Summary

Allied Marketing (Customer) has requested a security assessment of their network infrastructure. Winslow Technology Group (WTG) proposes an approach based on the services selected in the phases below. The focus of this assessment is to expose vulnerabilities and determine an organizations risk in order for them to perform proper remediation. The assessment process is intended to review Customer's security infrastructure; defined as procedural, technical and non-technical security initiative of the organization as a whole. Services are delivered by Secure Network Technologies ("SNT").

About SNT: Secure Network has achieved its growth and expertise as leading experts in cyber security. They focus on the risks that WTG's customers face every day, by employing the best certified information security engineers, understanding how the risk landscape is changing and addressing those risks with state-of-the-art tools and techniques. Combining these four elements with the use of tested methodologies and established standards, customers can maintain the integrity, and availability of mission critical assets.

WTG Professional Services Deliverables

The phases proposed define the services that will be performed. Each phase examines a security initiative that will determine the security posture of customer network.

THE PHASES INCLUDE:

1. Identify Internal Network Vulnerabilities
2. Assumed Breach

SERVICES

INTERNAL PENETRATION TEST

Secure Network's methodology of penetration testing applies a consistent and reproduceable approach that combines comprehensive identification and validation of risk-based vulnerabilities. This methodology ensures that common threat actor Techniques, Tactics, and Procedures (TTPs) are applied to each penetration test, identifying real world attack paths within the customer environment.

During the **Planning** phase, Secure Network will collaborate with customer Point of Contacts (PoC) to discuss Scope, Rules of Engagement, and to outline what to expect during the

penetration test. Senior cyber security engineers will be involved with PoC planning meetings to detail engagement information and to answer any questions or concerns.

The start of the penetration test will begin with the **Reconnaissance** phase. This phase consists of gathering information about targets within the pre-defined scope. Discovery and full-port scans are conducted to identify assets within the environment, which types of operating systems and services are in use, and what level of network segmentation is in-place. This phase will drive identification of potential initial foothold vectors.

The **Exploitation** phase will begin once an attack path to an initial foothold is discovered. This initial foothold may be exposed via software or services vulnerabilities, misconfigurations, man in the middle attacks (MITM), credential stealing, monitoring, or information leakage.

Once the initial foothold has been accomplished, Secure Network will move into **the Post-Exploitation** phase. This phase combines Reconnaissance and Exploitation phases to determine the likely attack paths of real-world threat actors. Analysis of Active Directory, base line security configurations, user access, password policies, AV/EDR capability with the potential of using custom payloads, and defense in depth will be exposed to demonstrate the actual impact that an adversary would have within the environment.

The **Reporting** phase will occur after attack paths and vulnerabilities have been exploited and validated. Reports will consist of relevant attack paths and TTPs that were executed against the customer environment. Secure Network does not create reports based on vulnerability scanner output or CVSS scores, but instead uses extensive experience and expertise to assign risk to individually exploited vulnerabilities, misconfigurations, and relevant attack paths to give the customer an immediately actionable report. Mitigation techniques are included in details of findings, where applicable, to provide guidance and a starting point to reduce the overall risk to the customer environment.

Deliverables:

Secure Network will deliver the final penetration testing report to the customer which will include identified and exploited attack paths, risk-based findings, finding remediation guidance (where applicable), and customer risk-based matrix. Secure Network will also deliver artifacts from the penetration test which may include tool output created during the penetration test. These artifacts can include files such as discovery scans, Active Directory reconnaissance, internal web application screenshots, etc.

ASSUMED BREACH

Secure Networks Assumed Breach penetration test will determine what actions can be taken by a threat actor that has successfully gained access to the internal network from an external context, such as phishing an employee or exploiting an externally facing host. This test will assess and discover the most likely attack paths that would be used by the attacker to move laterally and escalate privileges throughout the customer domain, with the purpose of gaining access to High Value Assets (HVA) or to escalate to Domain Admin, for the likely outcome of distributing ransomware or stealing protected or proprietary information.

