result in rescheduling of the project.
- Client shall inform Provider of any work areas where it has knowledge or reason to believe that facility may have hazardous materials such as Asbestos, Lead, or PCB's.

EXCLUSIONS

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

- 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.

© 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 that were contrary to our reasonable recommendations.
- Client Responsibilities - Any problems resulting from Client's failure to fulfill any responsibilities or obligations.
- Internet Connectivity Loss - Any loss of internet connectivity that occurs at Client locations for any reason.
- Software Maintenance - Any maintenance of applications software packages are involved, whether acquired from Provider or any other source.

We are not responsible for failures to provide Services that occur during any period of time in which any of the following conditions exist:

- Power Supply Malfunction – Instances where an uninterruptable power supply (UPS) or 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. You agree 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 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 or is 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 manufactures warranty or maintenance contracts or 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:

- Training - Any training service of any kind, unless specified in the Order.
- Software and Web Development - Any Services requiring software and web development work.

© Scott & Scott, LLP

- Remote Printers-– Unless otherwise outlined in an Order, Home or remote printers 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.
- Remediation of Vulnerabilities -- The Services do not include the actual remediation of identified vulnerabilities or implementation of security measures. Provider's role is limited to the identification and reporting of potential security weaknesses.
- Hardware and Software Corrections -- Any modifications, repairs, or replacements of Client's hardware or software are outside the scope of these Services.
- Guarantee of Security -- Provider does not guarantee that the network will be free from unauthorized intrusions or breaches post-testing.
- Long-Term Monitoring -- Continuous or long-term monitoring of the network post-testing is not included. The Services are confined to the agreed-upon penetration testing period.
- Compliance Certification -- The Services do not include certifications of compliance with specific regulatory standards (e.g., PCI-DSS, HIPAA). However, recommendations provided may assist in achieving such compliance.
- Liability for Security Breaches -- Provider is not liable for any security breaches, data loss, or any other damages that occur either during or after the provision of the Services, except as expressly covered under the Master Services Agreement.

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.

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

© Scott & Scott, LLP

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 such written notice is received 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).

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 all discounts and 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 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 consent to such uninstall procedures.

© Scott & Scott, LLP

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