SNT applies a consistent and reproduceable approach that combines comprehensive identification and validation of risk-based vulnerabilities. This methodology ensures that both new and common threat actor Techniques, Tactics, and Procedures (TTPs) are applied to each test, identifying real world attack paths that could be exploited within mature organizations.

During the **Planning** phase, SNT will collaborate with customer Point of Contacts (PoC) to discuss Scope, Rules of Engagement, and to outline what to expect during the assumed breach penetration test. Senior cyber security engineers will be involved with PoC planning meetings to detail engagement information and to answer any questions or concerns.

The **Reconnaissance** phase will be the beginning of the assumed breach scenario. With access to a Windows based workstation or server, SNT will implement commonly used threat actor TTPs to gain information about user context, host, AV/EDR, and the customer domain.

The **Exploitation** phase will begin once a privilege escalation vulnerability has been discovered. This initial vulnerability may be exposed via software or services vulnerabilities, misconfigurations, man in the middle attacks (MITM), credential stealing, monitoring, or information leakage.

The **Post-Exploitation** phase continues the exploitation of the attack path to validate the likelihood of a real-world threat actors' ability to compromise the customer domain. In-depth analysis of Active Directory, base line security configurations, user access, AV/EDR capability, and defense in depth will be exposed to demonstrate the actual impact that an adversary would have within the environment.
The **Reporting** phase will occur after the conclusion of testing. Any attack paths or vulnerabilities that have been discovered and exploited will be disclosed. Mitigation techniques are included in details of findings, where applicable, to provide guidance and a starting point to reduce the overall risk to the customer environment. Complete movements of

the threat emulation, along with their corresponding Mitre ATT&CK mapping, will be included in the report to give the customer a exact replication of the attack.

Deliverables:

SNT will deliver the final report to the customer along with detailed mappings of the attack path. The deliverables will also include any artifacts gathered during the attack, such as Active Directory enumeration output and privilege escalation tests.

RULES OF ENGAGEMENT

1. Secure Network will employ individuals with demonstrated expertise in this area.
2. Secure Network will NOT perform Distributed Denial of Service (DDoS) testing against any Customer systems.
3. Secure Network will perform all penetration testing during normal business hours of 8:00am – 5:00pm EST, unless stated otherwise by the customer during SOW stages.
4. In the event any network or system performance issues are seen on the Customer network, Secure Network requests to be notified immediately to let Customer troubleshoot the issue.
5. Secure Network certifies that the applicable background checks have been performed on individuals engaging in the penetration test.
6. During testing, if a potentially critical issue is discovered, it will be communicated to Customer as soon as possible.
7. Customer expects Secure Network to execute activities to ensure there is no data destroyed. Penetration test activities are limited to gaining access and reading system or security data and not specifically taking control of the system or deleting data. Creation or escalation of privileges or the placement of a small text file is acceptable.
8. Business production activities must continue. Any penetration testing during normal business hours of 8:00am – 5:00pm EST may be executed as long as prior coordination is done, and there is reasonable assurance that the device / system will not be taken out of service. Testing Activities of the web server must not result in loss of service or changes in system functionality, data or data presentation. Activities which could potentially cause a device / server to go down should be scheduled outside normal business hours with the applicable coordination.

9. Full communication of testing activities and schedule is necessary prior to execution. Coordination may be needed with external entities for a test to be executed. Due to production requirements, potential disruptive activities need to be planned for, communicated, and resolved as soon as possible.
10. Once Customer has determined there are no further questions or detail needed, Secure Network will close the project out. Secure Network will keep information up to six (6) months and then will erase any information regarding customer's vulnerabilities, network, systems, etc., unless notified to destroy prior. Secure Network shall securely protect any Customer information in its possession. The applicable Customer team will be notified as soon as practical of a system or network component that is found to be compromised or impacted due to the penetration activities so the unit may be restored to business operation.

CUSTOMER RESPONSIBILITIES

Customer agrees to provide timely access to all personnel, resources (including all necessary hardware, software, and network access) and requested information that is deemed necessary to ensure that we can fulfill its commitments stated herein. When possible, we will make reasonable efforts to provide lead-time to Customer. Typically, this notification will occur at the weekly status meetings. Customer also specifically agrees to:

1. Ownership of Systems: Customer warrants and represents that it is the owner of any network, systems, IP addresses, and/or computers upon which Secure Network performs the Services ("Customer Systems"), or that Customer is authorized to instruct Secure Network to perform Services on such Customer Systems pursuant to this SOW. Customer shall indemnify and hold harmless Secure Network for any claims by any third parties with respect to a breach of the foregoing warranty.
2. Assign a Point of Contact to represent Customer. The Point of Contact will have decision-making authority for most matters that may arise and will serve as an escalation point for relevant security testing activities, per the rules of engagement and cease-and-desist procedures. This Point of Contact will also be the escalation point for critical vulnerabilities identified during the course of the engagement.
3. Ensure that the Point of Contact be available to meet with us for status meetings at a frequency determined during the Kickoff Meeting.
4. The Customer Point of Contact will be responsible to facilitate the scheduling of interviews and information gathering sessions within Customer's organization unless other arrangements are agreed upon by the Point of Contact.

5. Provide all information and materials identified throughout the SOW on time. To the best of Customer ability, applicable pre-assessment evidence will be prepared prior to the site visits.
6. If applicable, provide proper documentation for existing network.
7. Provide Secure Network with the necessary physical and/or system access required to complete the deliverables.
8. Provide appropriate personnel to assist in identifying users of systems and contact information.
9. Provide timely access to staff and personnel to answer questions regarding business or network information.
10. Make Customer assets (network, application and users) available for observation at appropriate points in this engagement.
11. Inform us of any developments in other projects that might impact this engagement.
12. Notify Secure Network of and make available to us all relevant and previously developed information and documentation.
13. Provide us with all relevant documentation and information as it pertains to the business requirements and current network infrastructure at the kickoff Meeting.

If Customer fails to perform any of the responsibilities set forth herein, the parties agree to resolve the situation via the Change Order Process. Notwithstanding the foregoing, neither of the parties is bound to use the Change Order Process in the event of a material breach by the other party.

ACCEPTANCE OF DELIVERABLES

During the project kickoff meeting, the Winslow Technologies Deliverables will be reviewed. Completion of these deliverables will be used as the basis to determine the delivery team's execution of this SOW. If Customer does not believe noted Deliverables have been completed, a written reason should be provided back to Winslow Technologies within three (3) business days of receipt so Winslow Technologies can review and address issues with Customer. The deliverables will be considered as "accepted" within three (3) business days of delivery, unless noted by a written reason.

DELIVERABLES

Based on the scope of work, Secure Network has determined the deliverables for this project to be a security assessment of the Customer's network. The report will be documented into a variety of deliverables that will be included as follows:

Security Assessment Report

This report will detail the findings as identified in the customer's statement of work (SOW):

1. Detailed Vulnerability Report of Findings
2. Technical Data Obtained During Assessment

Executive Summary or Letter of Attestation can be provided upon request

Fee Schedule

SKU	Description	Fee
SNT-INT-50-100	Internal Penetration Test of 50-100 IP's	
SNT-BREACH	Assumed Breach Testing performed after the pen test is complete	$25,400.00
NA	Travel and Expense	$0.00
	Total	$25,400.00

An authorized signature and valid purchase order (PO) authorize the performance of this Statement of Work. Until provided, the terms, conditions, and pricing of this agreement are valid for 30 days from date of presentation. A valid PO is required, prior to scheduling or performance of any WTG Services.

Product Special Terms

If Customer elects for a rescan/retest of the found vulnerabilities, the Statement of Work will be broken out into two engagements. Each one will be invoiced separately, once for the initial engagement and a second invoice for the rescan following the inhouse/third party network remediation.

If a Secure Network Field System is used, this device must be returned to Secure Network within 7 days of the delivery of the Final Report. For every day past the allowable time, a $50 per day charge will be incurred above the agreed upon quote.

***Holiday Schedule**

- New Year's Day

- Martin Luther King Day
- President's Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- Day after Thanksgiving
- Christmas

Additional Terms and Conditions

1. The Service ("Services") are provided by Winslow Technology Group, LLC., with a place of business at 303 Wyman Street, Waltham, MA 02451 ("WTG", "us", "our", or "we"), to you ("Client", "you", or "your"). Your initial and on-going use of the Service indicates you agree with this Service Agreement. This agreement and its terms shall be governed by and enforced in accordance with the laws of the Commonwealth of Massachusetts.

2. Patches and other software-related maintenance updates ("Updates") may be provided and applied by WTG. WTG shall install Updates only if WTG has determined, in its reasonable discretion, that the updates will be compatible and are materially beneficial to the features or functionality of the applicable software or hardware. WTG will not be responsible for any downtime or losses arising from or related to the installation or use of any update, provided that the update was installed in accordance with the manufacturer's or applicable vendor's instructions. WTG will also not be responsible for any downtime or losses arising from not installing or applying an update or patch.

3. You agree to promptly follow and implement any direction we provide to you. WTG will make a reasonable effort to optimize and configure systems to avoid additional cost, however, depending on the situation, you may be required to make additional purchases or investments. If your failure to follow or implement WTG's advice renders part or all of the Services economically or technically unreasonable to deliver (in WTG's sole discretion), then WTG may terminate the applicable SOW for cause. Any services required to correct or remediate issues caused by your failure to follow WTG's advice or direction, as well as any services required to bring the systems up to minimum requirements, will be billed to you at WTG's then-current hourly rates.

4. You hereby grant to WTG the right to monitor, diagnose, manipulate, communicate with, retrieve information from, and otherwise access your computer systems for the purpose of providing the Service. It is your responsibility to secure, at your own cost and prior to the commencement of any Services, any necessary rights of entry, licenses, permits or other permissions necessary for WTG to provide the Service. Proper and safe environmental conditions must be provided and assured by you at all times. WTG shall not be required to engage in any

activity or provide any Services under conditions that pose or may pose a safety or health concern to any personnel, or that would require extraordinary or non-industry-standard efforts to achieve.

5. You understand and agree that WTG will be required to rely on any direction or consent provided by your personnel or representatives.

6. WTG-provided equipment: Under some circumstances WTG provides equipment to deliver all or part of a Service. If you are in receipt of WTG-provided equipment, except for ordinary wear and tear, you are responsible for protecting the equipment from damage, theft, destruction, and loss of any kind. If the equipment is damaged or lost, you agree to notify us immediately.

7. Services will be performed on a schedule, and in a prioritized manner, as determined by WTG and mutually agreed upon cadence.

8. For Northstar Managed Services: The Services shall commence on the Effective date and shall remain in effect until the Termination date or if the Agreement is terminated by WTG for cause. The Effective date is the first kick-off call to commence the Service and begin onboarding. The Termination date is the duration indicated in the Agreement from the Effective date. Service will automatically renew for a 1-year term at after Termination date, with a 7.5% increase. If no duration is indicated the Agreement is for 1-year.

9. Changes or additions to the Service shall be handled through our standard change process, including a detailed explanation of the change and impact to the overall Service. All change requests require approval by both WTG and Client.

10. WTG shall, in connection with its performance of Services, use reasonable efforts to adhere to all Client's policies and procedures that have been communicated to and accepted by WTG in writing.

11. The Services are contemplated for the benefit of your environment. As such, WTG is not responsible for your environment. This includes: uptime, data integrity, data breach, security, privacy, and the like. You should retain or have access to an Incident Response provider (via insurance or otherwise). In the event of a breach (or similar), WTG can provide additional services at a fee. Under no circumstances will WTG be responsible for any data lost, corrupted, or rendered unreadable for reasons including, but not limited to: (i) communication and/or transmissions errors or related failures, (ii) equipment failures (including but not limited to silent hardware corruption-related issues), (iii) WTG's failure to backup or secure data from portions, or (iv) cybersecurity incident/data breach. WTG does not warrant or guarantee that any system will operate in an error-free manner.

12. Each party shall maintain, at its own expense, such insurance as will fully protect itself from any claims or damages for death, and bodily injury, cybersecurity incident, and damage to real and tangible personal property with respect to its own employees and property which it owns or

leases or otherwise exerts control over. Each party agrees to furnish evidence of insurance coverage upon the reasonable written request of the other party.

13. Client will pay all fees agreed upon in a WTG quote, SOW or Agreement, including expenses and applicable taxes, if any, within thirty (30) days of the receipt of WTG's invoice, unless Client reasonably disputes an amount contained on an invoice. Additional or different terms included on a purchase order issued by Client to order, process, or pay for Services, shall not amend these terms; such additional or different terms shall be of no force or effect.

14. In the event Client disputes an invoice amount, Client and WTG agree to use their best efforts to resolve such dispute as soon as possible within sixty (60) days after Client provides written notification and supporting documentation to WTG. Late payments on undisputed amounts shall bear interest at the lesser of one and a quarter percent (1.25%) per month or the highest rate permitted under law.

15. WTG represents and warrants that it shall perform the Service in accordance with industry, OEM and generally accepted standards. In the event Client gives WTG written notice of non-compliance within ten (10) days of Client receiving Services, WTG shall have the opportunity to promptly correct or re-perform the Services.

16. Each party acknowledges that certain information that it shall acquire from the other party is of a special and unique character and shall, provided such materials are clearly marked as such, constitute "Confidential Information". Having acknowledged the foregoing, each party agrees: (a) to exercise the same degree of care and protection with respect to the other party's Confidential Information that it exercises with respect and governed by the local regulation(s) to its own Confidential Information, but in no event less than reasonable care; and (b) not to directly or indirectly disclose, copy, distribute, republish or allow any third party to have access to any Confidential Information of the other party.

17. NEITHER PARTY SHALL IN ANY EVENT BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, PUNITIVE, SPECIAL OR SIMILAR DAMAGES INCLUDING, WITHOUT LIMITATION, LOSS OF PROFITS (EXCEPT FOR FEES DUE AND OWING TO WTG), LOSS OF REVENUES, LOSS OF DATA, DATA BREACH, CYBERSECURITY INCIDENT OR FOR COVER AND THE LIKE, EVEN IF EITHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF THE OCCURRENCE OF SUCH DAMAGES.

18. NEITHER PARTY MAKES ANY OTHER EXPRESS OR IMPLIED REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE SERVICES TO BE PERFORMED BY WTG OR ANY DELIVERABLES THAT MAY RESULT THEREFROM. BOTH PARTIES DISCLAIM ALL OTHER EXPRESS AND IMPLIED WARRANTIES INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

19. Any changes to these terms shall be amended to a unique and specific Statement of Work ("SOW"). From time to time, these terms and conditions maybe amended with or without notice. It is your responsibility to regularly review WTG's Service Agreement available at:

https://winslowtg.com/services-terms-and-conditions/

Signatures

The following signatures authorize the performance of this Statement of Work. Until signed, the terms, conditions, and pricing of this agreement are valid for 30 days from date of presentation. This signed Statement of Work and purchase order are required, prior to scheduling or performance of any WTG services.

Accepted on behalf of **Client** by:

Signature:	DocuSigned by: Mike Eggermann 680E49D897B5484...
Printed Name:	Mike Eggermann
Title:	VP, IT
Date:	9/20/2023

Accepted on behalf of **Winslow Technology Group, LLC** by:

Signature:	DocuSigned by: 0962763AE714410...
Printed Name:	Winslow Technology Group
Title:	VP, Professional Services and Cybersecurity
Date:	9/19/2023